

LIVRE BLANC

Télévidéosurveillance

Un nouvel horizon pour la sécurité globale. La maturité à tous prix ?



USP TECHNOLOGIES

LIVRE BLANC - 2014

"Télévidéosurveillance"

SOMMAIRE

Préambule 8

Le mot du Président de l'USP 8

Le mot du Président de l'USP-Technologies 9

Quels sont les objectifs de la télévidéosurveillance ? 10

Quelle est la nature des lieux traités ? 11

Évolution du métier 12

1 GT N°1 – Qualification des risques 13

1.1 Constitution du GT N°1 13

1.2 Préambule 13

1.3 La malveillance 13

1.3.1 Les agressions verbales, les incivilités 13

1.3.2 Les agressions physiques, les vols à main armée (VMA), les prises d'otages 14

1.3.3 Les intrusions, les cambriolages 15

1.3.4 Les vols, la démarque inconnue 15

1.3.5 Les dégradations volontaires, le vandalisme 16

1.3.6 L'espionnage (secteur économique, industriel…) 16

1.3.7 Le terrorisme 16

1.4 Le risque incendie, les risques naturels, les risques industriels 17

1.4.1 Les incendies 17

1.4.2 Les risques naturels 17

1.4.3 Les risques industriels 17

1.4.4 Les risques individuels 17

1.5 En synthèse : 18

2 GT N°2 – Détection 19
2.1 Constitution du GT N°2 19
2.2 Préambule : bien comprendre la télévidéosurveillance 19
2.2.1 Ce que beaucoup imaginent… 19
2.2.2 … et la réalité 19
2.2.3 La ronde vidéo : un outil de contrôle 20
2.2.4 La levée de doute vidéo : un outil de qualification 20
2.2.4.1 Les techniques aléatoires et chronophages de levée de doute 20
2.2.4.2 Les techniques de récupération automatique d'images qualifiantes 21
2.3 Détecter des actes de malveillance 23
2.3.1 Agressions verbales, incivilités 23
2.3.2 Agressions physiques, vols à main armée (VMA), prises d'otages 24
2.3.3 Intrusions et cambriolages 24
2.3.3.1 Détecter une intrusion et lever le doute à l'intérieur de bâtiments 24
2.3.3.2 Détecter une intrusion et lever le doute à l'extérieur des bâtiments 25
2.3.4 Vol et démarque inconnue 27
2.3.5 Dégradations volontaires et vandalisme 27
2.3.6 Espionnage (secteur économique, industriel…) 29
2.3.7 Terrorisme 30
2.4 Détecter les risques incendie, les risques naturels, les risques industriels 30
2.4.1 Incendie 30
2.4.1.1 Détecter et lever le doute à l'intérieur 30
2.4.1.2 Détecter et lever le doute en extérieur 30
2.4.2 Risques naturels 31
2.4.3 Risques industriels 31
2.5 Risques individuels : télévidéosurveillance et vie privée 32
2.6 Proposition d'améliorations 33
2.7 En synthèse : 33

3 GT N°3 – Traitement au PC 34
3.1 Constitution du GT N°3 34
3.2 Introduction 34
3.3 Effets sur le métier 35
3.3.1 La formation de l'opérateur 35
3.3.2 L'organisation humaine et matérielle des stations de télésurveillance 36
3.3.3 Les modes de levée de doute vidéo sur alarme : 36
3.3.4 Les prestations vidéo-délivrées 36
3.4 Effets sur la technologie 37
3.4.1 Pour le télésurveilleur 37
3.4.2 Pour le constructeur 37
3.5 Effets sur l'organisation des stations de télésurveillance 38
3.6 Effets juridiques : limite, contexte... 38
3.7 Formation des acteurs de la télévidéosurveillance 39
3.7.1 Formation avant-vente 39
3.7.2 Opérateurs télévidéosurveillance 39
3.8 Effets sur la réglementation 41
3.9 En synthèse : 42

4 GT N°4 – Intervention....43
4.1 Constitution du GT N°4....43
4.2 Situation actuelle du marché....43
4.2.1 Nombre d'interventions....43
4.2.2 Plus de 90% des alarmes déclenchées en France sont injustifiées....43
4.2.3 Gendarmerie Nationale / Police Nationale / Polices Municipales / Sociétés de sécurité privées....44
4.3 Définition et perception par l'utilisateur....44
4.3.1 Définition de l'intervention....44
4.3.2 Rappel législatif et contraintes (véhicule non prioritaire, conditions météo…)....45
4.3.3 Remise en cause....46
4.4 Types d'interventions....47
4.4.1 Intervention humaine....47
4.4.2 Intervention vidéo....48
4.4.3 Intervention humaine et vidéo....49
4.5 Évolution du marché....50
4.5.1 Contraintes financières (augmentation du carburant, baisse du prix moyen de l'intervention, augmentation des charges, pénalités de + en + appliquées)....50
4.5.2 Contraintes géographiques (répartition nationale des sociétés de sécurité privée, apparition de zones « blanches »)....50
4.6 Perspectives d'avenir....52
4.6.1 Nouvelles technologies....52
4.6.2 Objectifs....53
4.7 En synthèse :....54

5 Conclusions....55

Préambule

Le mot du Président de l'USP

« Notre véritable défi est celui de l'opinion publique »



L'Union des entreprises de sécurité privée est une organisation qui produit des idées et rassemble des énergies. Elle anticipe et prépare les enjeux de demain.
Rien de plus naturel que la publication de ce Livre Blanc de la télévidéosurveillance par USP-Technologies !
Agitatrice d'idées, USP-Technologies essaie de dessiner le paysage dans lequel évoluera notre marché demain…
Le développement des technologies nouvelles, l'explosion de l'intelligence collaborative et des réseaux de communication, la globalisation et la convergence des solutions ouvertes par les télécommunications et l'informatique font naître un nouveau monde qui bouleverse les esprits et les rites culturels.
Notre véritable défi est celui de l'opinion publique. Elle vit avec angoisse ces mutations car elle craint pour sa liberté. Mais elle perçoit aussi l'espoir que l'évolution de l'offre fait naitre pour garantir, dans sa vie quotidienne, sa tranquillité.
C'est bien de cela dont il s'agit ! Organiser un marché avec des opérateurs responsables et citoyens agissant dans le respect des règles et traditions républicaines. Offrir des solutions attractives alliant les nouveaux outils modernes comme le traitement des images intelligentes et l'action des hommes formés et encadrés.
Ce mouvement est irréversible. Il est inscrit dans notre histoire.
À nous de trouver notre espace dans une logique de complémentarité avec l'État et non de compétition.
À nous de peser pour un cadre juridique clair et sécurisé.
À nous de favoriser l'innovation et l'émergence de nouveaux talents pour faire bouger les lignes et offrir aux entrepreneurs de nouveaux espaces de développement de leurs activités.
L'offre privée de sécurité va accompagner le quotidien des entreprises qui ont besoin de solutions neuves et compétitives et celui du citoyen qui doit se protéger, individuellement et collectivement, de tous les risques auxquels il est exposé.
Notre société est traversée par des tensions qui appellent un choc de lucidité. Il ne faut pas craindre le déploiement des solutions modernes à condition de rester fidèles aux principes fondamentaux de notre République.
Ce Livre Blanc pose un diagnostic, lève les tabous, ouvre le champ des expériences, précise les limites et bouscule les idées reçues.
Mais il souligne, surtout, qu'une nouvelle étape de maturité est franchie par tous les opérateurs du marché.

Le temps de la responsabilité partagée est venu…

Claude TARLET - Président de l'USP

Le mot du Président de l'USP-Technologies



L'arrivée du numérique a en quelques années seulement, profondément bouleversé le monde de la sécurité des personnes, des biens et de l'information.
Le numérique impose l'ère de la multitude ; il redessine les chaînes de valeur et limites d'intervention des acteurs.

Dans cet environnement où les frontières se redessinent, la profession regroupée au sein de l'USP-technologies propose un livre blanc pour éclairer le débat.
En pleine mutation, elle propose les pistes nécessaires pour une maturité assumée, pour garantir sécurité et qualité aux marchés.
Les thèmes essentiels tels que compétence, technologie, convergence « privé / public », ou défense des libertés individuelles et publiques sont abordés sans tabous pour éclairer l'ensemble des acteurs et ainsi formuler des propositions pragmatiques.

Par son engagement au cœur de la convergence homme-technologie, l'USP-Technologies contribue activement à la professionnalisation des métiers technologiques de la sécurité. En s'imposant comme le lieu d'échange et de faire savoir entre les constructeurs, les intégrateurs et les utilisateurs, l'USP-Technologies vulgarise les innovations technologiques au service de la sécurité.

Stéphane BIDAULT, Président de l'USP-Technologies, Président de TEB vidéoprotection.

Quels sont les objectifs de la télévidéosurveillance ?

Depuis son origine, la télésurveillance s'est positionnée au cœur de la chaîne de sécurité. En amont, il y a la détection des évènements, la transmission des alarmes. En aval, il y a les contacts Clients, les professionnels de l'intervention et les force de l'ordre.
Contrairement à l'autosurveillance, la télésurveillance réalisée par des professionnels de la sécurité reconnus et formés, apporte toutes les garanties qu'une action appropriée sera déployée suite aux déclenchements d'alarmes, que les systèmes seront supervisés. La réglementation et les diverses certifications métier assurent au Client une parfaite traçabilité des actions du télésurveilleur.
Deux configurations "juridiques" existent : l'installateur est télésurveilleur, ou il y a un installateur plus un télésurveilleur

- l'installateur est télésurveilleur : Sa responsabilité peut être engagée à 100% en cas de sinistre responsable,
- l'installateur et le télésurveilleur sont juridiquement dissociés : Il peut y avoir partage des responsabilités en cas de sinistre,
- Dans tous les cas, l'installateur a une obligation de conseil qui lui impose d'apporter toutes les informations nécessaires sur la réglementation en vigueur sur la nature des lieux à traiter.

La réflexion de l'USP-Technologie est d'encadrer les prestations (y compris la prestation humaine) dans une offre globale intégrant la technologie et la télésurveillance afin d'envisager les étapes d'optimisation et d'automatisation conduisant à une juste répartition des effectifs.

Quelle est la nature des lieux traités ?

La France est l'un des pays dans lequel l'usage de la vidéoprotection est le plus réglementé. C'est aussi l'un des pays où la réglementation est la plus restrictive. L'installation de vidéoprotection n'est pas libre, et quel que soit le lieu dans lequel elle est installée, il y a des règles à respecter, y compris dans un domicile, lieu pourtant strictement privé.

La nature du lieu à traiter est le critère le plus important de notre réglementation. En effet, les règles applicables à un dispositif ne sont pas les mêmes en fonction des différents types de lieux.

Rappelons qu'il existe trois grands types de lieux :

- **La voie publique** : qui est constituée de tous les espaces publics, ceux qui appartiennent à la collectivité et dans lesquels on peut habituellement circuler librement, à n'importe quelle heure du jour et de la nuit.
- **Les lieux privés ouverts au public** : Au sens de la jurisprudence des juridictions de l'ordre judiciaire, est un lieu ouvert au public « *un lieu accessible à tous, sans autorisation spéciale de quiconque, que l'accès en soit permanent et inconditionnel ou subordonné à certaines conditions* » (TGI de Paris, 23 octobre 1986, Gaz. Pal. du 8 janvier 1987, confirmé par un arrêt de la Cour d'appel de Paris du 19 novembre 1986). Ce sont des lieux qui peuvent être fermés à un moment quelconque de la journée, mais qui accueillent du public durant leur ouverture. Par exemple on trouvera ici un musée, un centre commercial ou le hall d'une mairie.
- **Les lieux strictement privés** : un lieu devient privé dès lors qu'un contrôle quelconque est mis en place aux accès : contrôle d'accès automatique, accueil avec présentation de papiers d'identité, digicode, visiophone… Un domicile entre donc logiquement dans cette dernière catégorie. La différence avec un lieu ouvert au public (ou un contrôle peut être effectué à l'entrée) est la fréquentation.

  Attention ! Pour qu'un espace extérieur puisse être considéré comme strictement privé, les tribunaux exigent que l'espace soit clôturé, avec un portillon équipé d'un dispositif de fermeture. Une maison abritant à la fois des locaux privés et des locaux à usage professionnel peut être concernée par plusieurs régimes juridiques différents. Pour un lieu de travail, si l'endroit dans lequel la vidéoprotection est déployée est occupé par des salariés, alors le droit du travail s'applique.

Évolution du métier

Initialement centré sur la détection intrusion basique, ce métier est en constante évolution. Très rapidement les prestations ont été étendues à la détection d'incendie, technique, froid, à la surveillance des individus (particulièrement en Téléassistance).

Face à l'intempestivité des alarmes et à la réglementation, il a fallu associer à la détection des moyens de levée de doute. Celle-ci a commencé par un appel sur site, de l'écoute grâce à des micros, de l'interphonie associant micro et haut-parleur, puis grâce à l'évolution de la technologie, notamment la qualité des images permettant une réelle identification, des réseaux de communications, par des moyens vidéo et des téléactions.

