SVDI

DOSSIER
VIDEOPROTECTION

La Vidéoprotection :

20 ans d'évolution

Adresse postale :
5 rue de l'Amiral Hamelin
75116 PARIS
Tél : 01 44 05 84 40
Fax : 01 44 09 73 01
Mail : [illegible]
WWW.svdi.fr

PANORAMA VIDEOPROTECTION [1995 – 2015]

Le déploiement de la vidéoprotection [vidéosurveillance] s'amorce en France au cours des années 1980-1990 et est surtout le fruit d'initiatives privées : Commerces, Banques, entreprises tertiaires, etc…, ainsi que dans le secteur des transports [*SNCF : les premiers équipements de ce type ont été testés en 1976*]. De leur côté les autorités publiques installent des caméras afin de protéger leurs bâtiments [*défense ou d'intérêt stratégique*]. Dans la majorité des cas, ces caméras ont pour unique objectif la « protection des biens » [*protection des immeubles, ou des valeurs entreposées dans ceux-ci*].

1. La perception de la vidéosurveillance par les français :

Particulièrement décriée dans les années 90 où elle est corrélée à l'effet romanesque du livre « 1984 » [*qui narre, la surveillance du public par un état devenu totalitaire, dans le roman de George Orwell*], elle conserve encore aujourd'hui pour certaines ONG, militants associatifs ou élus, une mauvaise image, ceux-ci dénonçant son inefficacité et son risque sur les libertés fondamentales.

Dans certaines villes, elle est utilisée dans de nombreuses variantes et plus seulement pour des objectifs sécuritaires. [Vidéoverbalisation à Nice, Marseille]. Pour la population elle est entrée définitivement dans les mœurs ; en effet, en 2008, 71 % des Français se déclaraient favorables à la présence de caméras de vidéoprotection dans les lieux publics [*Sondage réalisé par ipsos pour la CNIL en mars 2008*].

Début 2013, pas moins de 75 % des Français interrogés se disent favorables (75 %) au développement de la vidéoprotection dans les centres villes et les transports [*Sondage Bva réalisé en février 2013*], seulement 23 % y sont opposés. En septembre 2013, 83 % des personnes interrogées approuvent la mise en place de caméras de vidéoprotection et 72 % des Français accepteraient en outre un système de reconnaissance faciale via une caméra et 82 % l'utilisation de la biométrie (puce contenant par exemple des empreintes digitales) dans la carte d'identité ou le permis de conduire … [*Sondage ipsos pour les salons Milipol, septembre 2013, cité par la Gazette des communes*].

Si les résultats en matière de lutte contre la délinquance et la criminalité sont sujettes à caution [débats contradictoires entre plusieurs experts statisticiens], elles apportent à la population un effet bénéfique portant sur la très subjective notion de « sentiment de sécurité ». Il est cependant établi que les villes équipées de systèmes de vidéoprotection, voient baisser le nombre de violences aux personnes.

2. L'utilisation de la technologie a ouvert le champ à un questionnement juridique inédit :

Les premières réflexions sur la justification de la vidéosurveillance et les risques en matière de libertés publiques apparaissent dans les années 1990, l'un des plus emblématiques exemples est celui de la commune d'Avignon, qui voit son souhait d'installation d'un réseau de caméras géré par un poste central refusé par le Tribunal administratif de Marseille au motif que : «*l'installation généralisée et le fonctionnement permanent de caméras portaient une atteinte excessive aux libertés individuelles et notamment au droit à la vie privée et à l'image qui n'était justifiée ni par une habilitation judiciaire, ni par les nécessités de l'ordre public ou la constatation ponctuelle d'infractions au code de la route ou d'atteintes aux biens ou aux personnes* ». Un autre cas en 1993 celui de la commune de Levallois Perret, fut traité non par le tribunal administratif territorialement compétent mais par la CNIL [*Commission Nationale Informatique et Libertés*]. Elle souligne que ce système de contrôle est de nature à constituer un risque pour les libertés et principalement celle, fondamentale et constitutionnelle, d'aller et venir et qu'il pouvait également occasionner des atteintes à la vie privée. Sans avis tranché du conseil constitutionnel, on estime que cette ville d'Ile de France, fut celle qui a officiellement lancé le développement des systèmes de vidéosurveillance en France.

La même année survient dans un procès prudhommal, la première initiative de remise en cause de l'installation d'un système vidéosurveillé ! Dans le secteur de la logistique, l'employeur d'un entrepôt décide d'installer une vidéo dans le but de « surveiller » les salariés [*soupçonnés de détournement et du vol de marchandises*]. Ce cas a donné matière aux avocats des salariés, pour contester « l'objectif initial de l'installation » jugé profondément arbitraire ; mais aussi de juger de l'absence de preuves par l'inadéquation de la technologie (qualité des objectifs médiocres, qualité des images en noir et blanc imprécises voire floues, qualité de l'enregistrement par cassette VHS réutilisables produisant des images fantômes dues à un sur-enregistrement). Ce cas est inédit, car il permit aux salariés « incriminés » de pouvoir se sortir de l'acte d'accusation a connu de nombreux rebondissements judiciaires avec la victoire juridique de l'employeur en 2001 … Cassation sociale, 31 janvier 2001, n° 98-44.290, Alaimo c/ Sté Italexpress transports.

3. Une réglementation orientée sur l'utilisation :

Pour ce qui concerne son utilisation [exploitation] ; elle a bénéficié d'un cadre normatif en 1995 [toujours en vigueur, Loi n° 95-73 du 21 janvier 1995

d'orientation et de programmation relative à la sécurité, Article 10] et s'est aujourd'hui imposée dans le paysage urbain, les établissements ouverts au public, comme dans l'ensemble des espaces gérés par le privé. En 2013, la mise en œuvre d'un Code de Sécurité Intérieure est venue étoffer de nouveaux textes sur la vidéoprotection.

