

Ufficio studi ed analisi di settore



**Libro bianco CoESS
sulla sorveglianza elettronica:
lettura italiana**

Collana quaderni

Maggio 2010

Numero 5

Ufficio studi ed analisi di settore



FederSicurezza

**Libro bianco CoESS
sulla sorveglianza elettronica:
lettura italiana**

Centrali di Telesorveglianza: Una Funzione Centrale nel Panorama della Sicurezza Europea, Oggi e in Futuro

La pubblicazione di questo “Libro Bianco” da parte di CoESS, la Confederazione Europea dei Servizi di Sicurezza, e della presente edizione italiana curata da Federsicurezza, giunge in un momento particolarmente delicato per i futuri assetti del settore.

In Europa come in Italia, il legislatore è impegnato nello sforzo di definire nuovi ambiti e ruoli per il settore dei Servizi Privati di Sicurezza, cercando di contemperare i primari interessi di Pubblica Sicurezza insiti in tali servizi, con la natura commerciale delle imprese che vi operano, traguardando nel contempo un processo di armonizzazione a livello europeo che appare inevitabile, almeno in un'ottica di medio periodo.

Ebbene, in questo contesto le Centrali di Telesorveglianza costituiscono “terra di frontiera” in quanto rappresentano l'elemento di giunzione tra la tecnologia ed i servizi di vigilanza che, troppo spesso, vengono definiti “tradizionali” semplicemente perché svolti da personale (qualificato) piuttosto che da un “occhio elettronico”.

Le Centrali di Telesorveglianza, al contrario, sono il luogo dove i benefici dei sempre più sofisticati ed innovativi strumenti elettronici di sicurezza e controllo, vengono resi disponibili per servizi di sicurezza sempre più efficaci ed affidabili.

Questo documento ambisce a dare a tutte le parti interessate, prime tra tutte le Istituzioni Pubbliche, una completa rappresentazione del settore specifico della Telesorveglianza, affinché l'importantissimo ruolo svolto dalle Centrali di Telesorveglianza possa essere giustamente valorizzato, anche alla luce della riconosciuta eccellenza dell'Italia, soprattutto nei servizi di Localizzazione Satellitare.

L'auspicio è che in futuro anche per la Telesorveglianza possa essere attivata una virtuosa collaborazione tra i settori pubblico e privato, invece di dover registrare ulteriori occasioni mancate come recentemente accaduto in materia di monitoraggio dei rifiuti pericolosi e contrasto alle cosiddette “ecomafie” (sistema SISTRI).

Roma, maggio 2010

Antonello Villa
*Responsabile delle Relazioni Internazionali di FederSicurezza
Membro del Gruppo di Lavoro “Sorveglianza Elettronica” di CoESS.*

Le Centrali di Telesorveglianza (CT) nel Panorama della Sicurezza Europea

Libro bianco edito dal Working Committee Electronic surveillance di CoESS

Introduzione

Questo documento costituisce un Libro Bianco per descrivere la storia e le attuali e future questioni dell'attività delle Centrali di Telesorveglianza (CT) nel panorama della Sicurezza Europea.

Il suo scopo è di offrire una maggiore comprensione agli attori del mercato della sicurezza ed ai legislatori nazionali ed Europei di questa attività di vigilanza svolta da personale, che appartiene ai servizi privati di sicurezza, le necessità per un suo sviluppo e le condizioni per una collaborazione con le Forze dell'Ordine.

Il Libro Bianco spiega il punto di vista di CoESS come Confederazione Europea che cerca di armonizzare gli interessi dell'industria, dei legislatori, dei Governi e delle Forze dell'Ordine come pure degli utilizzatori finali/clienti e cerca di contribuire per un migliore contesto di sicurezza.

Riconoscimenti

CoESS desidera ringraziare tutti i membri del Gruppo di Lavoro Sorveglianza Elettronica per avere dedicato il loro tempo ed i loro sforzi per lo sviluppo di questo Libro Bianco come parte del Programma di Lavoro del Gruppo di Lavoro Sorveglianza Elettronica 2008-2009.

Sintesi

Questo Libro Bianco descrive il funzionamento delle Centrali di Telesorveglianza (CT) ed il loro contributo alla sicurezza totale. Le attività delle CT fanno completamente parte dei servizi privati di sicurezza, dove l'intervento umano da parte dell'operatore di CT è di grandissima importanza per l'accuratezza e la qualità del servizio fornito. L'utilizzo dei servizi delle CT dovrebbe essere visto all'interno della catena della sicurezza totale. In questo modo, il più alto grado di efficienza può essere garantito come documentato in questo Libro Bianco.

Un adeguato livello di standardizzazione, un corretto contesto legale per le attività degli operatori che operano in questi centri ed un corretto livello di informazioni all'utilizzatore finale e le altre parti coinvolte aumenta la qualità totale attraverso un controllato processo di verifica nella CT. Questo determina un'elevata accuratezza ed un ridotto tempo di reazione. Oltre a leggi e regolamenti correttamente descritti, un contesto legale dovrebbe definire anche requisiti addizionali (ad esempio riguardanti la formazione). Questo aumenta la professionalità delle attività di CT ed impatterà positivamente la sicurezza degli utenti finali.

Più allarmi possibili dovrebbero essere verificati dalle CT, perché questo sgrava enormemente le FF.OO. dalla necessità di trattare falsi allarmi. Le FF.OO. possono quindi meglio assegnare le priorità e concentrarsi sulla risposta agli allarmi urgenti. Ancor più, esse possono intervenire in allarmi reali e verificati con il massimo di informazioni utili. Per raggiungere questo scopo, il giusto livello di comunicazione e collaborazione tra le CT e le FF.OO. deve essere ufficialmente concordato. I Governi dovrebbero quindi promuovere il maggior uso possibile delle CT.