Dans le domaine de l'exploitation de la vidéo, deux métiers se distinguent :

- La **vidéoprotection** qui exploite des caméras en direct et en permanence. Cette pratique est associée au domaine **public** ou aux espaces privés ouverts au public (cf chapitre précédent).
- La **télévidéosurveillance** qui exploite des alarmes détectées soit par un système de détection classique associée à des caméras soit par une détection à partir des caméras. Cette pratique est associée au domaine **privé** et donc aux télésurveilleurs. Il est à noter qu'aucun professionnel de la sécurité globale n'est là pour surveiller les personnes, mais pour les protéger. Nous pourrions donc assister à terme à l'introduction du terme de **télévidéoprotection**.

Quelques prérogatives pour une solution exploitable, fonctionnelle et pleinement opérationnelle :
Lorsqu'il s'agit de vidéosurveillance, vidéoprotection, de traitement à distance de la levée de doute vidéo et de télévidéoprotection, les professionnels du secteur doivent préconiser des systèmes de haute qualité :

- Une caméra à haute résolution, équipée des fonctions adaptées à l'environnement dans lequel elle est installée (qualité des images, fort contre-jour, faible luminosité…),
- Un serveur adapté à la haute définition avec CMS (Logiciel) fonctionnel garantissant la prise en charge du flux vidéo combinant un nombre élevé d'images par seconde, et très haute résolution,
- Garantir des unités de stockage redondantes avec capacité de sauvegarde dimensionnées au nombre de caméras installées, au nombre d'images par seconde et à la durée de conservation souhaitée,
- Un dispositif de transmission et communication des flux vidéo de haut débit, et de bonne qualité de service (QoS),
- Une parfaite mise en sécurité de l'ensemble des dispositifs techniques face aux attaques potentielles ou avérées du système d'information (SSI = Sécurité du Système d'Information).

1 GT N°1 – Qualification des risques

1.1 Constitution du GT N°1

Rapporteur : M. Frédéric VIAL – ONET Sécurité

Experts :

- M. Christophe COUTURIER - Eurofeu technologies
- M. Philippe DEBAYE - Axis
- M. Pascal DEBOUT - TEB
- M. Olivier WEBER - Groupe Scutum
- M. Alain DELCROIX – AXA Corporate Solutions
- M. Dominique LEGRAND - AN2V

1.2 Préambule

Nous avons préalablement défini une liste de risques, pour lesquels la télévidéosurveillance pourrait constituer un moyen de prévention ou de traitement.
L'approche tient compte assez naturellement de la différenciation entre le traitement des actes de **malveillance** (toujours avec à l'origine une action volontaire d'une ou de plusieurs personnes), et le traitement des **accidents** (sinistres provoqués sans action volontaire).
A chaque type de risque, correspondent des modes de traitement préventif, d'évitement ou d'identification de causes. Dans de nombreux cas, les moyens de télévidéosurveillance sont une alternative dans le choix de ces modes de traitement.

L'approche du traitement du risque dans la sécurité globale est donc adaptée en fonction du domaine duquel il relève :

- **La sécurité** : désigne l'ensemble des moyens humains, organisationnels et techniques réunis pour faire face aux risques techniques, physiques, chimiques et environnementaux pouvant nuire aux personnes et aux biens sans avoir un but de profit. Elle répond à de nombreuses règles établies, notamment la sécurité incendie qui est de la compétence des sapeurs-pompiers
- **La sûreté** : concerne l'ensemble des moyens humains, organisationnels et techniques réunis pour faire face aux actes spontanés ou réfléchis ayant pour but de nuire, ou de porter atteinte dans un but de profit psychique ou/et financier. Elle répond à des règles distinctes de celles établies pour la sécurité, et est régie par des textes différents.

1.3 La malveillance

1.3.1 Les agressions verbales, les incivilités

Elles se produisent plutôt dans les lieux publics. A l' origine, des personnes dont le comportement devient agressif, suite à la non prise en compte et la résolution immédiate d'une requête, une demande.

Exemples :

- file d'attente,
- caisse de paiement dans un commerce,
- guichet Pôle Emploi,
- restauration rapide,
- banque,
- un différend avec une autre personne.

Dans tous les cas, une insatisfaction ou une exaspération qui fait que la personne ne se contrôle plus. Il s'agit d'un comportement irréfléchi et spontané, l'action n'est pas préméditée. La prévention est compliquée à mettre en œuvre (pas de classification juridique/pénale), il faut faire appel au sens civique, au comportement social, et avertir contre le risque de dérive vers l'agression physique (contravention, délit). Tout système de vidéosurveillance peut permettre le traitement de ce type de risque : détection (analyse comportementale), dissuasion et aide à la résolution : stockage d'images avec information préalable au public, identification. Difficulté majeure : il s'agit d'un risque, qui s'il ne dérive pas vers l'agression physique, n'expose pas l'auteur à des sanctions. Le nombre des incivilités augmente exponentiellement.

1.3.2 Les agressions physiques, les vols à main armée (VMA), les prises d'otages

Le risque est permanent, en tous lieux (intérieur, extérieur), où la présence de personnes est réduite. Les auteurs en sont des délinquants, des personnes en lien avec le grand banditisme, qui agissent individuellement, ou en bande organisée, avec ou sans armes : armes blanches, armes à feu…
A l'origine :

- un différend,
- une altercation,
- l'appât du gain,
- une revendication idéologique,

où la contrainte exercée sur une tierce personne, ou un groupe de personnes, va permettre à l'auteur de l'agression, du braquage, de la prise d'otage, d'atteindre son but.
Les actions peuvent être préméditées ou non, préparées ou irréfléchies :

- violence gratuite,
- racisme,
- homophobie,
- vol sous la contrainte,
- séquestration,
- home jacking…

Pour lutter contre ce type de risque : la protection physique des locaux (domicile, lieux de travail), les alarmes (boutons agression, alarmes individuelles avec géolocalisation…), la vidéosurveillance, à l'intérieur des bâtiments, ou sur les lieux publics avec la vidéoprotection. Difficulté majeure pour les alarmes volontaires : la menace peut inhiber toute réaction pour signaler la situation d'agression.

1.3.3 Les intrusions, les cambriolages

Dans les locaux d'habitation, les locaux professionnels, ce risque se présente plutôt en absence partielle ou totale d'occupants.
Les auteurs potentiels d'intrusions, de cambriolage sont très divers :

- petite délinquance (mineurs, isolés en groupes),
- grande délinquance, banditisme,
- bandes organisées : familles, mafias…

Les actes sont très souvent prémédités, en fonction des opportunités (absences, congés…), et c'est l'appât du gain, la revente potentielle d'objets de valeur, l'assouvissement immédiat de besoins personnels (stupéfiants) qui motive ces actes. Pour se prémunir : la protection physique des locaux, le contrôle des d'accès, les dispositifs d'alarme intrusion reliés en télésurveillance, les systèmes dissuasifs locaux (avertisseurs, diffuseurs de brouillard…), les agents de sécurité, et les systèmes de vidéosurveillance, permettant la dissuasion, la levée de doute, et l'exploitation des enregistrements par les enquêteurs, aux fins d'identification des circonstances, voire des auteurs.

1.3.4 Les vols, la démarque inconnue

Ces faits sont commis dans les lieux publics, en période d'affluence dans les commerces, dans les lieux privés, en présence ou non de tierces personnes. Les modes opératoires sont très diversifiés, ce qui rend compliquée leur détection.
Fait marquant, tout le monde peut être à l'origine d'un vol, il peut s'agir de délinquants, de personnes insérées socialement, mais en proie à une pulsion irraisonnée, d'hommes, de femmes…
Les cibles privilégiées :

- les individus avec vol sans violence (téléphones mobiles, sac à main…),
- les commerces,
- la grande distribution,
- les entreprises,
- les lieux publics, en intérieur, en extérieur…

Il peut s'agir d'actions préméditées, calculées, mais également d'actes opportunistes, qui se font avec rapidité et furtivité. Pour lutter : les marqueurs électroniques, les portiques antivols (boutiques), les codes et systèmes de protection logiques ou de blocage à distance (tél mobiles, ordinateurs…), le gardiennage, et la vidéo surveillance (analyse comportementale, vidéo haute définition pour l'identification). La difficulté majeure réside dans la fraude des dispositifs de protection antivol, et dans la ressource nécessaire en moyens humains pour exploiter un système de vidéosurveillance.

1.3.5 Les dégradations volontaires, le vandalisme

Il s'agit d'un risque permanent 24h/24, en tous lieux, en tous secteurs (urbain, rural, sites naturels…), qui peut survenir avec ou sans présence de tierces personnes. Les auteurs, comme pour les vols et la démarque inconnue, sont multiples et sans catégorisation précise.
Les motivations sont diverses :

- actes gratuits,
- vengeance et volonté de nuire à un tiers ou à la société,
- altercations,
- différends…

Les actes commis sont souvent rapides et furtifs. S'en prémunir est très difficile, sauf pour les lieux clos, où une protection physique efficace, combinée à un dispositif de détection électronique (Tags RFID dans les expositions) ou à un dispositif de gardiennage, peut dissuader les auteurs potentiels. La vidéo surveillance est un outil précieux pour anticiper (analyse comportementale) et identifier.

1.3.6 L'espionnage (secteur économique, industriel…)

Le risque est permanent, 24h/24, il concerne (hors secteur militaire & le Gouvernement) essentiellement le secteur économique, industriel, où des concurrents déloyaux pourraient être tentés de s'approprier toutes informations, toutes données techniques, commerciales…
Les auteurs sont difficiles à identifier, en interne ou en externe de l'entreprise victime d'espionnage. Le risque existe sur le lieu de l'entreprise, mais également dans les lieux publics, au domicile des personnes ciblées. Les actes sont toujours prémédités, savamment préparés, de manière à ce que leur exécution ne soit pas détectable par des tiers, ou par la personne directement visée. Pour se protéger : contrôle des accès, sécurité informatique, vidéo surveillance, en installations fixes ou en dispositifs temporaires (appât), en véhicules mobiles… Principale difficulté : difficile à anticipé, grande part d'aléatoire…

1.3.7 Le terrorisme

Le risque est directement lié aux évolutions géopolitiques, à l'émergence d'idéaux sociologiques, religieux, qui se placent en opposition avec les régimes gouvernementaux en place. Les mouvements ou groupes terroristes sont par essence non reconnus légalement et existent donc dans la clandestinité, ce qui rend leur identification et leur localisation extrêmement complexe. Les auteurs potentiels d'actes sont difficiles à identifier, cette tâche est de la responsabilité des services de l'état.
Toutefois, les observations menées par ces services de l'état, quels qu'ils soient (Ministère de l'Intérieur, Ministère de la Défense…) peuvent conduire ces mêmes services à solliciter les moyens privés de la sûreté pour compléter les investigations en cours.
Bien naturellement, les moyens de vidéosurveillance sont des outils précieux qui peuvent être utilisés pour rechercher un évènement, reconstituer son déroulé, et analyser de manière contradictoire certaines hypothèses. Au plus le réseau de vidéosurveillance est dense, au plus leur efficacité pour permettre la lutte contre le terrorisme est réelle.

1.4 Le risque incendie, les risques naturels, les risques industriels

1.4.1 Les incendies

Risque permanent, en tous lieux, tous secteurs, accentué sur certaines périodes : en été pour incendies de forêts, en hiver pour incendies habitations. Peu d'incendies « instantanés », il y a toujours une cause humaine : négligence, combinaison de facteurs déclenchant (accidents). Incendies volontaires, dans ce cas, plus assimilables à acte de dégradation volontaire, de destruction. La détection est possible dans les lieux clos en intérieur, sous certaines conditions en extérieur, avec la détection par caméras thermiques. La prévention également, avec le gardiennage, les postes de vigie locale ou à distance par vidéosurveillance. Principale difficulté : la rapidité de détection et de réactivité, opposées à la vitesse de propagation d'un incendie.

1.4.2 Les risques naturels

Ces risques sont essentiellement géologiques, climatologiques : tremblements de terre, tsunamis, et les conséquences sont considérables. Leur anticipation est effectuée par divers services de l'Etat : Services d'intérêt Vital, Points d'intérêt Vital. Le risque est existant 24h/24, en tous lieux, avec toutefois des zones potentiellement plus exposées que d'autres (cartographie des risques). La détection précoce est assurée par les services de l'état, par les entreprises : ERDF pour les barrages par exemple, avec de la détection sismique, du contrôle de mesures sur site, et également de la vidéosurveillance. Point majeur : le risque ne peut être éradiqué, il s'agit d'en minimiser les conséquences.

1.4.3 Les risques industriels

NRBC : les risques Nucléaires, Radiologiques, Biologiques, Chimiques
Risque permanent, lorsqu'il est identifié, est localisé sur les lieux de production d'énergie : centrales nucléaires, centres de production d'uranium, centres de traitement des déchets nucléaires. Au niveau des entreprises, secteur de la chimie, du médical, centres de recherche…
Facteurs déclenchants : combinaison de faits concomitants, non prévus dans leur globalité, négligences, erreurs humaines. Les moyens de prévention sont nombreux, gérés industriellement, la difficulté est similaire au risque incendie : propagation rapide, jusqu'à en rendre les effets incontrôlables. La vidéo peut constituer un moyen de coordination des actions de secours.