L'avènement du terrorisme djihadiste le 11 septembre 2001 à New-York, et les attentats de Madrid en 2004, et de Londres en 2005 ont permis de démontrer, l'efficacité des dispositifs de vidéosurveillance, aidant les enquêteurs à remonter les suspects des cellules et éviter de nouveaux attentats en identifiant et diffusant dans les médias les quatre poseurs de bombes [la qualité des images diffusées ont impressionné les principaux responsables de la sécurité intérieure des différentes capitales européennes]. Il est à noter qu'à l'époque des rapports critiquent le faible impact de la vidéosurveillance à Londres dans la lutte contre la délinquance, qui bien que disposant de 5000 caméras (4 millions d'unités dans tout le Royaume Uni), n'aide pas à limiter la propagation des agressions physiques. Cette critique rencontra un écho également en France entre supporters et détracteurs du système, et une bataille sémantique s'empare des experts comme des politiques sur l'efficacité de la technologie, les premiers parlant de « Vidéoprotection », les autres de « Vidéosurveillance ».

Selon un rapport de l'IGA [Institut Général de l'Administration] du 22 février 2010, « Efficacité Vidéoprotection Globale », il est indiqué que :

- La délinquance a baissé en moyenne plus fortement dans des communes équipées de vidéoprotection que dans celles qui ne disposent pas de vidéoprotection urbaine. Les atteintes volontaires à l'intégrité physique [AVIP] y ont, en outre, été mieux contenues comparativement aux données nationales. L'effet préventif et dissuasif est toutefois mieux marqué en zone de gendarmerie qu'en zone police ;
- Les enquêteurs ont recours de manière quasi-systématique aux images enregistrées lors des investigations, en particulier pour les faits graves. Le nombre de réquisitions d'images enregistrées progresse fortement. Le nombre de personnes mises en cause, pour lesquelles la vidéo a joué un rôle, augmente de manière significative et atteint près de 30% des personnes en zone de gendarmerie pour la délinquance de proximité;
- Le taux d'élucidation global ne progresse significativement que dans les villes où une forte densité de caméras a été installée. Dans les villes équipées de vidéoprotection, les taux d'élucidation progressent plus rapidement dans les zones équipées que dans les secteurs sans vidéoprotection ;

- La localisation des caméras, la qualité des images et des enregistrements sont déterminants pour une utilisation à des fins d'enquête judiciaire et la collecte d'éléments de preuve ;

- L'effet « plumeau », c'est-à-dire un déplacement de la délinquance des zones sous vidéoprotection vers les zones non couvertes, ne semble pas avéré, tant au regard des témoignages reçus des responsables de la police et de la gendarmerie nationales, qu'à la lumière des chiffres de la délinquance qui ne montrent pas de dérives vers les zones non vidéoprotégées, au sein des circonscriptions de police ou des brigades de gendarmerie qui disposent de vidéoprotection ;

Evolution de la délinquance comparée entre villes vidéoprotéges et non vidéoprotégées

	Délinquance générale	Délinquance de proximité	Atteintes aux biens	AVIP
Zone Police				
Total France métropole villes non équipées période 2000-2008	-6,9%	-27,2%	-20,6%	+40,5%
Echantillon 49 CSP équipées de vidéoprotection	-13,5%	-31,2%	-26,9%	+24,1%
Zone Gendarmerie				
Evolution totale France métropole période 2000 -2008	+6,5%	-20,1%	-7%	+64,7%
63 communes en zone gendarmerie équipées de vidéoprotection	-11,8%	-34,2%	-21,3%	+27%

4. Un arrêté technique remarqué par de nombreux pays :

Deux années après les attentats de Londres, les autorités publiques françaises ont mis en œuvre en 2007, [*en tenant compte de l'évolution technologique des*

systèmes et des menaces terroristes ou criminelles], un arrêté technique, qui exprime ce que doivent posséder en qualitatif et à minima les systèmes de vidéoprotection sur l'ensemble du territoire national. La création de cet arrêté technique représente une première au niveau mondial sur la qualité des matériels, et donnera naissance à la mise en œuvre d'une norme ISO 501132 [largement inspirée du texte français].

L'arrêté définit entre autre :

Prise d'image	doit être adaptée à l'environnement,
Transmission	doit permettre l'acheminement des images depuis la caméra vers l'unité de stockage et/ou de visualisation,
Enregistrement des images	doit garantir une qualité minimale des images enregistrées et la traçabilité de certaines actions,
Exportation	doit permettre aux services de police et de gendarmerie de relire les vidéos sans dégradation de qualité,
Cohérence globale	le système de vidéosurveillance doit permettre de répondre aux finalités pour lesquelles il a été mis en place.

En matière de « sécurité des réseaux », l'arrêté pose des principes sur la prise en compte des critères d'intégrité, de confidentialité et de disponibilité que la sécurité des réseaux doit apporter aux flux vidéo transportés mais il n'impose pas de certificats formels ni de chiffrement systématique du flux.

La locution "garantie d'intégrité" ne doit donc pas être comprise comme "absolue garantie d'intégrité, …", notion qui dans certains contextes n'a pas de sens puisqu'elle ne peut être mise en œuvre. L'arrêté ne fixe donc pas un niveau de sécurité générique pour ces trois critères.

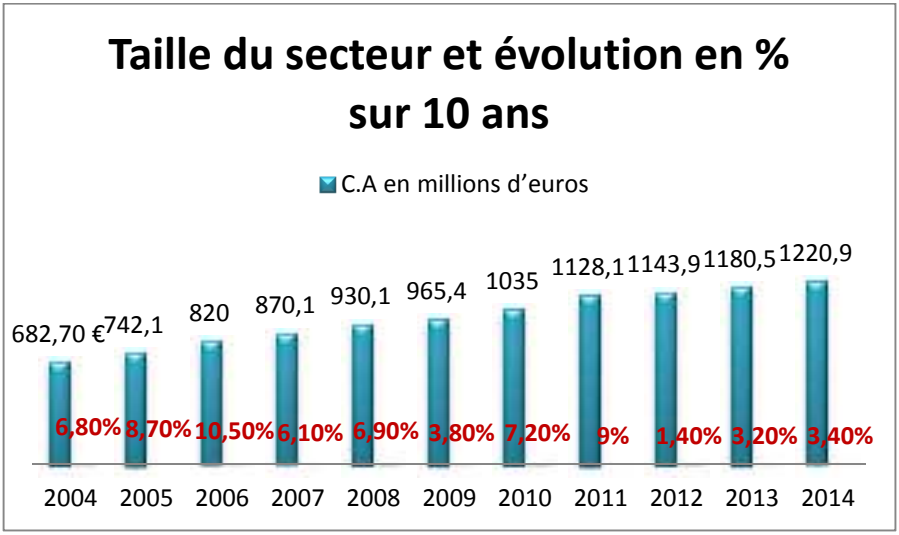
Les solutions techniques qui permettent d'adresser le niveau d'exigence pour ces 3 critères [*Intégrité, Confidentialité, Disponibilité*] dépendent du système et du contexte d'installation. Ainsi, dans les établissements ouverts au public, lorsque les liaisons entre les caméras et les systèmes d'enregistrement sont dédiées et protégées mécaniquement sur les tronçons vulnérables (notamment les tronçons terminaux), la simple sécurisation des matériels d'enregistrement dans des locaux fermés à clé peut être considérée comme suffisante. Si un renvoi