L'attuale panorama della Sicurezza Europea offre alcuni casi di "best practice" nei differenti campi come i casi in allegato dal Belgio, Regno Unito e Italia dimostrano.

C'è un importante compito per gli attori di questo settore nelle differenti nazioni (attraverso le loro organizzazioni nazionali) e per i legislatori (i Governi a livello nazionale, e la Commissione Europea a livello Europeo), di sviluppare correttamente i necessari contesti. Non solo il settore della sicurezza beneficerà da questo, ma ancor più ne trarranno beneficio i clienti, le società e le organizzazioni che aspirano ai più alti livelli di sicurezza; ed i rispettivi Governi che, attraverso le FF.OO., possono raggiungere una migliore efficienza.

Danny Vandormael

Presidente del Gruppo di Lavoro Sorveglianza Elettronica di CoESS

Indice

Centrali di Telesorveglianza?	...pag. 4
Attuale operatività/funzionalità	...pag. 6
Verso una Norma Europea per le Centrali di Telesorveglianza	...pag.9
Contesto legale e sociale europeo	...pag. 10
Cooperazione con le Autorità Pubbliche	...pag. 11
Tendenze e sfide per il futuro	...pag. 12
Best Practice Belgio	...pag. 13
Best Practice Regno Unito (UK)	...pag. 14
Best Practice Italia	...pag. 15

1. Centrali di Telesorveglianza?

Definizione

L'attività di una Centrale di Telesorveglianza (CT) è un'attività dove l'operatore è supportato elettronicamente nel raccogliere dati da differenti fonti, analizzare questi dati e interpretarli adeguatamente. L'operatore organizzerà poi un corretto intervento (es. intervento di guardie specializzate, verifica video etc.), seguirà il progredire dell'intervento e nel caso concluderà l'anomalia, informando di conseguenza tutte le parti interessate. Il fattore umano in queste procedure è di fondamentale importanza. Per questo, l'attività delle CT è parte dei servizi privati di sicurezza; un fatto che, in molti paesi, è confermato dall'inclusione dell'attività delle CT nella legislazione nazionale sui servizi di sicurezza.

Cenni storici

Il controllo remoto di segnali originati da un sistema di allarme è praticato da diversi anni, in una forma o nell'altra. Questo servizio era inizialmente fornito utilizzando reti telefoniche via filo, e affidato in larga parte a semplici combinatori telefonici elettromeccanici che chiamavano il custode delle chiavi, un istituto di vigilanza e in molti casi le Forze dell'Ordine (FF.OO.). Nella maggior parte dei casi, questi combinatori erano conosciuti come "combinatori telefonici automatici" che si sono evoluti nel tempo in "comunicatori digitali".

I combinatori telefonici automatici erano i progenitori dei sistemi di allarme a controllo remoto. Essi erano relativamente economici da installare e divennero un metodo molto popolare per le "richieste di intervento" che seguivano l'attivazione di un allarme. I combinatori telefonici automatici tradizionalmente usavano una linea telefonica esistente semplicemente chiamando le FF.OO. e riproducendo un messaggio registrato che forniva l'indirizzo e richiedeva l'intervento. All'inizio degli anni 60, questi sistemi erano parecchio utilizzati per gli obbiettivi ad alto rischio, banche, gioiellerie, depositi etc. Durante la fine degli anni 60, essi cominciarono ad essere popolari per i sistemi di allarme residenziale di fascia alta e, finalmente, nei primi anni 70 vennero installati in tutti i siti a rischio.

Questo capitolo vuole fornire un quadro del perché le CT sono divenute il punto primario di segnalazione per gli impianti antintrusione dagli anni 70 ad oggi. Alcune ragioni per questa evoluzione sono state le seguenti:

- l'incremento di popolarità nell'uso dei combinatori telefonici verso centrali di controllo determinò una grande richiesta di servizi alle FF.OO.;
- la chiarezza e la qualità dei messaggi che erano inviati dai combinatori telefonici divenne in molti casi inaffidabile e gli allarmi erano spesso generati senza ragione (falsi allarmi);
- divenne presto di dominio pubblico che creando un semplice guasto alla linea telefonica si impediva al segnale di allarme di raggiungere la sua destinazione;
- gli assicuratori e gli utenti finali persero fiducia e cercarono collegamenti più sicuri per la sicurezza, normalmente attraverso linee di comunicazione dedicate a partire dagli obbiettivi vigilati. Questo metodo parzialmente risolse alcuni dei problemi di sicurezza, ma continuò ad alimentare la domanda verso le FF.OO.

Questa è una breve lista delle prime esperienze di una soluzione immatura per portare un segnale da un'area ad un'altra in un modo relativamente sicuro; comunque, il costo e la pressione delle FF.OO. sul settore diedero origine alle odierne CT.

Durante l'inizio del periodo di transizione, le CT erano operate assieme alle esistenti Centrali Operative, che potevano allo stesso tempo raddoppiare la loro attività come centri di ricezione di segnali di allarme. Quando la popolarità del controllo remoto crebbe, i centri di controllo cominciarono a maturare sia come standards applicati che come qualità dei servizi offerti.

Negli anni 70, le FF.OO. cominciarono ad apprezzare il beneficio dell'attività economica di intercettazione dei segnali di allarme prima che venissero a loro passati, ma continuava a sussistere il problema della crescente domanda alle FF.OO. sia per la crescita del mercato, che per i falsi allarmi che venivano ricevuti.