1.4.4 Les risques individuels

Les moyens de protection individuelle pour les personnes isolées se sont développés avec l'évolution des moyens de communication (GSM, GPRS associés à la géolocalisation).
Les particuliers (personnes seules ou âgées, patients soignés à domicile…) peuvent bénéficier de ces moyens de protection individuelle, associés à des services de téléassistance.
Comme en télésurveillance, la difficulté et l'efficience de ces services sont proportionnels aux moyens de vérification du bien fondé du déclenchement de l'alarme ou de l'appel de détresse. Lorsque l'interphonie est inefficace, les moyens de visualisation à distance en temps réel sont un atout précieux pour gagner du temps et caractériser la situation avant sollicitation des forces de l'ordre ou des pompiers.

D’autres types de risque (risque sanitaire, risques liés à des mouvements sociaux de grande ampleur tels de manifestations, troubles à l’ordre public…) pourront être traités par le biais de la vidéo, dès lors que les moyens seront mutualisés et administrés de façon à permettre une continuité « logique et physique » de l’exploitation de ces moyens de vidéosurveillance.

Ce document couvre les applications principales, autres que ces risques spécifiques.

1.5 En synthèse :

En synthèse, quels que soient les risques identifiés :

- La malveillance : les agressions, les intrusions, les vols, les dégradations,
- Le risque incendie, les risques naturels, les risques industriels,

nous pouvons déjà, à l’énumération de ces événements, deviner et envisager l’apport que les moyens de télévidéosurveillance peuvent constituer, avec plus ou moins d’efficacité et d’efficience, suivant leur dimensionnement.

Ces moyens ne peuvent constituer à eux seuls la parade universelle et unique à tous ces risques, mais ils sont une composante incontournable dans la lutte contre ceux-ci.

Le chapitre suivant traite des moyens permettant d’identifier et déceler ces différents risques.

2 GT N°2 – Détection

2.1 Constitution du GT N°2

Rapporteur : M. Patrick LAUNAY – Groupe Scutum

Experts :

- M. Pascal DEBOUT - TEB
- M. Garry GOLDENBERG - Open IP video
- M. Philippe DEBAYE - Axis
- M. Edouard CHÂTEAU - Groupe ADEC
- M. Eric VANDER-MAELEN - Securitas

2.2 Préambule : bien comprendre la télévidéosurveillance

La prévention, la détection et la qualification/vérification des **actes de malveillance** et **des risques incendie, naturels et technologiques** utilisent de plus en plus la télévidéosurveillance : un déploiement efficace nécessite de bien connaître le fonctionnement d'un centre de télésurveillance, notamment lorsque les caméras de surveillance se trouvent au cœur du système en devenant elles-mêmes des détecteurs.

2.2.1 Ce que beaucoup imaginent…

Beaucoup trop de clients imaginent encore un centre de télévidéosurveillance comme un poste de gardiennage d'un grand site industriel, avec un nombre de gardiens et un nombre d'écrans beaucoup plus important, s'agissant de surveiller non pas un seul site mais **plusieurs dizaines de milliers de sites** : lorsqu'un site est en alarme, les caméras de ce site seraient automatiquement affichées sur un écran et un des opérateurs disponibles regarderait l'écran : une mutualisation de moyens de gardiennage en quelque sorte, rendue possible grâce au transport de la vidéo sur les réseaux publics.

2.2.2 … et la réalité

Un centre de télésurveillance est avant tout un centre de traitement d'alarmes entrantes, plusieurs milliers d'alarmes par jour, la plupart n'étant liées ou liables à aucune caméra : alarmes techniques, défaut de fonctionnement, défaut de liaison avec les sites, absence de mise sous surveillance… Ces alarmes entrantes s'empilent dans le système informatique de gestion du centre de télésurveillance et plusieurs opérateurs les dépilent en frontal devant leurs écrans de travail. Règle du jeu : respecter un délai de prise en compte réglementaire de 3 minutes maximum (Règle APSAD R31) entre l'arrivée de l'alarme et le début de traitement de cette alarme par un opérateur.

Toutes les alarmes reçues doivent être traitées. Elles font donc l'objet de consignes détaillées du traitement à réaliser par les opérateurs : appel du client ou de ses mandataires, envoi d'un intervenant sur place, suivi et compte-rendu de l'intervention…

Parmi ces milliers d'alarmes présentées aux opérateurs, quelques-unes sont notifiées comme bénéficiant d'un dispositif de levée de doute vidéo. Pour celles-ci, l'opérateur aura donc la possibilité d'analyser des images afin de qualifier ou vérifier l'alarme : à la suite de cette analyse, certaines alarmes seront classées comme fausses alarmes, d'autres alarmes entraineront l'appel direct des forces de l'ordre.

Ainsi, à la différence de **la vidéoprotection** où des agents postés dans des Centres de Supervisions Urbains observent **24h/24** des écrans et pilotent des caméras, la télévidéosurveillance relève plus d'**analyses ponctuelles** d'images par des opérateurs dans un contexte de vérification d'une alarme entrante.

2.2.3 La ronde vidéo : un outil de contrôle

C'est une prestation de télévidéosurveillance ponctuelle, opérée depuis un centre de télésurveillance pour une durée limitée dans le temps, généralement de quelques minutes au plus. Elle peut être programmée aléatoirement ou à heure fixe dans le système informatique de gestion du centre de télésurveillance : c'est donc une mission qui s'insère dans la pile des alarmes entrantes du centre de télésurveillance et dont se saisit un opérateur disponible du centre de télésurveillance.

La ronde vidéo constitue un moyen de **prévention des risques :** elle peut permettre aux opérateurs de constater une situation anormale, caractéristique d'un fait imminent, en cours ou déjà survenu. De par son caractère non permanent, elle ne peut être considérée comme un **moyen fiable de détection des risques**.

Par contre, la ronde vidéo permet de vérifier la disponibilité et la qualité des images des caméras déployées sur les sites distants, caméras qui pourraient se révéler capitales pour lever le doute sur une alarme future.

2.2.4 La levée de doute vidéo : un outil de qualification

Sous ce vocable, on regroupe toutes les techniques permettant aux opérateurs de **qualifier/vérifier** par l'image, les alarmes générées sur les sites distants par des personnes ou des équipements de surveillance automatique.

2.2.4.1 Les techniques aléatoires et chronophages de levée de doute

Beaucoup s'imaginent que la seule disponibilité d'un système de vidéosurveillance et d'une connexion Internet permet d'effectuer une levée de doute vidéo par télévidéosurveillance : ce sont évidemment deux conditions nécessaires, mais pas suffisantes.

En effet, il convient de se remettre dans le contexte du traitement d'une alarme : lorsqu'un opérateur se saisit d'une alarme dans la pile des alarmes entrantes, celle-ci date déjà de plusieurs secondes à … plusieurs minutes. Même si, grâce à des mécanismes de priorisation, la moyenne des temps de prise en compte des alarmes se situe le plus souvent au-dessous de la minute, ce décalage entre le fait générateur d'une alarme et la disponibilité d'un opérateur pour traiter cette alarme permet de comprendre le défit technique de la levée de doute vidéo.

2.2.4.1.1 Connexion en direct par l'opérateur sur les caméras

Cette technique est **aléatoire**, car plusieurs secondes après les faits, les images fournies en direct par les caméras peuvent ne rien révéler sans pour autant qu'il ne se soit rien passé : par exemple, dans le cas d'un système de détection d'intrusion extérieur, un intrus détecté au franchissement d'une clôture et visible à ce moment là par une caméra extérieure, peut déjà être hors champ de vision de toute caméra lorsque l'opérateur se connecte en direct. Si l'intrus est encore visible, tant mieux, on pourra prévenir les forces de l'ordre. Si l'opérateur ne constate rien d'anormal, il faudra le plus souvent prévenir le client et/ou envoyer un intervenant pour vérifier sur place.

2.2.4.1.2 Recherche d'images sur les enregistreurs vidéo des sites

Si l'opérateur dispose des moyens techniques et des droits pour consulter les enregistrements vidéo d'un site en alarme, il peut rechercher les images enregistrées au moment de l'alarme.

Cette technique est **chronophage**, car l'opérateur doit successivement rechercher la présence d'enregistrements sur les bonnes caméras à l'heure de l'alarme (pour faciliter les choses, la plupart du temps les enregistreurs ne sont pas à l'heure) et ensuite rapatrier ceux-ci ou les lire en streaming au travers d'un réseau ne disposant généralement pas d'une bande passante adaptée (l'ADSL privilégie les flux d'informations descendant vers le site client au détriment des vidéos qui remontent vers le centre de télésurveillance).

Il faut souvent plusieurs minutes supplémentaires pour aboutir (ou non) à une levée de doute qualifiante avec cette technique.

2.2.4.2 Les techniques de récupération automatique d'images qualifiantes

Les techniques les plus efficaces sont celles où les images qualifiantes sont automatiquement associées aux alarmes et directement soumises à l'analyse des opérateurs. Ces techniques nécessitent un couplage « caméra-détecteur » réalisé soit :

- par l'installateur des systèmes de sécurité, par réalisation d'asservissements entre les systèmes de détection et les systèmes de vidéosurveillance,
- au niveau du centre de télésurveillance, par paramétrage du système informatique de gestion du centre de télésurveillance,
- par Analyse Vidéo Intelligente, procédé consistant à transformer la caméra à la fois en détecteur et en dispositif de levée de doute vidéo

Dans tous les cas, un mauvais couplage « caméra-détecteur » peut conduire à la production d'images hors contexte à l'opérateur qui, de bonne foi, procédera au classement d'une intrusion réelle en fausse alarme. D'où la nécessité d'une conception sans faille des systèmes et d'une forte collaboration entre l'installateur du système de surveillance et le télésurveilleur du site.

2.2.4.2.1 Le mode « push »

Dans ce mode, les équipements de surveillance du site sous télévidéosurveillance transmettent à la fois les alarmes et des clips vidéo ou images qualifiantes au centre de télésurveillance. L'opérateur qui se saisit du traitement de l'alarme dispose déjà des images sur son poste informatique. Sa mission est donc de qualifier les images reçues sans avoir besoin d'aller les chercher. L'efficacité du dispositif repose sur la qualité du couplage « caméra-détecteur » réalisé par l'installateur du système de télévidéosurveillance.

2.2.4.2.2 Le mode « pull »

Dans ce mode, c'est l'informatique de gestion du centre de télésurveillance qui, à la réception d'une alarme et avant qu'un opérateur se saisisse de celle-ci, va se connecter sur les équipements vidéo du site et requérir les images qualifiantes afin de les associer à l'alarme reçue. L'efficacité du dispositif repose également sur le couplage « caméra-détecteur » conçu par l'installateur du système de télévidéosurveillance et communiqué au centre de télésurveillance. On parle de mode « pull » ou encore parfois d' «opérateur logique ».

2.2.4.2.3 Le mode « détection et levée de doute vidéo par Analyse Vidéo Intelligente »

Les alarmes et pré-alarmes sont directement générées par des systèmes d'Analyse Vidéo Intelligents exploitant les images des caméras de surveillance afin d'y repérer des « signatures » caractéristiques des faits et risques que l'on souhaite détecter : intrusion d'un intrus dans une zone, départ de feu, agression potentielle d'un employé…

Dans ce mode, il n'y a plus de problème de couplage « caméra-détecteur » car la caméra est, en quelque sorte, le détecteur. De plus, avant de transmettre les images au centre de télésurveillance, le dispositif d'Analyse Vidéo Intelligente les enrichit d'informations destinées à en faciliter l'analyse par les opérateurs.

Exemples :

- détourage dans les images du ou des intrus dans le cas d'une détection d'intrusion,
- inscription des valeurs de température mesurées dans le cas de la détection d'un départ de feu,
- détourage de l'employé et de l'agresseur dans le cas d'une détection d'agression.

La multiplicité des techniques de détection existantes et l'émergence de nouvelles techniques de détection par Analyse Vidéo Intelligente ne doivent pas faire oublier aux clients et aux installateurs que ce sont des hommes qui sont au cœur du traitement de l'information. Même si les dernières technologies autorisent des levées de doute rapides et plus sûres par les opérateurs, trop d'alarmes intempestives peuvent discréditer complètement un site télévidéosurveillé aux yeux des opérateurs et affaiblir leur vigilance pour l'analyse des images de celui-ci.

2.3 Détecter des actes de malveillance

2.3.1 Agressions verbales, incivilités

Un constat : il n'existe pas aujourd'hui de technologie mature de détection automatique d'agressions verbales.

Toutefois, des dispositifs de **prévention des incivilités** sont actuellement intégrés dans certains systèmes de vidéosurveillance. Ils sont basés sur :

- Un mode de signalisation volontaire par la personne se sentant agressée (bouton poussoir, tablette tactile…)
- Un affichage dissuasif via un écran PLV (Publicité sur le Lieu de Vente) dont le contenu va être modifié dynamiquement lorsque l'employé signale une dérive de comportement d'un client : commutation sur un film de sensibilisation aux incivilités, commutation en direct sur la caméra visionnant l'individu. L'objectif étant essentiellement de dissuader avant le passage à l'acte, la télévidéosurveillance n'est pas sollicitée à ce stade.