d'images à distance (hors site) est effectué pour l'exploitation, il faudra également prendre en compte ces 3 critères pour cette transmission hors site.

La disponibilité pourra être assurée par exemple par un temps de rétablissement compatible avec les objectifs fixés, par des tests réguliers de la capacité de transmission des flux vidéo...

Le marché de la vidéoprotection en France :

Entre 1996 et 2004, le chiffre d'affaires du secteur s'accroît de 111 %, évoluant de 360 millions à plus de 750 M€ pour atteindre plus d'1 Md€ depuis le début de la décennie 2010.



En toute sécurité – ATLAS 2014

	C.A en millions d'euros	Evolution en % sur 10 ans
2004	682.7	+ 6.8%
2005	742.1	+ 8.7%
2006	820	+ 10.5%
2007	870.1	+6.1%
2008	930.1	+6.9%
2009	965.4	+3.8%
2010	1035	+7.2%
2011	1128.1	+9%
2012	1143.9	+1.4%
2013	1180.5	+3.2%
2014	**1220.9**	**+3.4%**

La majorité des caméras se situe dans des lieux clos, qu'ils soient privatifs ou ouverts au public, d'où la complication d'estimer avec exactitude, le nombre d'installations existantes [Aucune nécessité de déclaration en préfecture]. Afin d'illustrer cette difficulté de recensement on relèvera que selon le ministère de l'intérieur sur les 350 000 caméras comptabilisées en 2006 en France, une vingtaine de milliers concerne la voie publique contre 75 000 dans les transports en commun [*INHESJ – Politiques publiques de vidéoprotection – Groupe de diagnostic – Travaux des auditeurs 2013-2014*].

Cette distorsion d'information publique démontre la grande difficulté à quantifier avec précision la taille du parc de vidéoprotection métropolitain. [*Chapitre VI Le développement de la vidéosurveillance - L'ORGANISATION ET LA GESTION DES FORCES DE SECURITE PUBLIQUE - Rapport public thématique de la Cour des Comptes – 2011].*

Malgré les restrictions budgétaires durant la période 2009 – 2012 [impact de la crise économique], le secteur retrouve un dynamisme en raison de l'arrivée de technologies plus sophistiquées [solutions IP]. Les analystes marchés spécialisés estiment que la croissance va de nouveau connaître une accélération mesurée, au cours des prochaines années.

5. Et à l'international ?

Dans une étude publiée en 2012 par le cabinet IMS Research, le marché mondial des équipements de vidéo-surveillance affiche, une forte croissance malgré les effets de la crise de la dette enregistrée en zone euro. Cette croissance serait portée par les BRIC (Brésil, Russie, Inde et Chine) qui représenteraient 30 % du marché actuel et quelque 40 % du marché en 2016. À titre d'exemple, depuis les attaques terroristes subies à Mumbai en 2008, la surveillance des villes est devenue une priorité pour l'Inde, avec des projets d'envergure corrélés à l'étendue des zones couvertes.

Le renouvellement d'un parc vieillissant ou l'utilisation de la vidéoprotection à des fins autres que sécuritaires, semble se mettre en œuvre dans les grandes villes. A titre de comparaison, Paris avec 2000 caméras recensées en 2013 semble loin du développement de sa consœur au Royaume Uni qui dispose de 5.000 unités. Le groupe Thalès a gagné en 2014 un appel d'offre en vue d'équiper la ville de Mexico [Métropole de 20 millions d'âmes] pour la mise en œuvre d'un projet monumental d'équipement de 8.000 caméras. Celui-ci s'inscrit dans une démarche innovante englobant les objectifs sécuritaires mais également de nombreux points liés au développement durable, la complémentarité et l'avancée technologique vont permettre aux systèmes vidéo de franchir de nouvelles étapes.

6. Le financement de la vidéoprotection par l'Etat :

L'article 5 de la loi n° 2007-297 du 5 mars 2007 prévoit que le fonds interministériel pour la prévention de la délinquance est destiné à financer la réalisation d'actions dans le cadre des plans de prévention de la délinquance et dans le cadre de la contractualisation mise en œuvre entre l'État et les collectivités territoriales en matière de politique de la ville.

Les dépenses de vidéoprotection des communes sont éligibles aux dotations du fonds interministériel pour la prévention de la délinquance (FIPD), dans le cadre des orientations fixées par le secrétariat général du Comité interministériel de prévention de la délinquance (SGCIPD). La participation de l'État contribue aux frais d'installation de dispositifs de vidéoprotection ou d'extension de dispositifs existants. Elle peut aller, jusqu'à une prise en charge totale du raccordement du centre de supervision d'une ville à un service de police ou de gendarmerie. Les dossiers pour lesquels une participation de l'État est demandée doivent être déposés auprès du préfet du département concerné et présenter un intérêt opérationnel en matière de lutte contre la délinquance. Les installations,

extensions ou raccordements envisagés doivent s'insérer par ailleurs dans le cadre plus global des dispositifs de lutte contre l'insécurité.

En 2007, la vidéoprotection a été l'une des principales sources d'emploi des crédits du fonds interministériel de prévention de la délinquance. 309 projets ont été financés dans 75 départements (y compris les 4 DOM) pour un montant total de 13,4 MEUR représentant 30 % environ des crédits engagés sur le FIPD au cours de cette année.