Parallelamente all'aumentare della popolarità tra gli utenti e gli installatori di sistemi di allarme, l'aumento del numero dei sistemi di allarme monitorati da società private crebbe di anno in anno per un considerevole periodo di tempo. Questa crescita determinò la creazione di una grande industria di CT i cui numeri stavano anch'essi aumentando ad un tasso impressionante. Questa spettacolare crescita causata dalla domanda del mercato alla fine causò preoccupazioni alle FF.OO. Quello che fu percepito come un beneficio per tutti, rapidamente divenne una causa di assorbimento di risorse per le FF.OO. Fu chiaro che la maggior parte dei segnali passati alle FF.OO. erano ancora falsi allarmi. Questo problema si verificò in tutta Europa e in entrambe le sponde dell'atlantico. Le cose dovevano cambiare e cambiarono.

Alle CT e agli utenti in tutta Europa vennero applicate limitazioni circa quanti falsi allarmi sarebbero stati tollerati per ciascun sistema. Alcune nazioni optarono per adottare una procedura per la quale l'intervento veniva attuato solo se veniva fornita la prova che l'allarme era reale. Una nuova era cominciò nella definizione del monitoraggio di allarmi in tutte le nazioni dell'EU. La parola "conferma" divenne il requisito minimo e gli standards europei vennero consolidati per quanto possibile.

Il ruolo di una Centrale di Telesorveglianza oggi

La CT d'oggi giorno gioca un ruolo vitale nella catena della sicurezza proteggendo allo stesso tempo proprietà residenziali e commerciali. La CT controlla i sistemi di sicurezza dei propri clienti 24 ore su 24 7 giorni su 7 (24/7), assicurando che se rilevassero un problema o un allarme, la CT metterà in atto le procedure concordate e si accerterà che il corretto intervento sia inviato ai locali protetti.

Una CT ha contatti quotidiani con i clienti, gli installatori dei sistemi di sicurezza e i servizi di pronto intervento:

- mandando loro giornalmente rapporti sugli allarmi che sono stati ricevuti nelle 24 ore;
- parlando con i clienti che hanno accidentalmente disinserito il loro sistema di sicurezza (questo caso potrebbe riguardare qualche problema con il loro collegamento di allarme e il cliente vuole contattare la CT per assistenza);
- parlando con i servizi di pronto intervento informandoli degli allarmi ricevuti dai sistemi installati;
- gestendo con i servizi di pronto intervento richieste di maggiori informazioni riguardanti gli allarmi.

La CT può di conseguenza essere percepita come il "volto" del settore da parte dei clienti ed i servizi di pronto intervento. Questi possono formarsi un'opinione sulla professionalità del settore della sicurezza dalle azioni della CT.

La CT è importante anche per altre organizzazioni, come gli assicuratori che fanno affidamento sulla CT per controllare i sistemi dei loro assicurati. I commercianti utilizzano le CT per controllare i loro sistemi di sicurezza non solo per proteggere i loro locali ed i loro beni, ma anche il loro personale, che rappresenta il bene più prezioso.

I collegamenti di allarme non proteggono solo immobili, persone ed oggetti, ma fungono da deterrente per i criminali che sanno che l'attivazione di un allarme causerà un pronto intervento con un'alta probabilità di essere catturati.

Le moderne CT possono monitorare differenti tipi di sistemi, compresi ma non limitati a:

- Sistemi antintrusione
- Sistemi antirapina
- TVCC

- Sistemi antincendio
- Telesoccorso
- Sistemi di telecontrollo tecnologico
- Localizzazione satellitare

Questa lista non è esaustiva dato che la CT è in grado non solo di monitorare un sistema remoto, ma anche di svolgere un numero di funzioni addizionali, come agire da controllo accessi remoto per siti utilizzando tecnologie audio o TVCC, ad esempio rispondendo per un sistema citofonico, o anche effettuando un ispezione remota utilizzando il sistema TVCC del sito per visionare il perimetro.

E' verosimile che l'attuale scopo di una CT è limitato solamente dall'attuale tecnologia usata o dalla mancanza da parte dell'utilizzatore finale della conoscenza di quale gran valore aggiunto una CT può portare alla sicurezza delle loro abitazioni e attività.

2. Attuale operatività/funzionalità

Introduzione

Le CT hanno anche espanso le loro attività e responsabilità dal filtro degli allarmi intrusione ricevuti da posti fissi (immobili) per includere azioni di intervento su allarme provenienti da persone e beni mobili e da segnali di natura tecnica, di incendio o di natura medica.

Per compiere adeguatamente il suo ruolo in caso di allarme, allo scopo di massimizzare sia la sicurezza del cliente che l'efficacia dell'azione correttiva o preventiva presa dalle Autorità come dalle forze di intervento private, la CT effettuerà sempre i seguenti passi durante un processo di filtraggio sicuro e controllato:

- ricezione automatica di dati da una moltitudine di fonti e tecnologie;
- scarto automatico di quei segnali che non richiedano l'attenzione dell'operatore;
- permettere che l'operatore svolga un'analisi e verifica dei dati ricevuti in modo tale che egli/ella possa classificare la segnalazione in una specifica categoria di allarme;
- sulla base di questa classificazione, la CT procederà con ulteriori azioni (intervento) o deciderà di non procedere ulteriormente;
- l'operatore della CT poi chiuderà l'anomalia fornendo rapporti come da accordi presi con il cliente.

Negli ultimi decenni, grazie ad una serie di sviluppi tecnici e organizzativi, le CT sono state capaci di migliorare la loro capacità di filtro, ad esempio identificando e conseguentemente eliminando, dal processo, gli allarmi che non richiedono intervento, spesso riportati come "falsi allarmi".