Signalons également que de nombreuses caméras IP disposent de micro intégré et peuvent détecter un franchissement de seuil du niveau sonore ambiant. Si ce type alarme peut constituer une alternative à l'alarme volontaire pour contrôler un affichage dynamique, les télésurveilleurs ne sont pas prompts à accepter la gestion d'alarmes sonores :

- d'une part le micro de la caméra ne fera pas la différence entre une élévation normale du niveau sonore (passage d'un camion de pompier) et une élévation sonore liée à un individu qui s'emporte, d'où de nombreuses fausses alarmes.
- d'autre part, même si la levée de doute par télévidéosurveillance est techniquement possible avec des clips **audio**/vidéo, il y a un problème juridique lié à l'écoute d'une personne sans son consentement puisque les images et le son sont enregistrés dans la caméra et au centre de télésurveillance…

L'Analyse Vidéo Intelligente propose également aujourd'hui la détection de signatures intéressantes dans la détection de ce type d'incivilité, les technologies étant issues de recherches sur les mouvements de foule :

- détection d'attroupement (les autres personnes prennent fait et cause pour l'agresseur),
- détection de dispersion rapide (les personnes se désolidarisent et s'éloignent de l'agresseur),
- détection de mouvements brusques d'une personne (l'agresseur, l'agressé ou un autre client effrayé).

Plusieurs de ces techniques sont actuellement testées en vidéosurveillance urbaine et dans des PC de Sécurité de lieux publics : il en ressort généralement qu'une multitude de faits normaux produisent des signatures similaires aux faits que l'on souhaite détecter, rendant rapidement ces dispositifs peu crédibles aux yeux des agents d'exploitation.

Enfin, des études scientifiques sur l'analyse comportementale permettent aux éditeurs de logiciels spécialisés dans l'Analyse Vidéo Intelligente d'entrevoir la possibilité d'intégrer dans les caméras des algorithmes de détection de changement d'expression des visages (colère, mépris, dégoût, peur…) : couplés à une levée de doute vidéo en télévidéosurveillance, ces technologies pourront peut-être un jour se substituer à la signalisation volontaire par la personne agressée ?

2.3.2 Agressions physiques, vols à main armée (VMA), prises d'otages

Actuellement, plusieurs techniques de détection sont déployées :

- L'alarme agression, par composition volontaire d'un code sous contrainte, appui sur un bouton d'agression, activation d'un équipement de protection individuelle, non appui sur un bouton d'acquittement…
- L'alarme dite « comportementale », par non respect volontaire, par les employés, des procédures obligatoires (ouverture d'un coffre tout en laissant la porte du local coffre ouverte…)
- La détection automatique d'agression d'un employé à l'ouverture d'un commerce le matin ; celle-ci utilise l'Analyse Vidéo Intelligente pour compter le nombre de personnes pénétrant dans le commerce : si l'employé rentre seul, tout va bien, si une personne l'accompagne (alors que la procédure l'interdit), il y a suspicion d'agression.

La télévidéosurveillance permet de lever le doute face aux erreurs de manipulations ou au non respect des consignes et d'alerter la police sur des situations critiques confirmées.

2.3.3 Intrusions et cambriolages

C'est dans ce domaine que la télévidéosurveillance rencontre aujourd'hui le plus de succès :

- en permettant la vérification des alarmes directement par les opérateurs, elle évite d'exposer inutilement les responsables des sites ou leurs mandataires par une vérification sur site alors que des intrus opèrent
- en autorisant l'alerte des forces de l'ordre lorsqu'une infraction est confirmée par les images, elle permet des arrestations en flagrant délit : encore faut-il que la police soit appelée très rapidement. Il convient donc que les clients, installateurs et télésurveilleurs, s'entendent sur la mise en œuvre des techniques de levée de doute rapide (push, pull, Analyse Vidéo Intelligente).

2.3.3.1 Détecter une intrusion et lever le doute à l'intérieur de bâtiments

2.3.3.1.1 Télévidéosurveillance par Pircam

De nombreux systèmes de télévidéosurveillance utilisent des détecteurs d'intrusion intégrant des caméras dont les champs de vision recouvrent les zones de détection des capteurs de mouvements : une série de photos ou clips vidéo pris au moment des alarmes est présentée aux opérateurs conjointement à l'alarme intrusion. Ces détecteurs/caméras sont appelés couramment **Pircam** (Passive Infra-Red Camera). Ils ne bénéficient généralement pas des certifications produits NFA2P qui pourraient être requises pour la couverture de niveaux de risques élevés (au sens de l'assurance).

2.3.3.1.2 Autres systèmes de télévidéosurveillance

D'autres systèmes de télévidéosurveillance consistent à coupler les systèmes de détection d'intrusion classiques avec les systèmes de vidéoprotection des mêmes sites.

Le couplage de type « asservissement entre systèmes » (ou mode « push ») n'est pas toujours aisé à réaliser techniquement et rarement pérenne : systèmes d'alarme et systèmes de vidéosurveillance ne répondent pas aux même attentes des clients et il n'est pas rare de voir les investissements successifs diverger dans le temps entre les deux systèmes, conduisant parfois à des installateurs et mainteneurs différents pour l'alarme et pour la vidéosurveillance.

C'est pourquoi, il est souvent préféré un couplage « logique » effectué par l'informatique du centre de télésurveillance (mode « pull » dont le fonctionnement a été décrit plus haut). Ce mode de couplage permet une évolution non concertée des équipements d'alarme et de vidéosurveillance : si un couplage caméra/détecteur est possible, il permettra une levée de doute automatique par télévidéosurveillance ; si aucun couplage caméra/détecteur n'est possible ou s'il n'est plus possible pour un détecteur, la levée de doute devra s'opérer par les moyens traditionnels. A noter que l'information du télésurveilleur par le client (via ses installateurs) lorsqu'une modification intervient sur un des systèmes d'alarme ou de vidéosurveillance est indispensable au maintien des couplages logiques.

2.3.3.2 Détecter une intrusion et lever le doute à l'extérieur des bâtiments

La télévidéosurveillance **à l'extérieur** des bâtiments représente un enjeu important pour de nombreux sites, notamment en raison de l'accélération des vols de carburants sur les véhicules parqués, et plus généralement, des vols de matériels et équipements stockés à l'extérieur des bâtiments.

La clé du succès consiste à résoudre une équation à trois inconnues :

- Un système de détection extérieur couvrant soit les secteurs à risques (parcs véhicules, aires de stockage), soit les points d'intrusion potentiels sur le site, va permettre la transmission d'une alarme en télésurveillance ; **inconnue 1 : quelle technique mettre en œuvre (barrières infrarouges, câbles détecteurs sur clôtures, lasers…)?**
- La vérification par télévidéosurveillance va permettre de faire appel aux forces de l'ordre ; **inconnue 2 : le système de vidéosurveillance est-il qualifiant sur tout le site et tout le temps (de jour, de nuit, par temps de pluie, neige, brouillard, en cas de coupure d'électricité sur le site…)**
- L'arrivée rapide des forces de l'ordre pourra conduire à des arrestations en flagrant délit ; **inconnue 3 : combien de temps s'est-il écoulé entre le déclenchement de l'alarme et l'arrivée sur place des forces de l'ordre ?**

Les techniques de type « Pircam » se révèlent peu efficaces en extérieur : portée de détection limitée, instabilité (fausses alarmes), faible qualité des images de levée de doute : installateurs et télésurveilleurs limitent généralement leur usage au piégeage de points de passages obligés.

Par ailleurs, associer des systèmes de détection extérieurs éprouvés (barrières infrarouges, hyperfréquences, laser, câble enterré, câble choc sur clôture…) à de la levée de doute vidéo nécessite une expertise technique importante. La difficulté essentielle consiste à fournir en télévidéosurveillance des images de levée de doute qualifiantes quelles que soient les conditions d'éclairage (jour/nuit) et d'intempéries (pluie, neige, brouillard) et quel que soit le point de pénétration sur le site : une image où un intrus ne représente que 2 ou 3 pixels à l'image parce qu'il est loin de la caméra ne permettra pas à l'opérateur de lever le doute.

Là-aussi, l'Analyse Vidéo Intelligente associée à des caméras « visibles » ou « thermiques » simplifie la conception des systèmes de détection et de levée de doute vidéo **qui ne font plus qu'un seul système**. L'équation à trois inconnues devient une équation à deux inconnues : détection/levée de doute, alerte/intervention des forces de l'ordre.

La contrepartie de la simplification de la conception est qu'il convient de s'assurer de la robustesse de ces systèmes, notamment leur résistance à la fraude et à la panne :

- stabilité satisfaisante du système (trop de fausses alarmes fragilise l'exploitation)
- autonomie de fonctionnement de plusieurs heures de la chaîne de détection, d'alerte et de levée de doute en cas de coupure secteur,
- modes de transmission multiples des alarmes vers le télésurveilleur afin de pallier à la défaillance d'un réseau de transmission,
- supervision de la bonne orientation des caméras et de leur non obstruction
- supervision du bon fonctionnement des caméras et des process d'Analyse Vidéo Intelligente

Des solutions de supervision automatiques existent :

- au niveau des enregistreurs numériques : détection de masquage, floutage, dé-azimutage, défocalisation des caméras, perte de connexions ; ces alarmes sont transmises en télésurveillance
- directement depuis les systèmes informatiques d'exploitation des centres de télésurveillance : interrogation cycliques des équipements, vérification de bon fonctionnement des process vitaux (comme l'analyse vidéo intelligente).

Quelle que soit la pertinence de ces process automatiques, il peut être intéressant de programmer également des rondes vidéo régulières effectuées par les opérateurs (une fois par mois ou par semaine).

2.3.4 Vol et démarque inconnue

De nombreux systèmes existent pour lutter contre la démarque inconnue, les plus connus étant les étiquettes antivol associées à des portiques de détection installés aux entrées/sorties des commerces.

L'exploitation est locale et mobilise des agents de sécurité en surface de vente et des agents de sécurité dans les PC de Sécurité. Les besoins de télévidéosurveillance actuellement exprimés par les responsables sécurité de grandes chaines vont dans le sens d'une mutualisation de leurs PC de sécurité (un PC de sécurité régional ou national, versus un PC de sécurité par magasin). Certains ont franchi le pas et sont satisfaits.

Nous n'avons pas connaissance aujourd'hui d'expériences d'externalisation de ces missions sur un centre de télésurveillance.

2.3.5 Dégradations volontaires et vandalisme

Avant de privilégier telle ou telle technique de détection en vue d'une télévidéosurveillance, il convient de se poser la question suivante :

- un délai de réaction de plusieurs minutes entre la commission des faits et l'arrivée sur les lieux d'une force d'interposition (privée ou publique) est-il acceptable ?

En fonction de la réponse à cette question, il conviendra de choisir entre plusieurs solutions possibles :

Réponse négative (un tel délai n'est pas acceptable) :

- Ne rien faire (les biens sont assurés ou les investissements trop importants par rapport à la valeur des biens)
- Agent de sécurité sur place
- Moyens de vidéosurveillance avec enregistrements pour dissuasion, investigation et dépôts de plaintes éventuels

Par exemple, les musées déploient des tags RFID pour détecter le mouvement/choc/déplacement des œuvres exposées, avec des caméras de surveillance pour vérifier les alarmes et identifier les auteurs : dans la journée, ces caméras sont toujours exploitées dans un PC de Sécurité local et un agent de surveillance est souvent à proximité immédiate des œuvres.

Par contre, la nuit, le conservateur pourra accepter une solution de télévidéosurveillance, car il sait que, avant d'accéder aux œuvres, un intrus aura été détecté en amont et que sa progression sera freinée par des obstacles mécaniques (portes des salles fermées à clés, par exemple), laissant ainsi le temps aux agents de sécurité d'intervenir.

Réponse positive (délai acceptable) :

- Télévidéosurveillance avec intervention des forces de l'ordre
- Éventuellement, installation de moyens de vidéosurveillance complémentaires

Par exemple, des caméras installées sur des mâts dans un quartier où s'opèrent des trafics de drogue peuvent provoquer deux réactions de la part des dealers :

- réorganisation du trafic en dehors de la zone sous vidéoprotection
- vandalisme des caméras

Nous pouvons citer un exemple concret où plusieurs mâts de vidéosurveillance sont sécurisés par télévidéosurveillance par des caméras thermiques opérant en vue plongeante depuis les toits des immeubles voisins.