Les communes ont représenté 82 % des porteurs de projet, loin devant les EPCI *[Etablissements Publics de Coopération Intercommunale]* (9 %), les organismes HLM (5,5 %) et les sociétés de transports publics (1,5 %). Pour 2008, la participation de l'État à ce type de dépenses a revêtu de nouveau un caractère prioritaire.

Subvention sécurité des débitants de tabac :

Depuis le 1er janvier 2012 et conformément au Décret 2012- 1448 relatif à l'aide à la sécurité des débits de tabac. Une aide spécifique est accordée aux débitants gérant un débit de tabac ordinaire ou spécial, pour financer un audit de sécurité du local commercial, ou pour acquérir et installer des matériels, des équipements ou un système de protection destinés à sécuriser :

- le local commercial où le débit de tabac est exploité ;
- la réserve où le tabac est stocké ;

La subvention sécurité est accordée par le directeur interrégional des douanes et droits indirects territorialement compétent au vu des pièces et informations requises et notamment des deux devis détaillés émanant de deux entreprises concurrentes, par nature de travaux. Il détermine le montant de l'aide en fonction du devis sur lequel figure l'offre économiquement la plus avantageuse au regard du prix, même si le demandeur retient un autre devis. La subvention sécurité est égale à 80 % du coût hors taxes des matériels et de leur installation concernant la sécurité des débits de tabac, tel que retenu par le directeur interrégional des douanes et droits indirects et, le cas échéant, à 50 % du coût hors taxes de l'étude de sécurité, avec un plafond de 15 000 €. Cette subvention est accordée tous les trois ans mais, dans la mesure où le plafond n'est pas atteint, plusieurs compléments peuvent être autorisés pendant la période triennale.

Les *matériels subventionnés sont :*

1) Les coffres forts ;

2) Les serrures, cylindres et verrous, les portes blindées et les blocs-portes anti-effraction ;

3) Les vitres anti-effraction ;

4) Les systèmes d'alarmes notamment ceux pouvant intégrer un générateur de brouillard ;

5) Les rideaux métalliques ou les grilles métalliques ;

6) Les balises de radiolocalisation par GPS;

7) Les barreaux en acier ;

8) Les bornes et murets devant la ou les entrées du local commercial contribuant à en empêcher l'intrusion ;

9) Les systèmes de vidéosurveillance ;

Le FISAC, aide directe aux entreprises sur les équipements destinés à assurer la sécurité des entreprises commerciales :

Il est à noter que les pharmacies sont exclues du dispositif. Le dispositif FISAC est mobilisable par les collectivités territoriales, leurs groupements ou leurs établissements publics, les CCI [Chambre de Commerce et d'Industrie], les CMA [Chambre des métiers et de l'artisanat] ou une SEM [Société d'Economie Mixte], pour un ensemble d'entreprises appartenant à un secteur géographique. Il intervient notamment dans le cadre d'opération urbaine, (Exemple : requalification d'un petit centre commercial, dans un programme de rénovation urbaine – PRU-) et porte sur des actions collectives et individuelles. Le FISAC peut prendre en charge une partie des dépenses de fonctionnement et d'investissement, à l'exception des aménagements urbains (circulaire du 21/04/12), pour la réalisation de ces actions. Le FISAC vise les dépenses d'un montant minimum de 10 000€.

Le FISAC prévoit un taux maximum de financement de 40 % des dépenses de travaux, dans un maximum subventionnable limité à 75 000 € HT, ce qui correspond à un montant de subvention de 30 000 €. La participation financière de la collectivité concernée doit être égale à celle du FISAC. Cependant, dans les territoires prioritaires d'un contrat urbain de cohésion sociale (CUCS), il n'y a pas d'obligation de concours financier de la ville. Le FISAC peut se cumuler avec d'autres financements publics dans la limite de 80 % du coût global H.T de l'opération visée.

FISAC : AIDES DIRECTES AUX ENTREPRISES	
Dépenses d'investissement éligibles	
• **Rénovation de vitrines.** • **Équipements destinés à assurer la sécurité des entreprises.**	**Conditions :** - La participation financière de la collectivité concernée doit être égale à celle du FISAC sauf dans les ZUS et les territoires prioritaires d'un CUCS. - Le chiffre d'affaires annuel de l'entreprise doit être inférieur à 1 000 000 € HT. - L'aide du FISAC est plafonnée à 10 000 € par entreprise

7. La vidéoprotection, est-elle un marché restreint :

Certification SVDI – Bureau Veritas	Certification AFNOR – CNPP

http://www.interieur.gouv.fr/Videoprotection/La-certification-des-installateurs

Pour ouvrir un salon de coiffure, il est demandé un C.A.P de coiffure, cette image peut sembler absurde d'évidence, et représente à juste titre l'idée communément admise que l'exercice d'une profession doit s'accompagner d'une justification professionnelle spécifique. A l'inverse et durant ces deux décennies, n'importe qui ou presque pouvait se prévaloir comme spécialiste de la vidéosurveillance. Si le marché public a été plus ou moins préservé par la venue massive de gens intéressés par ce nouveau marché ; nombreux sont les commerces ou entreprises à avoir été victimes de pseudos professionnels ayant vendu des systèmes de mauvaise qualité ou ne répondant en rien à l'expression des besoins initiale du donneur d'ordre.

Les autorités publiques, devant ce constat d'inefficacité et afin de promouvoir une culture professionnelle valorisante, ont mis en place à travers, l'arrêté du 5 janvier 2011, un modus vivendi qui fixe les conditions de certification des installateurs de systèmes de vidéosurveillance. Il définit le référentiel composé des exigences minimales à respecter par un installateur de systèmes de

vidéosurveillance ainsi que des procédures de vérification que devra suivre un organisme certificateur pour vérifier que ces exigences sont satisfaites et délivrer le cas échéant un certificat reconnu par les préfectures.