Le nuove tecnologie di telecomunicazione forniscono alle CT risorse e mezzi aggiuntivi; comunque, per mantenersi al passo con questi rapidi sviluppi, continui investimenti sono necessari alle CT a tutti i livelli. Nonostante ciò, la CT deve porsi in modo critico al riguardo del valore aggiunto delle nuove tecnologie per mantenere sotto controllo il processo con filtri appropriati, e per mantenere il processo stesso al sicuro e lontano da attacchi e perdite di controllo, e per assicurare un addestramento adeguato dei suoi operatori

Il processo di gestione degli allarmi e l'intervento su allarmi di sicurezza

Ricezione dei dati (ingresso)

L'era della trasmissione di dati analogica e di una chiara e semplice struttura tecnica è passato da molto tempo. La CT oggi tratta dati in arrivo da una moltitudine di sorgenti e tecnologie:

- volumi elevati: un cliente medio trasmette approssimativamente 60 segnali al mese alla CT;
- reti trasmissive diverse: PSTN, ISDN, GSM (fonia), GSM/GPRS, internet, linee dirette e reti dedicate;

- reti di diversi operatori, con diversi livelli di prestazioni e garanzie;
- dati che sono formattati secondo protocolli diversi per i quali la CT esegue una selezione di specifici ricevitori multiprotocollo, dai segnali analogici via PSTN a segnali IP.

In un mese una “tipica” CT con circa 50.000 clienti riceverà approssimativamente 3 milioni di segnalazioni dalla sua base di clienti, e tutti questi richiedono un adeguato trattamento da parte dei server operativi della CT.

Filtro

I server della CT fornirà un iniziale filtro dei dati in base al fatto che siano relativi ad allarmi o da trattarsi come informazioni di servizio per riferimento futuro. Più del 90% dei segnali entranti sono filtrati ed archiviati. I server tratteranno autonomamente anche un certo numero di anomalie attraverso rapporti, messaggi vocali o SMS, riducendo quindi il numero di anomalie che richiedono l'intervento dell'operatore a meno del 5% dei segnali entranti. Queste anomalie possono essere identificate come “allerta di sicurezza”.

Analisi e verifica da parte dell'operatore

Storicamente, l'operatore della CT poteva richiamare sul posto, per esempio usando recapiti come mezzo di verifica. Negli ultimi decenni, la tecnologia ha fornito nuovi e ulteriori strumenti per gli operatori delle CT, una tendenza che senza dubbio continuerà. Questo ha provocato lo sviluppo di procedure di verifica, che stanno, in molti Paesi, diventando una qualche forma di legislazione o prescrizione tra le CT e le autorità nazionali. Queste prescrizioni definiscono le procedure, lo scambio di informazioni, le priorità e gli obiettivi di prestazione che sono applicabili a questo livello, ad esempio “l'impegno con il comitato di controllo” (Raad van Commissarissen) del VEBON/VPB danese, e leggi specifiche in Belgio e nel Regno Unito.

In una tipica CT con circa 50.000 clienti, agli operatori della CT vengono presentate circa 100.000 anomalie per mese (ovvero una media di 2 anomalie per cliente e per mese). Dopo la selezione e tenendo conto delle informazioni, meno del 50% di queste anomalie sarà qualificato come allerta di sicurezza. Le rimanenti anomalie saranno qualificate e trattate come anomalie procedurali o tecniche. Il completo processo di verifica è applicato alle allerta di sicurezza secondo le procedure concordate con il cliente e usando tutti i mezzi di verifica disponibili:

- Verifica audio: lo stabilimento di un contatto verbale diretto con il sito e/o il cliente e le persone referenti del cliente, sia tramite richiamata che attraverso una connessione automatica per ascolto silente e/o una comunicazione bidirezionale;
- Verifica sequenziale: valutazione della sequenza dei dati in arrivo, che confermano la prima anomalia con uno schema ripetitivo e/o una conferma da diversi punti di rilevazione e/o uno schema generico;
- Verifica video: lo stabilimento di un controllo visivo diretto con il sito utilizzando immagini, filmati video o video in tempo reale, che permettono una conferma dei dati ricevuti;
- Ispezione sul posto: verifica sul posto sia da parte di una persona designata che attraverso l'intervento di guardie private specializzate.

In caso uno o più di questi elementi di verifica confermino una situazione di sospetto, la CT catalogherà l'allerta come un allarme di sicurezza e procederà con la fase seguente di reazione giustificata.

Reazione giustificata

L'intervento sul posto può essere organizzato da istituti di vigilanza e/o dalla Polizia, a seconda delle leggi e circostanze locali. La pattuglia di intervento valuterà e consoliderà la situazione sul posto e richiederà ulteriore supporto se necessario. Per mantenere l'operatore della CT completamente informato sul progredire dell'intervento e per completare e automatizzare il flusso di informazioni verso la pattuglia di intervento, miglioramenti tecnici e procedurali sono già stati fatti e continueranno ad essere introdotti in futuro. Utilizzando apparati di localizzazione satellitare, PDA e altri strumenti, le informazioni possono

essere trasmesse in tempo reale alla squadra di intervento.