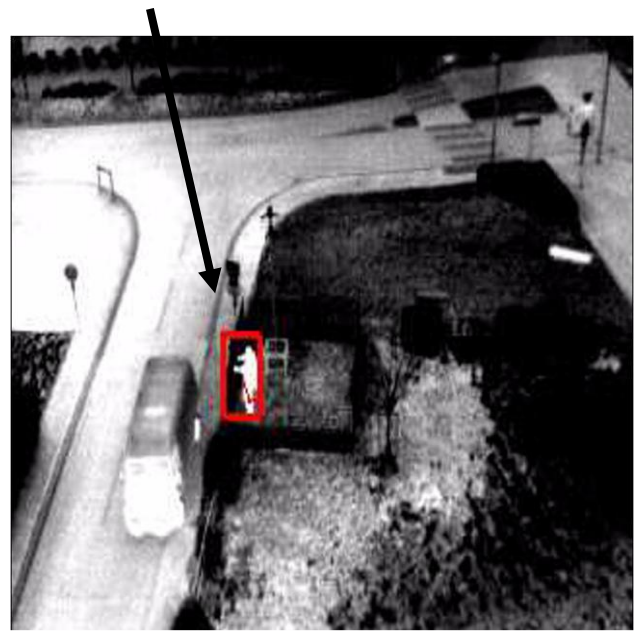
Un no man's land doit être construit autour des mâts pour renforcer leur protection physique et pour éviter les déclenchements d'alarmes intempestifs par les chiens qui viendraient se soulager…

En cas de détection d'intrusion dans le no man's land, l'Analyse Vidéo Intelligente détoure l'intrus dans les images et transmet l'alarme et la vidéo au centre de télésurveillance. Après vérification, l'opérateur alerte la police municipale et la gendarmerie.

Caméra de télévidéosurveillance thermique



Intrus détecté dans le no man's land



Élément protégé en plein jour (dispositif de vidéoprotection urbain, géré par la Ville) :



2.3.6 Espionnage (secteur économique, industriel…)

Les mesures de prévention en matière d'espionnage généralement prises par les entreprises sont :

- Le contrôle des accès (DESFire, biométrie, reconnaissance faciale avec alertes en télévidéosurveillance)
- La détection des intrusions en secteurs sensibles (salles informatiques)
- La télévidéosurveillance des locaux sensibles, par des caméras en installations fixes ou en dispositifs de vidéosurveillance temporaires (caméras cachées)

La principale difficulté pour un opérateur de télésurveillance amené à lever le doute sur une alarme intrusion dans un bâtiment, est qu'il n'est pas en capacité de faire la distinction entre un employé et un espion. Tout au plus, peut-il informer rapidement le client de la présence d'une personne dans un lieu sécurisé et lui transmettre les images sur son téléphone portable ; charge au client de consulter les images et de demander à l'opérateur soit de classer l'alarme, soit d'envoyer la police ou un intervenant privé.

2.3.7 Terrorisme

L'analyse vidéo intelligente permet de détecter des objets abandonnés dans un lieu public sous vidéoprotection. Cette technologie fonctionne, mais elle détecte tout ce qui n'a pas bougé depuis plus d'un certain temps dans une zone donnée, en éliminant le fond (murs et mobiliers).

En pratique, de nombreux cas non anticipés de stationnarité normale viennent polluer le fonctionnement de ses détecteurs automatiques rendant cette technologie complexe à utiliser en télévidéosurveillance privée.

De plus, suite à l'explosion d'un colis explosif réellement abandonné ayant généré une alarme qu'un opérateur aurait classé trop rapidement sans suite, on peut imaginer les conséquences en recherche de responsabilité pour la société de télésurveillance impliquée…

2.4 Détecter les risques incendie, les risques naturels, les risques industriels

2.4.1 Incendie

2.4.1.1 Détecter et lever le doute à l'intérieur

La détection par des détecteurs automatiques d'incendie est réglementaire et normalisée. La télévidéosurveillance permet, dans certaines conditions, de lever le doute sur un déclenchement intempestif d'un détecteur automatique. Mais, dans une pièce enfumée, une caméra avec leds infrarouges produit une image inexploitable. Compte-tenu des responsabilités en cas de mauvaise interprétation, les télésurveilleurs acceptant d'assurer ce type de prestation déclinent contractuellement toute obligation de résultat.

2.4.1.2 Détecter et lever le doute en extérieur

Sous certaines conditions, une détection de départ de feu peut être réalisée en extérieur par des **caméras thermographiques** (caméras thermiques mesurant la température en tout point de l'image) avec :

- alarme par détection de franchissement de seuils de températures (fonctions intégrées dans les caméras)
- et alarme par une Analyse Vidéo Intelligente des images mesurant la croissance et/ou détectant la propagation d'une zone « chaude » (isotherme), signature caractéristique d'un départ de feu.

La télévidéosurveillance est toujours associée à un dispositif de signalisation locale d'incendie sur le site destiné à alerter les personnes éventuellement présentes.

2.4.2 Risques naturels

La détection et la vérification de risques naturels à **évolution lente** pourraient techniquement être gérées en télévidéosurveillance : par exemple, la détection de la montée des eaux sur les berges d'une rivière. Là encore, même si des techniques de détection et de levée de doute vidéo existent, il convient de s'interroger sur la pertinence de l'intervention d'un prestataire privé dans la chaîne de détection et d'information et de mesurer les conséquences :

- d'un délai technique d'information de l'autorité responsable de plusieurs minutes après la détection des faits
- de la possibilité d'une mauvaise interprétation des images par un opérateur « généraliste » par opposition à un agent d'exploitation public ou privé spécifiquement formé et sensibilisé pour ce type de risques

2.4.3 Risques industriels

Généralement détectées par des capteurs industriels, les alarmes liées à la prévention des risques industriels ne peuvent pas toujours être confirmées par des caméras de vidéosurveillance : par exemple, une fuite de gaz n'est pas visible, ni avec une caméra traditionnelle, ni avec une caméra thermique standard.

Il existe toutefois des caméras thermographiques disposant de capteurs spécifiques, fonction du type de gaz à détecter, permettant de visualiser les fuites de gaz : ce type de caméras peut-être relié sans problème en télévidéosurveillance.

D'une manière générale, la télévidéosurveillance peut constituer un moyen de coordination des actions de secours en permettant aux opérateurs de rétrocéder aux services d'intervention des informations utiles comme :

- la localisation précise des secteurs en alarme,
- l'ampleur d'un phénomène,
- l'évolution d'un phénomène d'une alarme à une autre.

2.5 Risques individuels : télévidéosurveillance et vie privée

Les risques liés la personne recouvrent la détection de chute ou de malaise par PTI (équipement de Protection du Travailleur Isolé), les systèmes de téléassistance (médaillons d'appel d'urgence pour personnes âgées ou handicapées), ou encore les bracelets électroniques.

La télévidéosurveillance, lorsqu'elle est possible, permet de qualifier l'alarme, éliminer des fausses alarmes et parfois rendre compte de la gravité d'une situation.

Pour autant, on constate en pratique que la présence de caméras de levée de doute est souvent ressentie comme **intrusive et policière** aussi bien par les personnes concernées par la surveillance que par les intervenants amenés à travailler dans l'environnement vidéosurveillé de la personne.

Ainsi, on a vu des infirmières refusant d'intervenir auprès d'une personne âgée si les soins devaient être dispensés devant une caméra et exiger de pouvoir couper la caméra lorsqu'elles sont présentes.

La miniaturisation et la baisse de coût des caméras thermiques peuvent révolutionner le marché de la télévidéosurveillance individuelle. Par rapport à une caméra traditionnelle ce type de caméra est non intrusif car elle ne permet pas de reconnaître une personne.

Une caméra thermique peut être installée en fixe dans une pièce, mais aussi embarquée dans un Smartphone. Les images produites peuvent parfaitement lever le doute suite à un appel volontaire, sans porter atteinte à l'intimité des personnes.

Associées à une Analyse Vidéo Intelligente, une caméra thermique peut détecter une situation anormale comme la chute d'une personne.



2.6 Proposition d'améliorations

Il apparaît clairement que le temps de réaction du centre de télésurveillance est un élément important de dans la chaîne de détection et d'information. Il est donc nécessaire de généraliser les techniques de levée de doute vidéo optimisant le temps de traitement par les opérateurs, notamment les techniques de « push » et « pull » et l'Analyse Vidéo Intelligente qui produit des images où les risques sont clairement détourés et identifiés dans les images.

Par ailleurs, une fois que l'on s'est assuré que ce travail de vérification/qualification et d'information est effectué dans les meilleures conditions techniques possibles par les centres de télésurveillance privés, on s'interroge alors sur la possibilité d'optimiser également l'intervention des services publics : eux-mêmes sont également dans une problématique d'appels entrants à traiter, de gestion des équipes terrain disponibles et de priorisation des interventions.

En ce sens, la profession convient qu'il serait utile de pouvoir transmettre aux Centres d'Information et de Commandements les images qualifiantes dont dispose le télésurveilleur.

2.7 En synthèse :

Ce groupe de travail a démontré que le choix des bonnes techniques de télévidéosurveillance conduit dans de nombreux cas à une vraie efficacité dans la prévention, la détection et le traitement des risques. L'Analyse Vidéo Intelligente prend aujourd'hui le pas sur les technologies classiques et le couple humain-technologie rencontre des succès indéniables : le nombre d'arrestations en flagrant délit par les forces de l'ordre sur appel télésurveillance après levée de doute en télévidéosurveillance en témoigne.

Comment l'exploitant en bout de chaîne, le centre de télésurveillance, vit-il cette mutation ?

3 GT N°3 – Traitement au PC

3.1 Constitution du GT N°3

Rapporteur : M. Eric VANDER-MAELEN – Securitas

Experts :

- M. Francis SERRANO - Securitas
- M. Garry GOLDENBERG - Open IP video
- M. Philippe DEBAYE - Axis
- M. Patrick LAUNAY - Groupe Scutum
- M. Claude NERI - ESI
- M. Stéphane BIDAULT - TEB

3.2 Introduction

Le métier de télésurveilleur poursuit son évolution naturelle, principalement grâce aux innovations technologiques, qui sont à notre disposition et que la plupart d'entre nous utilisent déjà, la vidéosurveillance à distance par l'IP avec l'analytique en est une.
Si le rythme de transformation de certaines missions du télésurveilleur s'accélère, cette phase de développement de nos activités est logique et déjà anticipée par les professionnels de la sécurité et sûreté à distance.
Le télésurveilleur possède un véritable rôle d'intégrateur, tant par la multitude de protocoles gérés, les réseaux, serveurs, logiciels et matériels divers,… et ce avec le souci de rendre interopérable toute la chaîne pour délivrer le service au client. Le professionnel de la télésurveillance, qui en principe est soumis aux règles APSAD, est vigilant quant à la fiabilité de tous ses systèmes et ceux-ci sont testés régulièrement, aucune faille n'est permise dans ce métier à hauts risques.
L'exigence de nos clients est croissante, tant par la qualité et rapidité du traitement des évènements, que par les « reportings » fournis et l'accès aux informations.
La télévidéosurveillance ne vient pas se substituer aux missions de prestations humaines (agents, personnel du client, etc.) mais les complète et les améliore.

3.3 Effets sur le métier

La mission principale du télésurveilleur est bien de surveiller à distance des personnes et/ou des biens avec les pré-requis suivants :

- Disposer de tous les moyens pour recevoir, analyser, traiter et gérer des informations en provenance de systèmes de détection et de respecter les procédures définies avec le client, en cas d'évènement, incident ou simplement sur demande.
- Mettre en place des « Process » clairs pour le personnel exploitant, définis avec le client pour anticiper chaque incident ou évènement, permettant d'appliquer les mesures adaptées à une situation et/ou nature d'évènement (l'opérateur a une mission prioritaire qui est l'application des procédures et consignes définies au moment de la signature du contrat).
- Acteur principal lors d'un déclenchement d'alarme, il est le lien entre les différents services ou entités, susceptibles d'être sollicités pour intervenir : Agent d'intervention, forces de l'ordre. Ce rôle lui assigne dans la plupart du temps le pilotage des actions engagées et les reportings.

Les technologies et matériels devenant plus fiables, performants, et s'appuyant sur des réseaux permettant le traitement en temps réel, ce n'est pas un scoop en affirmant que le couplage de systèmes de détection avec de la vidéo, est désormais incontournable, voire il devient presque inacceptable de continuer à transmettre des informations « aveugles » aux télésurveilleurs.

3.3.1 La formation de l'opérateur

- Les capacités intrinsèques de l'opérateur pour ces nouveaux métiers (acuité visuelle)
- Comment réagir en situation extrême (violence/agression dans le champ de la caméra)
- Réguler la charge mentale de l'opérateur (1 alarme toutes les 3 à 4 mn) : capacité à maintenir son attention et donc la gestion des poses ; les quarts de 12 heures sont-ils adaptés, faut-il imposer des rotations entre postes ?
- Prévenir du découragement, lié aux fausses alarmes (techniques, humaines, comportementales)
- Prévenir de l'exaspération conduisant à de mauvaises décisions ou des comportements vis-à-vis du client limite.