Rappel des exigences minimales à respecter par les installateurs :

- L'installateur doit connaître et comprendre les exigences réglementaires de l'administration sur la vidéoprotection (Loi no 95-73, décret no 2008-1401 et l'arrêté d'exigences techniques du 3 août 2007), et également être informé des principales réglementations administratives du domaine général (législation du travail, directive sur les déchets...).
- L'installateur doit s'engager à effectuer avant toute installation un devis qui supporte des matériels et une prestation conformes aux exigences techniques de l'arrêté du 3 août 2007. Le devis de l'installateur doit comporter un descriptif technique, permettant notamment au maître d'ouvrage de justifier par lui-même la conformité de l'installation envisagée à ces mêmes exigences techniques.
- L'installateur doit disposer de la compétence technique pour conseiller utilement le maître d'ouvrage dans la mise en place des caméras.
- L'installateur doit proposer au client une installation au meilleur rapport qualité/prix, sans imposer des matériels ou installations pouvant conduire à des surcoûts injustifiés.
- L'installateur doit disposer de personnels qualifiés sur la base de formations dans le domaine (vidéo, transmission IP, stockage...) ou justifiant d'au moins deux années d'expérience.
- L'installateur doit proposer une procédure de recette technique des installations, assurer au minimum le délai légal de garantie et proposer un contrat de maintenance au maître d'ouvrage (ce dernier n'étant pas tenu de l'accepter). Il doit être en mesure de fournir des pièces de rechange à la demande du client.
- L'installateur doit remettre au maître d'ouvrage un procès-verbal de réception des installations.
- L'installateur doit préciser par écrit au maître d'ouvrage quelles sont les actions d'exploitation et de maintenance nécessaires au bon fonctionnement du système.

Avant la délivrance d'une certification à un installateur

- La demande de l'installateur doit spécifier qu'il est candidat à la certification suivant le présent référentiel.
- L'organisme certificateur doit effectuer une visite préalable d'au moins une demi-journée chez l'installateur, pour vérifier le respect des exigences.
- L'organisme certificateur, doit s'assurer, par questionnaire ou entretien, que les connaissances des personnels leur permettent de réaliser des installations conformes aux exigences.
- L'organisme certificateur, doit visiter au moins une installation réalisée chez un client.
- Le certificat délivré doit explicitement mentionner que la certification est délivrée en application du présent arrêté, qui inclut les exigences techniques de l'arrêté du 3 août 2007.

Surveillance de l'installateur :

- L'organisme certificateur, s'assure par sondage auprès des maîtres d'ouvrage clients que les exigences et les engagements de l'installateur sont bien respectés.
- L'organisme certificateur, met en place une procédure de contrôle de la compétence de l'installateur et de la conformité de ses engagements et installations qui tient compte du nombre d'installations faites par l'entreprise sur l'ensemble de la France mais comporte au minimum deux visites d'une demi-journée tous les deux ans chez l'installateur ou chez certains de ses clients (avec un minimum d'une visite tous les quatre ans chez l'installateur et un minimum d'une visite tous les deux ans chez les clients).
- L'organisme certificateur doit avoir le choix des clients qu'il souhaite contrôler (dès lors qu'il contrôle des installations sur des lieux recevant du public et que la confidentialité du fichier client de l'installateur est préservée).

En cas d'installations manifestement défectueuses ou non conformes à la réglementation détectées suite à des plaintes ou lors des visites de sondage, l'organisme certificateur doit adresser une mise en demeure à l'installateur. Si cette mise en demeure n'est pas suivie d'effet, l'organisme peut suspendre ou retirer sa certification à un installateur. Il doit alors en avertir le ministère de l'intérieur.

8. Les nouvelles technologies en vidéoprotection

La vidéoprotection est un marché en constante effervescence : Automatisation, interopérabilité, intelligence, mémoire, HD, explosion de l'IP. Toutes ces innovations entrainent l'obsolescence et le remplacement de la technologie analogique [toutefois encore ancrée dans les petites structures privées ou publiques]. L'informatique ainsi que la sécurisation des données investissent le champ de la vidéoprotection, bouleversent toutes les filières métiers et imposeront à terme de profonds changements pour les techniciens et installateurs, comme pour les donneurs d'ordres. Dans les grosses structures, c'est bien souvent le Responsable Sécurité Informatique qui gère en grande partie la vidéoprotection, lorsqu'elle n'est pas directement intégrée dans un ensemble plus vaste de systèmes d'information ou de communication, voire dans les systèmes de Gestion Technique du bâtiment.

Qu'est-ce que la Vidéoprotection intelligente … [Détecter, pister, analyser]

Capacité de pré-événement, le temps de la vidéosurveillance basique semble rangé au rayon moyen-âge. Désormais, la vidéo intelligente est capable de mesurer dans le champ de vision, quelque chose bouge, la caméra l'a repéré… oui, mais en fonction de quoi ? La détection d'un mouvement est conditionnée par la présence de plusieurs critères :

1. La variation proportionnelle au sein de l'image.
2. La variation colorimétrique par rapport à l'image de référence.
3. L'analyse de la rapidité de déplacement de l'ensemble volume/couleur.

On peut en déduire, que dès que la caméra a détecté un objet d'une certaine proportion et constaté une variation colorimétrique dans l'image, elle analyse que cet ensemble se déplace à une certaine célérité. Ces trois conditions doivent être concurremment réunies pour garantir une détection.

En conséquence, après l'avoir repéré et identifié, la caméra peut suivre l'objet dans son mouvement et, si besoin, déclencher une alarme si l'objet en question est entré dans une zone d'intérêt. Une autre fonction intéressante est le tracking vidéo qui est une fonctionnalité aujourd'hui couramment répandue dans les solutions de vidéosurveillance intelligente. La détection d'un individu ou d'un objet en mouvement conduit à l'analyse des informations enregistrées par la caméra.

En effet, un système doté de fonctionnalités de détection et de pistage en temps réel doit également se démontrer capable de « qualifier » un événement

pour fournir une information la plus pertinente possible. Les fonctionnalités sont alors variées :

- déclenchement d'alarmes anti-intrusion,
- comptage,
- mesure,
- ou enlevés…

L'ensemble automatique de trafic, détection d'immobilité, de contre-sens ou d'unicité de passage dans un sas, d'objets déposés de ces fonctions existe et fournit des réponses proportionnellement fiables, [pour certaines d'entre elles, il reste cependant de nombreuses améliorations à mettre en œuvre pour les rendre efficientes qualitativement].