Evitare interventi non necessari offre diversi vantaggi:

- al cliente:
 - meno situazioni di pericolo
 - costi più bassi
 - nessun compromesso sulla sicurezza
- alla pattuglia di intervento:
 - minore carico di lavoro riscontrabile in minori costi e interventi più rapidi
 - migliori informazioni relative alla situazione sul posto riducendo i rischi sulla loro sicurezza
 - in alcuni paesi sono stati realizzati progetti tendenti ad automatizzare e uniformare lo scambio di informazioni con le autorità nazionali

Riscontro (rapporto)

Il processo di verifica è completato fornendo un riscontro al cliente e le altre parti coinvolte come gli installatori, le pattuglie di intervento etc.- La tecnologia ora permette di avere informazioni immediate e in linea:

- tecnologie di messaggistica: chiamate vocali, messaggi automatici, informazioni visualizzate su PDA o altri apparati etc.;
- accesso in linea a server sicuri dove ulteriori informazioni sugli eventi sono rese disponibili.

La tecnologia facilita anche la fornitura di migliori riscontri alle Istituzioni relativi alle anomalie stesse, il rateo di anomalie in particolari aree geografiche o il tipo di anomalia accadute. Ancora, le CT sono ben posizionate per disseminare queste informazioni ai clienti se richiesto e giustificato.

Altre attività riguardanti la sicurezza

Il descritto processo di filtraggio e verifica è in atto in molte CT al fine di gestire adeguatamente allarmi di sicurezza di obiettivi fissi (immobili). Dal 2000 comunque, le CT hanno gradualmente espanso le loro attività e responsabilità fino ad includere le seguenti funzioni:

- Localizzazione satellitare. Dato che le rapine a veicoli e abitazioni hanno raggiunto un livello critico, le CT hanno proposto di installare un apparato che permetta la trasmissione in tempo reale di dati e coordinate GPS. Questa periferica è installata in beni in movimento come autovetture, camion, equipaggiamenti etc.- I segnali sono processati in accordo con il summenzionato processo di filtraggio e verifica, ma la natura dell'apparato permette servizi aggiuntivi di localizzazione, immobilizzazione controllata, e altri servizi come da richiesta del cliente e secondo le leggi applicabili. La collaborazione tra le CT e le autorità nazionali ha portato a tangibili successi rispetto alla riduzione dei falsi allarmi, ritrovamento dei veicoli (oltre il 90%) e l'arresto di criminali.
- Con riferimento al monitoraggio di persone, un servizio da parte delle CT è attualmente in corso di sviluppo per gestire i rischi di sicurezza ai quali i lavoratori isolati e altri addetti sono esposti. Un dispositivo portatile, simile ad un telefono GSM, provvede alla trasmissione di dati e coordinate del luogo attraverso LBS o GPS. I segnali sono elaborati secondo il processo di filtraggio e verifica precedentemente esaminato.
- I sistemi TVCC sono usati dalle CT non solo per la verifica video, ma anche per eseguire funzioni di videosorveglianza attraverso ronde virtuali o visione sistematica di materiale video. Spesso non sussistono specifici segnalazioni che attivino l'azione della CT, ad eccezione di un'immagine entrante, che la CT reputi essere anomala.

Altre attività

Nel precedente paragrafo il processo di filtraggio e verifica delle allerta di sicurezza e degli allarmi provenienti da sistemi di allarme in funzione in immobili, persone o obiettivi in movimento è stato descritto in dettaglio. A fianco di attività riguardanti esclusivamente la sicurezza (security), la CT tocca anche i campi tecnico e della safety.

Allarmi tecnici

Procedure di filtraggio e verifica simili a quelle delle allerta/allarmi sono applicabili agli allarmi provenienti da apparati tecnologici che indicano un malfunzionamento tecnico, per esempio il controllo della temperatura, la caduta di tensione etc.-

Allarmi relativi alla safety

- Allarmi sociali: La CT fornisce servizi di assistenza per certe classi demografiche che richiedono una verifica di posizione, per esempio persone anziane, prigionieri etc.-
- Allarmi medici: La CT fornisce la prima linea di interazione con persone che hanno necessità di cure mediche.
- Ascensori: La CT processa segnali e chiamate dagli ascensori e organizza l'intervento.
- e-Call: La CT reagisce a segnali provenienti da veicoli "in pericolo", per esempio in caso di attivazione degli airbags, rilevatori di collisione etc. verificando la posizione e se necessita aiuto e assistenza. Per maggiori informazioni fare riferimento alla Comunicazione della Commissione Europea COM(2009) 434 ad oggetto 'e-Call: Time for Deployment'.
- Allarmi incendio: Procedure di filtraggio e verifica per allerta/allarmi di sicurezza sono applicabili agli allarmi incendio, ma con procedure su misura e i Vigili del Fuoco come squadra di intervento designata.

3. Verso una Norma Europea per le Centrali di Telesorveglianza

Nel 2000, è stata lanciata l'idea di preparare un'iniziativa europea per la standardizzazione delle attività di centralizzazione e sorveglianza elettronica. L'iniziativa assunse una forma concreta quando il Gruppo di Lavoro Sorveglianza Elettronica di CoESS ed il comitato permanente n°7 di Euralarm decisero di riunire le forze per elaborare una bozza di proposta comune riguardante le Centrali di Telesorveglianza. L'intenzione era quella di definire una serie di criteri ai quali le CT in tutta Europa si dovessero attenere.

Nel giugno del 2005, dopo 4 anni e mezzo di intenso lavoro, un comune "Codice di Condotta per la Centralizzazione e le Centrali di Telesorveglianza" è stato definito. Entrambi i gruppi di lavoro concordarono di presentare il documento ai rispettivi consigli. Una volta approvato formalmente il Codice di Condotta è stato trasmesso alle maggiori agenzie di standardizzazione europee come documento di discussione per lo sviluppo di una norma europea.