3.3.2 L'organisation humaine et matérielle des stations de télésurveillance

Les stations de télésurveillance gèrent la sécurité des biens et des personnes de leurs clients, elles sont en possession de nombreuses informations sensibles leur permettant d'appliquer les plans d'actions en cas d'alarme, en particulier des mots de passe, coordonnées de contacts, codes d'accès,….
Elles doivent être en mesure d'assurer un service fiable 24h/24 365j/an quelles que soient les conditions. Les données vidéos et autres informations liées à l'évolution du métier sont autant de risques qu'il faut gérer au quotidien. Pour toutes ces raisons, les stations de télésurveillance sont pour la plupart des centres fortement protégés, tant physiquement par la protection des structures, des alimentations électriques et téléphoniques et des secours qu'électroniquement par le contrôle strict des accès aux locaux, aux données, aux vidéo et aux réseaux IP à fortiori. La traçabilité totale des actions opérateurs, les sauvegardes et l'accès à celles-ci sont une garantie de transparence pour les clients et de preuves le cas échéant. Le backup d'une station sur une station de repli est un élément majeur de la sécurité d'une station. Les opérateurs ainsi que les superviseurs sont les pièces maîtresses du fonctionnement de la station. Ils traitent les évènements d'alarmes reçus par la station. La planification pour une bonne adéquation charge/capacité est également une des clés de qualité du service produit. Grâce aux moyens informatiques, les opérateurs ne traitent en moyenne qu'environ 2% des informations reçues en station, ce qui représente néanmoins un volume important, mais seulement 0,1% de celles-ci font l'objet d'un appel des Forces de l'Ordre. L'APSAD, grâce à la règle R31 pour les stations, est actuellement l'organisme qui garantit le référentiel et le contrôle objectif de l'application des règles édictées.

3.3.3 Les modes de levée de doute vidéo sur alarme :

- Mode Push : Le site « pousse » un clip vidéo qualifiant
- Mode Pull : La télésurveillance « demande » les images aux caméras concernées
- Connexion directe et recherche d'enregistrements
- La détection par la caméra ou la caméra confirme l'alarme avec détourage de l'évènement.

3.3.4 Les prestations vidéo-délivrées

- Cyber guardien
    - Téléactions
    - Contrôle d'accès
    - Accueil
    - …
- Cyber ronde
    - Drones
    - Robots
- Vidéo mobile
    - Plateforme mobile de vidéo surveillance analytique
    - …
- Cyber détection/protection
    - Incendie
    - Individu : Hospitalisation à domicile, Téléassistance, Elsheimer…

3.4 Effets sur la technologie

3.4.1 Pour le télésurveilleur

- multi-flux lié aux attentes qualitatives d'exploitation de l'image
- les outils : la caméra intelligente
- les réseaux et la bande passante
    - Définir les pré-requis sur la sécurité des réseaux
    - Qualité de services réseau IP
    - Risques sur les réseaux (voir R82)
    - Brouillage radio très sophistiqué
- le Cloud : enregistrement local ou centralisé
- la problématique : qualité enregistrée (HD), qualité transmise (basse définition)
- la conception globale : système, réseau, télésurveillance
- Nécessité de définir des règles et préconisations sur la compatibilité des produits (matériels et logiciels) aux organisations des stations de télésurveillance

3.4.2 Pour le constructeur

- Travailler sur une nouvelle approche d'amélioration de l'analyse d'images sur la détection d'anormalités
- Reconnaissance faciale sur obstacle physique
- Lecture de plaques
- Prendre en compte les besoins des télésurveilleurs afin d'améliorer l'interopérabilité les différents systèmes et produits.

Aujourd'hui la technologie n'est pas totalement prête dans l'analyse contextuelle (télé-exploitation). Elle doit encore évoluer.

3.5 Effets sur l'organisation des stations de télésurveillance

La Convention collective contraint les télésurveilleurs à une organisation structurée.
Il faut donc faire évoluer les structures dans ce contexte.

- Utiliser la technologie pour éviter l'interprétation de l'opérateur et donc de limiter le risque d'erreur humaine.
- Estimation des temps opérateur souvent complexe
    - Généraliser l'analyse d'image et détourage car sinon temps d'analyse opérateurs très long. La réception d'image à privilégier à la connexion.
    - Savoir quantifier le temps opérateur. A partir du moment où il y a un détourage l'opérateur se retrouve dans un contexte d'alarme classique.
        - prestation difficile à vendre et à estimer et une exposition aux risques
- Besoin de pré-qualification fiable des évènements
- Difficultés face à la multiplicité des outils en station. Ce qui engendre des soucis de formation, fiabilité, APSAD sur l'enregistrement et la traçabilité.

3.6 Effets Juridique : limite, contexte, ...

La sécurisation des sorties par vidéo est un risque important. Plus orienté sur la sécurité de la personne et non du site. Quelles en sont les limites ? La sécurisation des entrées est possible et plus maitrisable par les télésurveilleurs. Dans ce cas, il s'agit de temps opérateur et donc une charge très ponctuelle en station, d'où difficulté de gérer les présences d'opérateurs face à la Réglementation du travail.

Aujourd'hui, les images peuvent être envoyées vers un autre pays. La réglementation ne l'interdit pas. L'analyse des images peut-être faite à l'extérieur de la station.
Dans l'état de la législation, il faut faire évoluer la levée de doute (clip,…) suite à alarme, l'analyse d'image ainsi que les téléactions, et orienter les télésurveilleurs vers les téléservices. C'est une évolution majeure du métier de télésurveilleur.
Le fonctionnement des télésurveilleurs est basé sur la mutualisation des opérateurs. Quels aspects de la télévidéosurveillance peuvent être mutualisés en poste de surveillance centralisé :

- Téléactions en contrôle d'accès assisté par la vidéo : pas toujours très simple de remplacer le gardien local par un gardien dé-contextualisé (même exemple pour la vidéoprotection urbaine, en CSU en intercommunaux, les opérateurs sont dédiés par commune).
- Vigilance préventive : démarque inconnue par suivi préventif de personnes ciblées, est-ce externalisable ?
- Les missions demandant une attention exclusive d'un opérateur (mono-site) sur une mission donnée : quelle économie d'échelle par la mutualisation ?
    - système automatisé, gestion par exception ?
    - des opérateurs en frontal avec une densité suffisante pour rendre le service ?

Les assureurs ont-ils des exigences particulières à formuler sur la mutualisation ? Approche à avoir auprès des assureurs pour mettre des contraintes adaptées.

3.7 Formation des acteurs de la télévidéosurveillance

Les services des télésurveilleurs professionnels sont très encadrés. Seuls la fiabilité et le contrôle de chaque étape de nos procédures et actions entreprises donnent confiance aux clients, et permettent d'obtenir des résultats.
Si nous sommes assurés, que le télésurveilleur a largement sa place dans le dispositif de sécurité intérieure, néanmoins de par l'utilisation et influence forte de la technologie, le professionnel de la télésurveillance est souvent un promoteur de nouvelles solutions et innovations de services à distance, la télévidéosurveillance en est l'exemple.
Il faut donc aborder la formation sur l'ensemble de la chaîne, et s'assurer que les différents processus soient étanches pour des raisons de sécurité. Chaque étape du processus de télésurveillance doit être encadrée afin que l'accès aux données, l'exploitation des données soient limités à une population identifiée.

Il faut former les acteurs à l'application stricte des processus. Il faut commencer par la définition des processus avant de créer les modules de formation.

3.7.1 Formation Avant vente

Avant-vente technique

- Étude,
- Conception,
- Architecture.

Avant-vente commerciale

- Discours,
- Contractualisation, promesse de valeur, mesure conservatoire en cas de panne,
- Engagements.

Installation

- Réglementation, sécurité,
- Règles de l'Art,
- Habilitations,
- Agréments, certifications constructeurs,
- Contrôles, mesures.

3.7.2 Opérateurs télévidéosurveillance

Pré-requis :

- Titulaire du CQP (4 semaines de formation) : formation type agent de sécurité d'une société privée,
- Carte professionnelle (déclaration CNAPS),
- Formation théorique (15j) législation, réglementations, loi, matériel, outils,
- Formation pratique (15j) en binôme avec un opérateur confirmé.

Formation opérateur à la télévidéosurveillance :

- Définir le périmètre de la vidéo, (même cheminement que pour la télésurveillance classique),
- Formation outils spécifiques (théorique et pratique),
- Quel est le rôle de l'opérateur, et comment gérer les situations auxquelles l'opérateur pourra être confronté,
- Interprétation des scènes (levée de doute, tracking, ronde, …),
- Comment réagir en situation extrême (violence/agression dans le champ de la caméra). Comment préparer et/ou accompagner l'opérateur dans la décharge du stress,
- Prévenir de la perte de vigilance (processus, alerte, organisation des postes de travail, type de séquencement des opérations réalisées par l'opérateur, charge mentale, présentation des images),
- 2 solutions :
  - écrans avec vidéo permanente = Inutile
  - gérer le mode alarme, c'est-à-dire alerter l'opérateur sur évènement, rend son action plus performante
- Savoir faire le lien entre un plan et l'espace du site,
- Capacité de l'opérateur à s'adapter au passage d'un client à un autre,
- Savoir reporter la situation efficacement de l'opérateur vers les FO, intervenant, …
- L'analyse comportementale vidéo est à prendre en compte dans la formation des opérateurs. Pour détection des situations à risque.

Formation des managers des opérateurs :

- Détection de défaut opérateur (vigilance, stress, difficulté, …),
- Gestion/Relation humaine (en particulier sur la détection des effets secondaires à situation extrême). Voir site médecine du travail (Web), psychologue…
- Approche technique des solutions.

Formation après-vente (service client, techniciens,…) :

- Télémaintenance,
- Supervision,
- Téléparamétrage,
- Mesure de qualité de service, optimisation.

3.8 Effets sur la réglementation

Nos métiers se sont toujours appuyés sur des normes et des certifications, dès que la maturité des activités le permettait.
C'est un moyen de structurer le marché, de le faire monter en compétence, et par définition d'augmenter la qualité des prestations vers nos clients finaux.
Les exigences de nos règles, sont en fait un garde-fou contre les dérives de certaines entreprises qui font "fi" de toute volonté de professionnaliser nos activités.
Nos métiers sont bien trop sensibles, pour laisser n'importe quel acteur agir, sans contrainte, ni engagement, ni règle.
Notre démarche est de non seulement respecter les lois, les règles qui encadrent nos métiers, mais aussi de participer à leur évolution et révision, quand cela est nécessaire.
La rapidité et la progression des technologies est telle, que nous sommes vigilants pour ne pas intégrer de nouveaux services ou produits, sans au préalable nous être assurés, que ces derniers s'intègrent bien dans nos offres, et qu'il seront exploitables.
Notre souci premier, est bien de créer de la valeur pour nos clients, et nos entreprises.
Sans qualité, sans règles, sans engagements, il est difficile de faire bien…

Si la Loi N°83-629 du 12 juillet 1983, règlemente les activités de sécurité privée, nous nous appuyons également sur des organismes tels que le CNPP, pour encadrer et règlementer nos activités de sécurité électronique, et dans ce cadre précis de la vidéo, tant pour l'installation, que le report d'images à distance, leur traitement, analyse et exploitation, c'est une garantie de professionnalisme.
Les règles R31 (télésurveillance) et R82 (installation vidéosurveillance) ont déjà fait l'objet de révisions, et c'est une preuve qu'elles essayent d'accompagner la demande du marché, tout en respectant un engagement de qualité et de professionnalisme.
Cependant, la télévidéosurveillance n'est pas encore traitée dans son ensemble, et c'est une demande de notre syndicat professionnel.
L'objectif n'est pas de rajouter des contraintes, mais de bien définir le service, et les services associés à la gestion et traitement des images à distance (supervision, interopérabilité, télémaintenance, téléparamétrage, etc.), à savoir :

- Archivage/traçabilité à affiner
- Traçabilité : attention à la limite de normalisation (volume par exemple)
- Ajoute un module sur la partie gestion des images et des consignes spécifiquement liées à la vidéo.
- Automatisation des actions opérateurs & analyses d'images
- Garder la notion de module pour les cas de CSU déporté
- Imposer l'exploitation en centrale de télésurveillance avec des infrastructures techniques et humaines backupées, une exploitation tracée, des engagements sur la qualité de service.
- Formation minimum requise pour les techniciens, opérateurs vidéo
- Etc..

Dans le cadre de la levée de doute, l'outil que représente la vidéo et notamment la vidéo-analytique sur IP est une réelle opportunité pour les professionnels, de disposer d'informations plus fiables, en temps réel, permettant de prendre des dispositions immédiates et participer à éviter l'incident.
Il existe cinq approches dans la levée de doute :

- L'identification avec mot de passe,
- L'audio,
- La double-détection ou la corrélation d'alarmes,
- L'intervention par un agent de sécurité,
- La vidéo.

Bien entendu, les télésurveilleurs professionnels combinent souvent plusieurs solutions, en fonction des risques et de la qualité de l'information recherchée.
La télévidéosurveillance sur IP est de loin, la solution la plus intéressante :

- Images en temps réel,
- commandes ou pilotage à distance (haut-parleurs, portes, SAS, éclairage, tracking, etc.)

Nous pouvons grâce à ce service, disposer d'informations fiables et sûres et transmettre aux autorités des données précieuses dans le cadre de leur mission.
La disposition qui règlemente l'appel aux forces de l'ordre, sera encore mieux appliquée.

3.9 En synthèse :

L'intégration de la technologie chez les télésurveilleurs est un incontournable depuis de nombreuses années. Elle impose de la rigueur, la mise en place de process précis et la formation de tous les acteurs. Ces évolutions permettent aux Opérateurs de télésurveillance de réagir aux alarmes avec le plus de discernement possible.

Pour une meilleure efficacité, les constructeurs doivent intégrer les besoins des télésurveilleurs dans leurs démarches. Leurs technologies doivent être innovantes, fiables et interopérables.