Quels sont les avantages de l'analyse intelligente de la vidéo

Les caméras raccordées [souvent HD] à des logiciels, sont devenues intelligentes. Cette construction permet ainsi de seconder avec efficience les opérateurs afin de prendre des décisions rapides [plusieurs études ont démontré que l'attention des individus chute sous un niveau acceptable après seulement 20 minutes à regarder et analyser des écrans de surveillance vidéo. Or, si la vidéo-surveillance intelligente ne fournit pas encore de systèmes totalement autonomes, elle assiste les vidéo opérateurs en leur apportant des informations cruciales]. Pour réaliser des investigations performantes afin d'enclencher des interventions ciblées tout en augmentant les effets visuels qualitatifs [Ex : de donner une alerte d'un véhicule roulant à contre sens, de signaler un mouvement de foule ou bien de réaliser du comptage]. Elles sont aussi en mesure de faire de la recherche contextuelle d'événements passés permettant par exemple d'identifier un individu avec un pull d'une couleur donnée ou bien portant un chapeau, d'identifier la disparition d'un objet ..., les paramétrages sont infinis! Elle réduit également la bande passante et l'espace d'archivage nécessaires en ne transmettant ou n'enregistrant que les données relatives aux informations pertinentes.

9. L'interopérabilité des technologies de vidéoprotection :

Une installation de vidéoprotection de nouvelle génération est un système complexe, mélangeant de nombreuses technologies, et qui ont pour seul dénominateur commun le réseau IP. Les protocoles de communication entre la gestion des métadonnées, les équipements périphériques, les caméras et les algorithmes de compression sont la propriété des différents constructeurs.

La technologie évolue vite. In fine, on se retrouve face à une complexification des cahiers des charges et face à des clients qui expriment des besoins, sans nécessairement en avoir mesuré le ratio objectif / finalité.

La réalité opérationnelle sur le terrain démontre la difficulté de déployer un système de vidéoprotection, avec un unique fournisseur en mesure de répondre à tous les besoins. Cela se complexifie d'autant plus, qu'il faut prendre en compte l'évolutivité et le développement rapide de la recherche et développement des constructeurs. L'intégrateur comme l'utilisateur pourra être confronté en définitive avec un problème de compatibilité entre les différents composants de son système.

Quels sont les avantages de l'interopérabilité

Utilisateurs	- Plus grande indépendance dans le choix des solutions - Amortissement et pérennité des investissements
Installateurs, intégrateurs et bureaux d'études	- Plus grande indépendance dans le choix des équipements - Simplification dans l'installation des équipements [compatibilité]
Editeurs et constructeurs	- Opportunités de marchés renouvelés ou développement à l'étranger - Réduction des coûts de recherche et de développement - Réduction des coûts d'intégration

Plusieurs initiatives sont en développement constant, afin de promouvoir l'interopérabilité, mais il est à noter qu'aucune de celles-ci ne domine suffisamment les technologies de vidéoprotection, pour s'imposer.

AFNOR en collaboration avec l'iso	Norme ISO 22311
ONVIF [forum industriel 500 membres]	Développe des standards et spécifications [environ 900 produits conformes]
PSIA [consortium 65 constructeurs]	Organisme concurrent d'ONVIF [environ 200 produits conformes]

Une interopérabilité garantie par la compatibilité à une norme n'est donc pas pour les utilisateurs, bureaux d'études et installateurs, éditeurs et constructeurs dans l'immédiat, alors que les besoins comme les marchés mutent rapidement. Si tous les acteurs conviennent de l'intérêt de l'interopérabilité des systèmes,

certains constructeurs ont encore des résistances et continuent à valoriser les systèmes propriétaires. Paradoxalement pour certains clients, il peut être aussi confortable de s'orienter avec un seul constructeur. Une licence propriétaire peut présenter un gage de sécurité non négligeable. Un arbitrage parfois difficile et au cas par cas, en fonction des objectifs et des attentes du client final.

Perception situationnelle « Physical Security Information Management System » :

L'emploi de systèmes en réseau permet leur communication pour des applications intégrées et convergentes. Le champ des possibles apparait alors sans limite, la vidéoprotection se combine avec d'autres technologies de sécurité électronique :

- Boutons anti agression dans les agences bancaires, déclenchant le pré-événement des caméras,
- Aide à la levée de doute assistée pour les agents de sécurité en cas de détection intrusion sur un grand site industriel, pourquoi pas en assistance suite à une alarme incendie,
- Intégration dans un mur d'image interactif avec des cartes géographiques vectorielles, ou des plans en trois dimensions équipées de vignettes actives,
- Suivi d'un employé dans une zone à risque, équipé de dispositif « protection du travailleur isolé géolocalisable ».

Au-delà des notions d'hypervision déjà connues par le grand public, les systèmes PSIM *[Physical Security Information Management System]*, incorporent un ensemble de systèmes mixtes, de sûreté, sécurité, maintenance et de gestion bâtimentaire dans une seule interface globalisée. Ils permettent de gérer un nombre conséquent de données plurielles et de les présenter à l'opérateur dans une synthèse tenant compte du contexte situationnel. Seules, les données pertinentes sont affichées, ce qui représente une valeur ajoutée pour l'opérateur dont l'aide à la décision est améliorée et qui accroit la réactivité des actions des équipes face à une situation de crise ou d'urgence, mieux les PSIM peuvent être pré-paramétrés pour répondre à des scénarii tenant compte de l'analyse des risques et des menaces du client. Avec les PSIM, la notion de « vidéoprotection » est démontrée. Asservie avec d'autres équipements, elle devient un outil contribuant à valoriser les fonctions sûreté et sécurité dans l'entreprise.