La bozza era destinata ad essere discussa all'interno del CENELEC, il comitato elettrotecnico europeo per la standardizzazione. Il CENELEC fondò un nuovo gruppo di lavoro (n°14) secondo la prassi: le organizzazioni nazionali di standardizzazione hanno designato gli esperti a livello nazionale delegati a partecipare al gruppo di lavoro europeo. La fase preparatoria si tenne a metà del 2006, quando il gruppo di lavoro cominciò ufficialmente le sue attività.

Un totale di 20 esperti nazionali partecipano agli incontri bimensili o trimestrali del gruppo di lavoro. Vale la pena di segnalare come diversi partecipanti della precedente task-force CoESS-Euralarm sono ancora presenti nel gruppo di lavoro CENELEC, rappresentando quindi molti degli stessi paesi.

Il gruppo di lavoro CENELEC procede essenzialmente nello stesso modo della task-force CoESS-Euralarm nel senso che tutti i maggiori argomenti, punti e questioni sono discusse in dettaglio. Le specifiche CENELEC per le CT saranno divise in tre parti:

- Standard Europeo EN 50518-1 – Parte 1: Sede e requisiti costruttivi
- Standard Europeo EN 50518-2 – Parte 2: Requisiti tecnici
- Standard Europeo EN 50518-3 – Parte 3: Procedure e requisiti operativi

L'intero processo preparatorio e le specifiche finali è previsto che siano concluse nel corso del 2010.

La futura norma CENELEC è un esempio di una iniziativa di armonizzazione, guidata da esperti tecnici e distribuita in un notevole lasso di tempo, iniziata da una comune task-force CoESS-Euralarm che ha preparato una bozza che è in revisione all'interno della struttura CENELEC con l'intento di diventare una norma Europea.

Attualmente il comitato tecnico sicurezza (security) (IEC TC/79) appartenente all'agenzia mondiale di standardizzazione, la Commissione Elettrotecnica Internazionale (IEC) sta cercando di scrivere uno standard internazionale per le CT. E' previsto che il lavoro CENELEC sarà usato come parte dei documenti di base per questo lavoro.

4. Contesto legale e sociale europeo

Disposizioni legali

All'inizio del 2007 e in previsione dell'inizio dello sviluppo di uno standard europeo (EN50518) per le Centrali di Telesorveglianza, CoESS ha condotto un'indagine nell'ampio mercato europeo della telesorveglianza al fine di determinare l'esistenza o meno di specifici regolamenti nella regione. Questa indagine è stata aggiornata all'inizio del 2009.

In termini generali, l'indagine era rivolta a tre aree specifiche:

1. Qual'è l'attuale situazione legale in relazione alla telesorveglianza in ogni nazione europea?
2. Esiste uno standard nazionale obbligatorio per le CT?
3. C'è una disposizione fissata dalla polizia che deve essere da loro seguita per offrire un servizio di intervento alle CT?

Tutti i 27 stati membri sono stati invitati a partecipare all'indagine. I seguenti paesi non hanno fornito il loro contributo: Cipro, Danimarca, Lettonia, Lituania, Lussemburgo, Malta, Portogallo e Svezia. I seguenti paesi esterni all'EU hanno preso anch'essi parte all'indagine, nello specifico Bosnia Erzegovina, Norvegia, Serbia, Svizzera e Turchia.

Situazione legale in relazione alla telesorveglianza

Tutte le nazioni dell'EU partecipanti hanno indicato che accanto alle generali leggi che regolano le attività economiche, sono in vigore leggi specifiche riguardanti il funzionamento di una CT nel loro paese.

Delle nazioni non EU sia la Norvegia che la Bosnia Erzegovina hanno leggi, mentre la Svizzera ha riferito che, a parte la legislazione generale sulle attività economiche, non ha leggi specifiche.

Standard nazionali per le CT

Qui le risposte sono state molto diverse con solo i seguenti paesi che hanno confermato l'esistenza di uno standard nazionale corrente: Austria, Francia, Germania, Irlanda, Italia, Olanda, Spagna, Slovenia e Regno Unito.

Le seguenti nazioni non hanno confermato di avere uno standard nazionale: Bulgaria, Estonia, Finlandia, Grecia, Polonia, Repubblica Ceca, Romania, Slovacchia e Ungheria.

Riguardo le nazioni non EU Serbia, Svizzera e Turchia non hanno standard nazionali, mentre la Bosnia Erzegovina ha confermato di averlo.

Disposizioni di Polizia

Le seguenti nazioni hanno confermato l'esistenza di regole della locale Polizia per le loro CT per ottenere un intervento da parte della Polizia stessa: Austria, Belgio, Francia, Germania, Irlanda, Olanda, Regno Unito, Repubblica Ceca e Slovenia.

Le seguenti nazioni non hanno regole specifiche di Polizia che determinino requisiti al fine di intervenire su un evento di allarme ricevuto da una CT: Bulgaria, Estonia, Finlandia, Grecia, Italia, Polonia, Romania, Slovacchia, Spagna e Ungheria.

Tutte le 3 nazioni non EU e quindi Norvegia, Svizzera e Bosnia Erzegovina, hanno specifiche disposizioni di Polizia.

Sistema sanzionatorio o perdita della possibilità di ottenere un intervento dalla Polizia

In Europa, la Polizia affronta i falsi allarmi in molti modi differenti. In alcuni paesi, multe sono irrogate alla CT o all'installatore o all'utilizzatore finale. In altre nazioni, non ci sono multe, ma la Polizia non interviene per sistemi di allarme che abbiano già generato un certo numero di falsi allarmi in un determinato periodo.

Requisiti di formazione

Gli stessi paesi hanno risposto alla domanda se esista o sia obbligatorio un formale programma di formazione per gli operatori delle CT.