L'intervention humaine sur alarme est un complément indispensable de la télévidéosurveillance.

4 GT N°4 – Intervention

4.1 Constitution du GT N°4

Rapporteur : M. Christophe ROMAIN – Directeur Corporate Securitas Télésécurité

Experts :

- M. Vincent BONNARD – Directeur Commercial Securitas Télésurveillance
- Raphaël MAURO - GIP2 / EPSITRONIC

4.2 Situation actuelle du marché

4.2.1 Nombre d'interventions

Concernant le marché des interventions en France, aucune donnée officielle n'est disponible. En effet, le marché des interventions représente une composante de la surveillance humaine et seules quelques sociétés se sont spécialisées dans ce domaine d'activité.
Cependant et en recoupant les données des principaux acteurs, nous pouvons estimer que ce marché représente environ 600 000 interventions physiques par an.
A noter que ce marché est en constante baisse avec des raisons que nous évoquerons dans les chapitres suivants.

4.2.2 Plus de 90% des alarmes déclenchées en France sont injustifiées

La nature même du déclenchement d'une alarme entraîne automatiquement un taux d'erreurs et d'interprétations de la part de l'opérateur qui a généralement pour conséquence la demande d'un déplacement d'un agent de sécurité mobile.
De nombreuses alarmes sont en effet déclenchées par des évènements jugés sans risque tels que des erreurs d'utilisation, une méconnaissance des consignes de télésurveillance de la part du personnel ou de tiers (livreurs, ménage, services annexes…), un mauvais paramétrage du système en place ou tout simplement une porte ou une fenêtre ouverte.
La simple analyse ne permet pas de différencier rapidement et facilement les alarmes intempestives des vraies.
Par défaut, l'opérateur de télésurveillance demande donc la réalisation d'une levée de doute visuelle facturée entraînant ainsi la plupart du temps un coût supplémentaire ainsi qu'une insatisfaction du client.

4.2.3 Gendarmerie Nationale / Police Nationale / Polices Municipales / Sociétés de sécurité privées

Le redéploiement récent de la police-gendarmerie a pour objectif de gagner en cohérence et en efficacité en faisant coïncider les territoires d'actions des deux forces principales. En effet, l'urbanisation redessine les bassins de délinquances et l'harmonisation des rôles est primordiale afin d'assurer l'efficacité de chacun.

En plein développement, les polices municipales ont également évolué dans leurs missions et se transforment progressivement en une force de police mutualisée au service des intercommunalités.
La coordination sur le terrain avec la police-gendarmerie est donc primordiale afin de coordonner les missions de chacun à travers l'organisation d'opérations de sécurisation conjointes.

Au même titre que les polices municipales et parce que les sociétés de sécurité privée ont acquis de la légitimité grâce à la création du CNAPS (Conseil National des Activités de Sécurité Privée : date de démarrage : 1er janvier 2012), ce secteur privé est devenu un élément incontournable de la vie quotidienne des citoyens.
A ce sujet, les 200 000 agents de sécurité privée représentent un levier considérable d'action sur lequel peuvent s'appuyer les forces publiques sans verser dans la confusion des genres, ni la dilution du service public.
Cependant, aucune politique transversale visant à coordonner les actions de chacun n'a été entreprise à ce jour, chaque force en présence restant sur son domaine juridique « espace privé – espace public ».
La volonté des pouvoirs publics, à travers l'évolution de la loi de 1983, devrait permettre de dynamiser et d'influer une synergie positive visant à redéfinir les domaines de chacun tout en accordant à l'ensemble des acteurs un même cadre juridique.

4.3 Définition et perception par l'utilisateur

4.3.1 Définition de l'intervention

La définition de l'intervention physique proprement dîte fait souvent référence à une notion associée beaucoup plus imagée : la levée de doute.
En effet et par rapport à la législation en vigueur, l'opérateur de télésurveillance a besoin de confirmer visuellement la nature du déclenchement de l'alarme avant de prévenir les forces de l'ordre.

Définition 1 : « En cas de déclenchement de l'alarme d'un site sous surveillance électronique, un agent de sécurité mobile est immédiatement dépêché sur place à la demande de l'opérateur de télésurveillance afin d'y effectuer une levée de doute. Rendu sur place à bord de son véhicule, l'agent de sécurité mobile effectue une ronde extérieure ou intérieure. Si l'incident est avéré, la mission de l'agent de sécurité mobile est alors de contacter l'opérateur de télésurveillance qui, soit avertira les services compétents, soit avisera le client par téléphone.
L'agent de sécurité mobile ne quitte le site qu'une fois la situation sous contrôle. »

Définition 2 : « Une intervention est nécessaire pour vérifier sur place l'origine de l'alarme reçue par l'opérateur de la station de télésurveillance. C'est ce qu'on appelle communément la levée de doute. L'intervention est déclenchée et exécutée en fonction de consignes préalablement mises au point avec le client dans les délais les plus réduits possibles par des équipes motorisées et pré positionnées par secteur géographique. Arrivé sur place et après une ronde de reconnaissance, l'intervenant prend les mesures conservatoires qui s'imposent. »

Définition 3 : « La levée de doute est l'opération consistant à vérifier la matérialité d'un évènement ayant provoqué le déclenchement d'une alarme. Préalable indispensable à l'appel des forces de l'ordre, la levée de doute est majoritairement opérée par une personne physique, dans la plupart des cas un agent de sécurité. L'agent de sécurité effectuera une ronde sur site et procédera aux vérifications idoines qui attesteront du bienfondé ou pas de l'alarme reçue. »

4.3.2 Rappel législatif et contraintes (véhicule non prioritaire, conditions météo…)

Les contraintes liées à un déplacement sur site d'un intervenant ne sont généralement pas prises en compte par les clients, volontairement ou pas, voire sont inconnues du grand public :

- Véhicule d'intervention non prioritaire,
- Aléas de la circulation,
- Conditions météorologiques,
- Diverses manifestations,
- Moyens mutualisés d'intervention à l'ensemble des clients sur un même secteur géographique.

Il va de soi que le délai d'intervention doit être le plus rapide possible afin de limiter les dommages sur site et dans certains cas, mettre en échec toute tentative d'effraction, mais il est utile de rappeler ici que les agents de sécurité en charge de ces interventions n'ont en aucun cas pour mission d'interpeller les malfrats.
Le rôle de l'intervenant consiste :

- à s'assurer de la véracité des alarmes,
- permettre à l'opérateur de la station de télésurveillance de clôturer les alarmes reçues,
- rétablir le bon fonctionnement normal du système de détection électronique en place,
- assurer la mise en place des mesures conservatoires en cas d'incident.

Au niveau de la responsabilité et des engagements demandés vis-à-vis de la société intervenante, il ne peut s'agir que d'une obligation de moyens et non de résultat compte tenu des éléments développés ci-dessus. C'est en ce sens que la jurisprudence se prononce régulièrement : « la société de gardiennage chargée d'assurer la prestation d'assistance est tenue d'une obligation de moyens et qu'il lui incombe à ce titre d'adapter ses moyens d'intervention aux différents engagements qu'elle a souscrits pour assurer à ses abonnés un traitement satisfaisant des demandes d'intervention qu'ils lui adressent » (arrêt du 06 mars 2007 - CA Montpellier n°06/00997).
Ceci entraîne de facto l'inassurabilité de l'obligation d'intervention de résultat.

4.3.3 Remise en cause

- de l'utilité et de l'efficacité de l'intervention par l'utilisateur final (délai d'intervention, coût de l'intervention),

Dans le domaine de la sécurité, l'intervention est souvent assimilée à un phénomène d'urgence et prioritaire sans tenir compte de la mutualisation des forces humaines sur un même secteur géographique. Chaque client a le sentiment de disposer de moyens humains totalement dédiés à son site et qu'un intervenant attend l'ordre de l'opérateur de télésurveillance dans un endroit géographiquement proche du sien.
Ainsi, le délai d'intervention et donc, la nature même de l'intervention, sont souvent remis en cause par l'utilisateur final, à la fois au niveau de l'efficacité mais également au niveau de la facturation.

- de l'efficacité du système en place proposé,

Une fois arrivé sur place, la cause du déclenchement d'alarme est recherchée par l'intervenant dans la limite de ses moyens (mise à disposition des moyens d'accès, configuration géographique, végétation, éclairage public, superficie du site…) et de ses compétences.
Les caméras ou détecteurs installés sur site doivent être configurés afin de répondre précisément aux risques détectés lors de l'audit et la visite préventive du site lors de l'évaluation des risques. A ce titre, le système proposé et accepté par le client doit être adapté.

- de la réputation de l'installateur,

Pour des sites complexes ou étendus, le matériel installé doit être configuré de telle manière à ce que l'opérateur de télésurveillance puisse guider l'intervenant sur l'origine du déclenchement d'alarme. Dans le cas contraire, l'intervention risque d'être inefficace et peut entraîner des conséquences néfastes dans la compréhension de l'incident.

- de l'organisation de la société intervenante.

Tous ces éléments sont donc une source d'insatisfaction et sont susceptibles de remettre en cause la nature même de l'intervention humaine.
Les conditions économiques avec une baisse constante constatée sur le prix facturé de l'intervention ont entraîné la disparition de plusieurs centaines de sociétés de sécurité privée, accentuée avec la mise en place des contrôles CNAPS.

4.4 Types d'interventions

4.4.1 Intervention humaine

Secteur d'activités	Type d'interventions		
	Humaine		
	Avantages	Limites	Commentaires
Particulier urbain	Délai	accès et embouteillage	Hormis les VIP, intervention humaine appelée à disparaitre compte tenu de l'évolution du prix à la baisse
Particulier rural	Sauvegarde immédiate des lieux - Analyse et prise de décisions adaptées	délai et repérage	cout d'intervention non répercuté sur le prix de vente
Particulier résidence secondaire	Sauvegarde immédiate des lieux	délai et repérage	Hormis les VIP, intervention humaine appelée à disparaitre compte tenu de l'évolution du prix à la baisse et des coûts de fonctionnement à la hausse
Particulier SAP	Délai	Responsabilité engagée en cas de dommages corporels	Notion de responsabilités juridiques en cas de décès ou d'invalidité due à la notion de délai d'intervention
Artisan / commerce de proximité	Sauvegarde immédiate des lieux	zone de couverture	Concurrence de l'intervention réalisée par le personnel interne
Chaîne de magasins	Sauvegarde immédiate des lieux	zone de couverture	Intervention low cost souvent en extérieur
PME-PMI	Sauvegarde immédiate des lieux	zone de couverture	Intervention utile compte tenu de la spécificité de chaque site. Réelle valeur ajoutée.
Site industriel / de production	Sauvegarde immédiate des lieux	zone de couverture	Souvent proposer des rondes aléatoires avec et/ou sans contrainte horaire
Site sensible et/ou Seveso	idem - application des mesures de sécurité	zone de couverture	Souvent proposer des rondes aléatoires avec et/ou sans contrainte horaire
Transport & Logistique	Sauvegarde immédiate des lieux	zone de couverture	Intervention low cost compte tenu de l'activité du client
Zone d'activité / industrielle	mise en place rapide - efficace car visible	le cout	Intervention utile et économiquement viable dans le cadre d'une mutualisation
Commune / Collectivité	bon alternatif à la police municipale - très dissuasif	voie publique et mission	Intervention utile et économiquement viable dans le cadre d'une mutualisation. Attention au rôle dédié à la PM

4.4.2 Intervention Vidéo

Secteur d'activités	Type d'interventions		
	Vidéo		
	Avantages	Limites	Commentaires
Particulier urbain	immediat	le budget	la meilleure solution !
Particulier rural	immediat	couverture de transmission	sous réserve d'une couverture réseau fiable, la meilleure solution avec intervention directe des forces de l'ordre
Particulier résidence secondaire	immediat	couverture de transmission	sous réserve d'une couverture réseau fiable, la meilleure solution avec intervention directe des forces de l'ordre
Particulier SAP	Réactivité	Respect de la vie privée	Législation concernant l'utilisation des images pas adaptée
Artisan / commerce de proximité	immediat	pas sur place	solution à terme avec un équipement par branche d'activité
Chaîne de magasins	immediat	pas sur place	la meilleure solution à travers un équipement fiable et standardisé
PME-PMI	immediat	pas sur place	complément vidéo approprié dans le cadre de certains secteurs d'activité ou certaines zones sensibles
Site industriel / de production	immediat	pas sur place	Opportunité de nouvelles technologies type drone
Site sensible et/ou Seveso	immediat	pas sur place	Opportunité de nouvelles technologies type drone
Transport & Logistique	immediat	idem - la superficie à vidéo surveiller et la définition des cameras	complément vidéo approprié dans le cadre de certains secteurs d'activité ou certaines zones sensibles (carburant)
Zone d'activité / industrielle	le cout	voie publique	Opportunité de nouvelles technologies type drone sur zones privatives
Commune / Collectivité	le cout	voie publique	Investissements lourds mais en pleine expansion