10. Sécurité des systèmes d'information et vidéoprotection :

L'arrivée massive des nouvelles technologies et des logiciels informatiques dans les systèmes de vidéoprotection, pose une problématique inédite à l'ensemble des acteurs. Quelle intégrité pour mon système au vu des menaces représentées par les « pirates » qui peuvent agir seuls, ou sur commande en sous-traitance de la criminalité organisée, voire des terroriste ! Le sabotage, la captation d'information sont des impacts malveillants qui revêtent une prise en compte nouvelle et pose pour l'ensemble des acteurs, la mise en œuvre d'une stratégie dans toutes les fonctions et les couches métiers : quel degré de sensibilisation devra être donné, quel niveau d'information devra être transmis, quelle nouvelle formation ou compétence acquérir. C'est un nouveau défi qui viendra se poser pour la profession, peut-être même l'intégration de nouveaux collaborateurs issus de la sécurité informatique, ou des experts en gestion des risques capables d'interagir avec les équipes de techniciens. Les innovations technologiques et la recherche et développement chez le fabricant sont un enjeu déjà pris en compte sur les produits [caméra disposant de sa propre clé de cryptage], sécurisation du wifi ou du fournisseur d'accès, des protocoles de communication, du stockage virtualisé dans les nuages [cloud computing].

Quels critères pour définir la Sécurité des données :

Le Ministère de la Défense, dans son Instruction Générale Interministérielle N°1300 du 23 juillet 2010, apporte les éléments de réponse suivants :

INTEGRITE	Est la propriété assurant qu'une information ou un traitement n'a pas été modifié, ou détruit de façon non autorisée.
CONFIDENTIALITE	Est le caractère réservé d'une information ou d'un traitement dont l'accès est limité aux seules personnes admises à la connaître pour les besoins du service, ou aux entités ou processus autorisés, on appelle cela le « besoin d'en connaître ».
TRACABILITE	Est l'aptitude à retrouver l'historique, l'utilisation, la localisation d'un produit ou d'une activité au moyen d'informations enregistrées.

Ces trois niveaux définissent la sécurité des systèmes d'informations et sont déjà connus des prescripteurs informatiques comme des acteurs de la sécurité dans les entreprises. Les constructeurs sont déjà équipés d'ingénieurs capables de réfléchir voire d'implémenter leurs nouveaux produits.

A l'heure actuelle, aucune obligation ne définit la sécurité du système d'information dans le domaine de la vidéoprotection. Des prescriptions viendront probablement apporter des réponses aux attentes des professionnels pour l'année 2016. En effet le Ministère de l'Intérieur par le biais de l'adjointe au délégué aux coopérations de sécurité chargée de la vidéoprotection et son groupe de travail élaborent en ce moment un document afin de tenir compte de l'évolution des règles de l'art et des technologies dans le domaine de la vidéoprotection en complément de l'arrêté technique du 3 aout 2007.

Dans l'attente d'une réponse formalisée par les pouvoirs publics, que peut faire l'intégrateur, lorsqu'il est confronté à une demande spécifique de la part d'un donneur d'ordre dans le domaine de la sécurité des transmissions en vidéoprotection dans un CCTP formalisé ?

Nous ne pouvons que conseiller au responsable du bureau d'étude ou au responsable technique de l'entreprise, la prise en compte des éléments développés par la mission pour le développement de la vidéoprotection et de sa fiche sortie en 2013. Celle-ci aborde des éléments de réponse techniquement concrets qui permettront de répondre aux exigences des RSSI (Responsable des systèmes de sécurité de l'information) des entreprises publiques et privées.

11. Synthèse de la note :

www.interieur.gouv.fr/.../file/Fiche%20SécuritéV3%20mars2013-2.pdf	
Introduction sur les nouvelles menaces	• *Comprendre les risques sur les réseaux de vidéoprotection eux-mêmes* • *Comprendre les risques induits sur d'autres systèmes*
Analyse	• *Considérations générales sur le schéma de réseau* • *Recommandations de l'ANSSI* - *Cas des réseaux de voie publique* - *Utilisation des liaisons Wifi* - *Architecture novatrice avec enregistrement dans la caméra* - *Aspects organisationnels des liaisons permanentes …*

La tentation du stockage dématérialisé

Durant la période de commercialisation de l'analogique, la sécurisation du système de vidéoprotection concernait surtout des aspects de « protection physique » [contrôle d'accès du local d'enregistrement et de paramétrage, protection du câblage], tel que défini dans l'arrêté technique du 3 aout 2007.

Avec la montée en puissance de l'IP, la doctrine évolue afin de tenir compte de tous les événements redoutés et palier autant que faire se peut aux failles de sécurité des réseaux informatiques et aux actes cybercriminels, on parle là de « protection logique », la sécurisation est plus compliquée qu'avec l'ancienne technologie. En effet, pour les réseaux IP disposant d'une partie sans fil, la moindre porte d'entrée sur le réseau qui aura été négligée sera une faille béante à la merci des délinquants informatiques. Pire en remontant le réseau IP du système de vidéoprotection, c'est la totalité du système d'information de l'entreprise qui se trouve vulnérable, compromis, voire en passe d'être totalement neutralisé.

Les matériels eux même, comme les caméras ou les câblages sont susceptibles de produire à distance un rayonnement qui peut être capté [le transport de l'IP sur câble coaxial, devient ainsi une véritable antenne], cela représente un événement redouté de plus à prendre en compte dans l'analyse des risques. Une criticité forte avec une probabilité faible, concerne dès lors les opérateurs des sites les plus sensibles, les plus prudents d'entre eux sur l'utilisation de cette technologie IP, mixent celles-ci, afin de garantir une stratégie de sécurisation des sites optimale ; [Ex : caméras IP pour le périmètre intérieur, analogique pour l'extérieur ou sur les sites jugés ultra vulnérables, en les liant par exemple avec des encodeurs à l'intérieur des bâtiments].

Pour un certain nombre de D.S.I [Directeurs de Sécurité Informatique], les systèmes de vidéoprotection apparaissent comme une application informatique similaire aux autres composantes du système d'information, s'intégrant comme un CRM [logiciel de Gestion de la Relation Client], un ERP [logiciel de gestion intégré], au sein d'une GTC [Gestion Technique Centralisée]. Elle repose en règle générale sur les standards H264 pour la vidéo, protocole LDAP, protocole IP, et nécessite une infrastructure disponible H24 et 7/7 avec une capacité de stockage souple et capable d'enregistrer une volumétrie de données conséquente provenant des caméras. Les systèmes de vidéoprotection sont gérés dans les grands groupes ou grandes administrations, comme un projet IT afin d'intégrer ceux-ci dans une démarche de gestion des coûts globalisée, pour faciliter l'utilisation des opérateurs et par strate jusqu'au management des S.I, sans oublier une tendance prégnante et stratégique incontournable que sont

les objectifs de développement soutenable [ces objectifs se retrouvent de plus en plus souvent dans les cahiers des charges des clients].