In molti paesi, per esempio Belgio, Finlandia, Francia, Italia, Olanda, Polonia e molti altri, gli operatori delle CT, essendo queste parte della sicurezza privata, necessitano di qualificarsi come guardie private di sicurezza.

Vale a dire che essi necessitano dell'approvazione ufficiale da parte dell'autorità competente nel loro paese e hanno l'obbligo di seguire la formazione iniziale delle guardie private di sicurezza.

Oltre a questa formazione di base, un certo numero di paesi hanno introdotto requisiti aggiuntivi per gli operatori delle CT, obbligatori per legge o altro (per esempio in Belgio un requisito di legge impone di completare una formazione specifica di 70 ore in aggiunta alla formazione di base di 132 ore e di passare un test in un centro governativo d'esame; dopodichè alla guardia è rilasciata una licenza), o una specifica formazione organizzata da istituti di formazione specializzati; per esempio il Nordic Centre for Alarm Technique (NUSA), Inspectorate of the United Kingdom, Security institute of Ireland etc.-

5. Cooperazione con le Autorità Pubbliche

Il fattore chiave, ma ancor più il ponte tra la sicurezza privata e le Istituzioni statali, è costituito dalle CT.

In molte nazioni, le Istituzioni sono piuttosto apprensive circa la loro connessione con la vigilanza privata ed anche con le possibilità offerte da dispositivi di sicurezza come telecamere, dispositivi TVCC e sistemi di controllo accessi. Questi sospetti sono spesso causati dalla mancanza di conoscenza della realtà odierna e/o da visioni politiche ristrette. La sicurezza (security & safety) si crede ancora sia riservata esclusivamente all'ambito dell'autorità pubblica.

Nonostante ciò, il settore delle CT è percepito come il segmento più affidabile della sicurezza privata. Le ragioni di questo sono molteplici. Le CT godono dell'impressione di neutralità tecnica e beneficiano della percezione di qualità e professionalità. Le Istituzioni collaborano con le CT sempre più costantemente.

E' infatti quasi impossibile e troppo costoso per la Polizia ed i Vigili del Fuoco essere collegati a milioni di case, attività e immobili pubblici nelle loro rispettive aree.

Il fatto che le CT sono spesso le prime ad essere avvisate di un'intrusione, furto o incendio è una caratteristica molto opportuna per le Istituzioni.

La situazione come si presenta per esempio in Belgio, Olanda o nel Regno Unito è in molti aspetti un modello per il futuro. E' importante che le Istituzioni firmino accordi con le CT che prevedano reciproci impegni e responsabilità. Rimane cruciale per le CT impegnarsi in stringenti procedure, politiche di riservatezza ed un'immediata risposta agli allarmi. Le Istituzioni (sia la Polizia che i Vigili del Fuoco) in cambio devono impegnarsi ad intervenire in maniera tempestiva. Troppo spesso, solo le CT hanno contratti

in termini di servizio e qualità verso i loro utenti finali.

Parimenti importante è la necessità per la Polizia e i Vigili del Fuoco di fornire un resoconto alla CT a seguito di un intervento. Questo non solo riassicurerà il cliente in questione, ma migliorerà le misure correttive e/o preventive ed aumenterà la sicurezza totale.

Cooperando fianco a fianco con le CT, non c'è bisogno per le Istituzioni di investire in costoso hardware e software, neppure sono obbligate a pagare il personale delle CT 24 ore su 24, ma, di maggior importanza, è il fatto che le Istituzioni possono rifarsi alla responsabilità delle CT in caso di insuccesso o errore.

Queste sono solo alcune delle ragioni del perché la cooperazione tra le Istituzioni e le CT ha bisogno di essere rafforzata e ufficialmente riconosciuta nella legislazione nazionale e sovranazionale.

Una stretta collaborazione necessita del giusto bilanciamento tra l'interesse pubblico e l'interesse del cliente finale della CT. Viste le attuali sfide in termini di accresciuti rischi, della globalizzazione e continua democratizzazione del mondo, la cooperazione tra tutte le parti coinvolte nella sicurezza (Istituzioni statali, clienti e CT) continueranno ad aumentare. La relazione tra le Istituzioni e le CT evolverà verso una collaborazione di sussidiarietà nella quale la CT esegue le sue mansioni di sicurezza e le Istituzioni assicurano il contesto legale entro il quale la CT deve operare. Al fine di evitare una collaborazione sbilanciata, è imperativo mettere in campo una legislazione Europea basata sui valori democratici degli Stati Membri, le conoscenze detenute dalle parti coinvolte nella sicurezza ed una visione positiva per il futuro.

6. Tendenze e sfide per il futuro

Negli anni, il mercato Europeo delle CT è cresciuto in modo considerevole in termini di base di clientela, e sembra essere indirizzato a continuare questa tendenza per il futuro. Nonostante ciò, le CT devono continuamente affrontare nuove sfide causate da importanti cambiamenti e dalla comparsa di nuove tecnologie, alcune delle quali presentano interessanti opportunità.