4.4.3 Intervention humaine et vidéo

Secteur d'activités	Type d'interventions		
	Humaine & Vidéo		
	Avantages	Limites	Commentaires
Particulier urbain	sauvegarde des lieux	le cout	Economiquement et compte tenu de l'évolution des technologies B to C , le particulier urbain se transforme en opérateur de TLS et en intervenant
Particulier rural	sauvegarde des lieux	le délai d'intervention	Economiquement, difficile à commercialiser
Particulier résidence secondaire	sauvegarde des lieux	le délai d'intervention	Prestations humaines plutôt consacrées à la mise en place d'un agent de surveillance ne cas de dégradations
Particulier SAP	Solution idéale sur le papier !	le coût	Economiquement non viable sauf client VIP
Artisan / commerce de proximité	sauvegarde sur place - levée de doute immédiate	le cout	Economiquement difficile à proposer
Chaîne de magasins	sauvegarde sur place - levée de doute immédiate	le cout	offre standardisée et de masse afin d'être économiquement intéressant
PME-PMI	sauvegarde sur place - levée de doute immédiate	le cout	offre à établir avec optimisation nécessaire
Site industriel / de production	sauvegarde sur place - levée de doute immédiate	le cout	association de vidéo ciblé et de rondes techniques ou de contrôle
Site sensible et/ou Seveso	sauvegarde sur place - levée de doute immédiate	le cout	association de vidéo performante et de rondes techniques. Investissement lourd mais nécessaire
Transport & Logistique	sauvegarde sur place - levée de doute immédiate	le cout	Compromis économiquemen viable
Zone d'activité / industrielle	efficace si report vehicule zone	le cout	Mix efficace. Démarche commerciale compliquée
Commune / Collectivité	bon alternatif à la police municipale - très dissuasif	voie publique	Efficace sous condition d'une bonne coordination entre privé et public

4.5 Évolution du marché

4.5.1 Contraintes financières (augmentation du carburant, baisse du prix moyen de l'intervention, augmentation des charges, pénalités de + en + appliquées)

Le marché de l'intervention humaine en France est en régression depuis plusieurs années. Ce phénomène a été accentué par plusieurs évènements :

- Augmentation du prix du carburant (+57% entre janvier 2004 et juin 2014 source INSEE).
- Augmentation des frais de carrosserie et plus globalement des frais de réparation des véhicules.
- Baisse du prix de l'intervention facturée (environ -30% environ en 10 ans).
- Mise en place de plus en plus fréquente de délais d'intervention imposés, voire de pénalités en cas de non respect.
- Politique urbaine des municipalités visant à restreindre ou exclure les véhicules des centres-villes entraîne des surcoûts difficilement répercutables chez le client et des délais d'intervention allongés (frais de parkings, changement de véhicule une fois arrivé sur le secteur de l'intervention – 2 roues – vélo électrique, véhicule électrique avec frais de garage).

4.5.2 Contraintes géographiques (répartition nationale des sociétés de sécurité privées, apparition de zones « blanches »)

Les sociétés de sécurité privée, et plus particulièrement celles qui possèdent plusieurs activités, sont confrontées depuis plusieurs années à une stagnation du marché de la surveillance avec des marges bénéficiaires en baisse constante.

L'activité la plus touchée par les restructurations est l'intervention sur alarme et ce, pour plusieurs raisons :

- Facturation aléatoire et hypothétique de cette activité (facturation à l'unité au « coup par coup » avec de plus en plus de contraintes des donneurs d'ordre telles que des pénalités appliquées en cas de dépassement de délai).
- Activité à risques entraînant des coûts de fonctionnement importants (entretien général du véhicule d'intervention, accidentologie forte, assurances, environnement à risque pour l'intervenant…)
- Recherche en responsabilité de plus en plus fréquente de la part du donneur d'ordre entraînant une obligation pour la société de sécurité privée à faire appel à des cabinets juridiques spécialisés ou à une organisation interne qui entraîne des coûts de fonctionnement le plus souvent à fond perdu.

Ceci entraîne inexorablement un abandon de cette activité au profit de domaines plus rentables comme l'installation de matériel ou la télésurveillance.

Certaines zones géographiques deviennent donc des « zones blanches » sur lesquelles plus aucune société de sécurité privée n'effectue les missions d'intervention avec des délais raisonnables.
Le marché de l'intervention s'oriente donc naturellement vers des solutions gérables à distance et dans cette perspective, les moyens déportés de détection et d'analyse qui servent à vérifier le bien-fondé des alarmes reçues sont en plein développement.

4.6 Perspectives d'avenir

4.6.1 Nouvelles technologies

- Vidéo

La vidéo se propose de visualiser en « live » et à distance des images reçues des matériels vidéo équipant les sites protégés.
De plus, cette technologie en constante évolution, constitue un mode de levée de doute fiable et adapté à un grand nombre d'usages.
L'opérateur de télésurveillance effectue lui-même la levée de doute et prend donc la responsabilité d'appeler ou pas les forces de l'ordre.
Le rôle de l'opérateur est donc primordial et son analyse est beaucoup plus subtile qu'une analyse binaire qui consiste à demander à un intervenant de compléter l'étude de la situation grâce à une levée de doute.
En cas d'un état de flagrance évident, l'opérateur appelle immédiatement les forces de l'ordre qui peuvent ainsi agir rapidement et constater idéalement un flagrant délit.

- Auto surveillance

Les nouveaux systèmes présentés actuellement sur le marché, notamment pour les particuliers, proposent au client d'assurer à la fois le rôle d'opérateur de télésurveillance en visualisant en direct sur un support adapté le lieu télésurveillé (ordinateur, tablette, Smartphone) mais également d'assurer le rôle d'intervenant en réalisant lui-même la levée de doute ou par l'intermédiaire d'un tiers non professionnel (voisin, ami, membre de la famille…).
C'est la solution low cost par excellence mais également celle qui attire de plus en plus de clients grâce à son aspect hightech.
Le client a l'impression de maîtriser l'ensemble de la chaîne sécuritaire et réduit ainsi les coûts de fonctionnement en assurant lui-même l'ensemble des tâches.

- Combinaison de moyens (techno + humain)

L'utilisation combinée de la vidéo et de l'humain reste préférable dans un certain nombre de situations.
En effet, il est souvent nécessaire de recourir à une association de moyens, ne serait-ce que pour palier à un éventuel défaut de transmission d'images (images dégradées, qualité fluctuante du réseau, communication impossible…).
De plus, certains sites sensibles ou avec un environnement complexe exigent une combinaison de moyens pour apporter une véritable réponse sécuritaire en fonction des besoins, de la nature du risque et/ou des valeurs à protéger.

- Drones

Le nouvel « outil » du futur pressenti sur le marché des interventions levées de doute est le drone.
Le drone est à la mode et envahit l'audiovisuel public en créant un nouvel angle de vue enrichissant.
Cette nouvelle technique est issue de l'usage militaire et les applications civiles tendent à se développer. La surveillance préventive et les missions liées à la sécurité privée semblent être à court terme la prochaine cible de ce marché en pleine construction.
Les constructeurs et utilisateurs de drones s'organisent à travers la création d'une fédération nationale, la FPDC (Fédération Professionnelle du Drone Civil).
Le seul bémol demeure l'adaptation de la législation française et européenne à ce nouvel outil qui se heurte pour l'instant au cadre réglementaire de l'aviation civile (DGAC) mais également dans la formation et la qualification des « télépilotes » en charge de l'utilisation du drone.
Quel statut pour cette nouvelle profession en charge de la détection à distance de toute tentative d'effraction sur un site ?
Le télépilote sera-t-il intégré dans la station de télésurveillance au même titre qu'un opérateur de télévidéosurveillance ?
En fonction de l'évolution de la réglementation, les professionnels de la sécurité privée devront également intégrer cette nouvelle technologie qui sera, soit complémentaire à un système existant avec intervention humaine possible sur le lieu même du déclenchement d'alarme (agent de surveillance en poste sur une zone d'activité ou industrielle avec intervention rapide en équipe avec le télépilote qui le guidera à distance), soit permettant de prévenir directement les forces de l'ordre pour constater un flagrant délit.

4.6.2 Objectifs

- Réduire les coûts et les interventions générées par les alarmes intempestives

La levée de doute par télévidéosurveillance permet de limiter les coûts d'intervention d'un agent de sécurité, notamment lors d'interventions inutiles en cas d'alarmes intempestives.

- Simplifier le circuit de décision

La levée de doute par télévidéosurveillance présente l'avantage d'être efficace et rapide grâce à une vision en direct de la situation sur place. C'est à priori le seul moyen qui permet de faire appel immédiatement aux forces de l'ordre à l'aide de numéros dédiés qui raccourcissent le délai de transmission.

- Augmenter l'efficacité de l'intervention en privilégiant le flag

La levée de doute par télévidéosurveillance doit permettre d'apporter une preuve certaine de l'évènement, constatée en temps réel et enregistrée.
La traçabilité et la consignation de preuves sécurisent les démarches ultérieures du client auprès de son assureur et de la justice.
En cas de qualité d'images qui ne permet pas forcément l'identification des personnes, la levée de doute par télévidéosurveillance permet de vérifier la matérialité de l'alarme et de conforter l'opérateur de télésurveillance dans sa décision.

4.7 En synthèse :

Intervenir physiquement sur un déclenchement d'alarme à la demande du télésurveilleur semblait jusqu'à présent la solution majoritairement et historiquement la plus répandue sur le marché de la sécurité.
Les évolutions, liées notamment à l'environnement défavorable des contraintes imposées par les acteurs de ce marché, ont rendu ce secteur extrêmement fragile financièrement.
En conséquence, les sociétés de surveillance se désengagent massivement d'un marché devenu à risques et de moins en moins rentable.
Parallèlement, l'émergence de la télévidéosurveillance oriente le marché de l'intervention vers la levée de doute à distance.

Est-ce une tendance lourde et irrémédiable ?
Les prescripteurs seront-ils prêts à en accepter les conséquences, notamment financières en terme d'investissement ?
Les solutions technologiques répondront-ils exhaustivement aux attentes du client final ?
Quel est l'avenir à moyen terme des sociétés d'interventions avec cette orientation technologique ?
Comment gérer l'abandon des clients qui continueront à solliciter les interventions humaines ?
Les années à venir nous le diront très rapidement.

5 Conclusions

Dans un monde futur et forcément idéal, la levée de doute par télévidéosurveillance permettra à un opérateur déporté :

- De prendre connaissance en temps réel et sans déperdition de la situation sur place grâce à des détecteurs audios, vidéos, sensoriels…
- D'analyser rapidement la situation grâce à la transmission d'images qui seront analysées préalablement par le logiciel intégré à la caméra et qui ne transmettra les images paramétrés qu'en fonction de l'environnement immédiat et spécifique.
- D'agir immédiatement en entrant en communication directe avec les personnes suspectes sur place.
- De transmettre en temps réel les images aux Forces de L'ordre et/ou à des équipes de sécurité privée qui pourront intervenir rapidement et conjointement directement sur place.
- De guider à distance les forces de l'ordre et/ou les sociétés de sécurité privée afin de prévenir tout risque d'aggravation ou de constater le flagrant délit.
- De suivre à distance les personnes suspectes grâce à l'accès aux caméras de surveillance présentes sur les lieux publics (communes, réseaux routiers, gares, aéroports, parkings, etc.) ainsi que les drones de surveillance.

Pour cela, plusieurs améliorations devront intervenir dans les années futures tant sur le plan technique que juridique :

- L'évolution de la qualité des images : jour/nuit, contrejour, résolution, nombre d'images par seconde,
- l'évolution des techniques de transmissions d'images au niveau des flux et du réseau garantissant la rapidité et la sécurité des données transmises,
- l'évolution de la législation en permettant l'accès du domaine public aux entreprises de sécurité privée,
- l'évolution vers un consensus dans les systèmes de transmission et d'analyse d'images à l'ensemble des intervenants privés et publics afin d'inter-réagir efficacement sur le lieu choisi.

L'agent d'intervention évoluera quant à lui vers un rôle beaucoup plus centré sur la dissuasion et la connaissance personnalisée de son secteur géographique permettant ainsi d'anticiper tout acte de malveillance grâce à sa présence sur le terrain et à l'accès en temps réel des images analysées préalablement par l'opérateur de télé vidéosurveillance.

Il ne sera plus l'acteur low cost par défaut qui constate le délit ou la tentative d'effraction mais un maillon essentiel de la chaîne de prévention sécuritaire en liaison permanente avec les installateurs de systèmes de protection et les forces de l'ordre de son secteur géographique.
Il sera financé en amont par l'ensemble des clients adhérents grâce à des subventions locales, régionales (région, département communauté de communes ou agglomérations urbaines…) ou privées à travers des collectivités publiques ou des associations privées (zones d'activités ou industrielles, chambres de commerce et d'industrie, associations de commerçants, zones pavillonnaires ou résidentielles…).
Sa valeur ajoutée sera donc essentiellement axée sur la proximité et la prévention.

En cas de nécessité, l'intervention physique ne représentera plus un coût supplémentaire vis-à-vis du client mais un complément de prestation inclus dans la prestation de sécurité globale.
L'intervention ne sera plus vécue comme une action servant à constater le sinistre mais comme une présence rassurante en attendant l'arrivée du client.



usp TECHNOLOGIES

24, rue Firmin Gillot 75015 Paris