Les caméras IP HD [haute définition] engendrent des flux vidéos importants que les infrastructures réseaux et de stockages doivent porter. La caméra numérique nécessite entre 4 et 10 mégabites / seconde. Un flux 24 images par seconde nécessite en moyenne un flux réseau de 1,3 gigabits / seconde. L'infrastructure de stockage ne doit jamais être arrêtée, [même si un nombre considérable de données sera jugé obsolètes très vite], le taux de fiabilité impose une obligation de résultat voisinant les 100% avec un objectif de stockage avant écrasement qui est porté à 15 jours [mensuelle dans l'arrêté technique du 3 aout 2007] pour de gros systèmes vidéo. Les unités de stockages [ainsi que les locaux adaptés et sécurisés] peuvent engendrer des budgets de fonctionnement voire de maintenance lourds et inadaptés pour des structures déjà adeptes de la virtualisation des données.

Tous ces éléments indiquent que la dématérialisation et/ou virtualisation des données constituent une étape pour certains une révolution qui rendra probablement obsolète, tous les autres supports externes de stockage,[sous réserve de voir les sites de serveurs géants (datacenters), physiquement présents en France et en Europe ; Des programmes de développement sont actuellement à l'étude pour favoriser leurs implantations et notamment repris dans les plans de confiance numérique ou des futurs labels gouvernementaux voire européens de cyber sécurité].

Vous souhaitez en savoir plus :

Problématiques de sécurité associées à la virtualisation des systèmes d'information	http://www.ssi.gouv.fr/uploads/IMG/pdf/NP_Virtualisation_NoteTech_v1-1.pdf
Recommandation de sécurité pour la mise en œuvre de dispositifs de vidéoprotection	http://www.ssi.gouv.fr/uploads/IMG/pdf/videoprotection_notetechnique_anssi.pdf

12. La nécessaire prise en compte de la reconnaissance professionnelle des intégrateurs en vidéoprotection

Le monde de la sécurité privée a depuis 1983 effectué un travail laborieux de reconnaissance par les pouvoirs publics afin de démontrer le professionnalisme de ses acteurs et faire reconnaitre la valeur de son éthique [dirigeants et employés]. L'urgence de l'époque était d'assainir une profession souvent confrontée à un déficit de réputation et d'image dans des affaires médiatisées qui avaient abimé auprès du grand public l'ensemble de ses métiers.

30 années plus tard, confrontés aux menaces et crises protéiformes [délinquance, criminelles, terroristes, économiques], au développement exponentiel, les pouvoirs publics ne pouvant pas répondre à l'urgence considérable de la protection de l'ensemble des infrastructures privées présentes dans les pays a dû faire le choix de l'arbitrage en se concentrant sur ses missions régaliennes aux impératifs stratégiques majeurs. L'opportunité et le pragmatisme politique ont transformé l'essai, en intégrant les acteurs de la sécurité privée comme partenaire contributeur à la sécurité intérieure du pays. Les textes régissant la profession ont été intégralement admis [avec des modifications tenant compte de l'évolution des règles de l'art] dans le Code de Sécurité Intérieure [livre 6]. Une petite révolution car la profession se trouve sous responsabilité d'un préfet. L'embauche de ces employés ou la création de sociétés pour les dirigeants soumises au contrôle d'un organisme ayant pouvoir de Police Administrative, et régit sous contrainte d'un Code de Déontologie drastique empêchent la moindre dérive. Entrer dans la profession est soumis à une enquête préalable et à l'attribution d'une Carte Professionnelle justifiant de la probité de l'employé.

Toute la profession ? Hélas, les acteurs de la sécurité électronique ne sont pas concernés. Nous avons vu dans le développement de ce dossier l'importance prise par le respect de la Confidentialité, de l'Intégrité, et de la Sécurité de l'information pour ce qui concerne le matériel. Quelle dichotomie en fait pour ne pas dire schizophrénie … On s'interroge sur le niveau de sécurité logique à apporter au matériel, mais pas sur les acteurs qui possèdent les plans, les schémas techniques, les mots de passe, les clefs ou les badges des sites des donneurs d'ordres.

Cible potentielle demain des malveillants qui y verront une faille humaine à exploiter, ou malveillance interne d'un employé mécontent de son sort, voire infiltration ou parasitisme d'une organisation criminelle ou terroriste dans les capitaux des entreprises, osera-t-on évoquer à voix basse le risque de radicalisation d'un salarié [l'épouvantable tentative d'attentat en Isère en avril 2015 par pénétration du site et utilisation d'un véhicule bélier contre les bouteilles de gaz stockées à l'extérieur du périmètre et la décapitation du dirigeant de l'entreprise sous-traitante reste dans toutes les mémoires]. Ne pas intégrer cette réflexion dans une logique d'analyse de gestion des risques globaux, pose un problème de fond.

C'est le combat mené par Philippe BLIN, Président de SVDI qui pressentant ces risques a souhaité que notre organisation intègre l'ANAPS et œuvre auprès des instances professionnelles comme des représentants des autorités publiques afin que les intégrateurs en vidéoprotection et les acteurs de la sécurité

électronique, soient reconnus dans ce Code de Sécurité Intérieure, et puisse bénéficier de cette reconnaissance partenariale et de la carte professionnelle. Le temps est venu de solidifier tous les maillons de la chaîne sécuritaire [si l'un de ces maillons reste vulnérable, c'est l'ensemble qui reste poreux et donc fragilisé]. Il est temps de donner corps de manière empirique au concept de sécurité globale.

5 rue de l'Amiral Hamelin - 75116 PARIS
Tél: 01.44.05.84.40
Nous contacter : l.caule@svdi.fr
www.svdi.fr