Da un punto di vista tecnologico, ci sono tre fattori chiave che determinano lo sviluppo del mercato delle CT:

le CT sono abituate a collegare i sistemi di allarme dei loro clienti attraverso linee telefoniche analogiche (PSTN), che stanno per essere abbandonate a favore di linee telefoniche digitali (VOIP). Questo nuovo assetto richiede la sostituzione di un sostanziale numero di dispositivi con più sicuri e più capaci dispositivi abilitati alle reti TCP (ADSL o GPRS);

le informazioni di allarme ricevute da una CT comprendono sempre più video e/o audio, che a loro volta forniscono una migliore qualità per la verifica, e permettono all'operatore di CT di eseguire remotamente una analisi approfondita della situazione sul posto. Le nuove funzioni di monitoraggio includono i controlli di inserimento/disinserimento parziale o totale, cambio remoto di parametri e aggiornamento del firmware;

il rapido sviluppo di applicazioni di sicurezza machine-to-machine (M2M) schiude possibilità completamente nuove per le CT, cambiando l'obiettivo del monitoraggio da un ambiente fisso ad uno mobile fino ad arrivare alla posizione di un individuo. Le CT sono ancora perlopiù ad una fase iniziale di questi eccitanti sviluppi, i quali è previsto che determinino una rapida espansione nei prossimi anni anticipando prossime normative (ad esempio l'iniziativa e-Call) e la crescente disponibilità del GPS ed altre tecnologie per il tracciamento personale o di altri beni.

Le CT in tutta Europa stanno compiendo sforzi considerevoli per ridefinire il loro ruolo in preparazione di questi cambiamenti, specialmente in termini di infrastrutture IT, nuove procedure ed adeguati programmi di formazione. Quest'ultimo elemento migliorerà la permanenza nelle CT di operatori capaci, che diventerà

una crescente preoccupazione per il settore dato che i requisiti di formazione continuano ad innalzarsi.

La percezione ed il valore aggiunto delle CT nella gestione di allarmi di sicurezza ha bisogno di essere affrontata e migliorata in alcune aree, come il mercato residenziale, che dimostra un forte potenziale dato che la penetrazione di mercato in questo particolare segmento, non è sempre alta in ogni nazione. Le nuove tecnologie permettono al cliente di beneficiare più o meno delle stesse funzioni che sono disponibili nella CT, ad esempio il cliente può ricevere allarmi in tempo reale via SMS, MMS e e-mail, può vedere immagini o filmati, può attuare un ascolto silente ed è abilitato a gestire il suo sistema di sicurezza a casa o dall'ufficio usando un PC od uno smartphone. Queste utili funzioni devono, comunque, essere usate parallelamente al servizio effettuato dalle CT, in quanto non sostituiscono la gestione professionale degli allarmi e la verifica. Un cittadino non è addestrato a garantire queste mansioni, e neppure egli/ella è disponibile 24 ore su 24. Le FF.OO. Dovrebbero quindi scoraggiare l'approccio "fai da te" alla sicurezza.

In questo mutevole ambiente, rimane uno sfidante compito per il settore della sicurezza privata di avere un ruolo attivo nella definizione di nuove norme e protocolli, inclusi i manuali di addestramento, fissando quindi il più alto livello possibile di standard di qualità. L'elevata qualità comporta un riconosciuto valore aggiunti e reciproci benefici per i clienti, le Istituzioni ed il settore della sicurezza.

7. Best Practice Belgio

Il caso di best practice del Belgio è stato fornito dalla ACA¹ (Alarme Centrale Associatie/Association Centrale d'Alarme), l'associazione belga delle centrali di telesorveglianza, che è membro attivo di CoESS.

La cooperazione pubblico-privato su una migliore verifica porta ad un più efficace e sicuro intervento a seguito di un allarme

L'intervento del Ministero dell'Interno Belga è stato uno dei primi e più importanti fattori nella regolamentazione del settore della Sicurezza Privata. Dopo la creazione della struttura legale per il settore della Sicurezza Privata (che riguarda, tra le altre, l'attività delle CT) avvenuta il 10 aprile 1990 (la cosiddetta "Legge Tobback"), questa Istituzione ha continuato con chiarimenti e aggiornamenti sotto forma di Decreti Reali. Con riguardo al ruolo delle CT, due specifici Decreti Reali hanno giocato un ruolo importante:

Il primo è stato pubblicato il 17 maggio 2002 e ha regolamentato l'obbligatorietà del ruolo delle CT riguardo alla "Localizzazione di un Veicolo Rubato" (SVT). E' stata la prima regolamentazione per questo tipo di attività in EU. I principi operativi che soggiacciono a questa legge sono stabiliti in stretta collaborazione con i fabbricanti dei dispositivi, gli assicuratori e le CT. Le CT ricevono allarmi da circa 30.000 veicoli collegati e hanno limitato la loro richiesta alla Polizia per un intervento a meno di 300 casi per anno. Più del 70% delle richieste si rivelano essere furti reali o tentativi di frode. Il rateo di recupero di veicoli rubati è ben oltre il 90%.

Una seconda legge è passata come Decreto Ministeriale il 10 gennaio 2003 e riguarda le comunicazioni tra le CT e la Polizia. Il decreto è stato seguito da documenti contenenti chiarimenti aggiuntivi riguardanti ad esempio la verifica degli allarmi in arrivo e la successiva comunicazione con la Polizia. Queste procedure di verifica sono state elaborate in stretta collaborazione tra le Istituzioni e le CT. L'implementazione di queste hanno permesso alle CT, nel 2005, di meglio filtrare la massa di allarmi in arrivo (stimati in oltre 4.000.000 ogni anno) e di ridurre le richieste alla Polizia per l'intervento a meno del 25% del livello del 2002. Durante il simposio su "La Sicurezza Privata in movimento!" il 7 dicembre 2006, il Ministro dell'Interno ha riconosciuto questo risultato come l'abbattimento di decine di migliaia di inutili interventi della Polizia per anno. Egli ha anche annunciato la sua strategia per ulteriormente supportare l'incremento dell'utilizzo delle CT nel processo di verifica degli allarmi per la migliore accuratezza delle informazioni da loro ricevute

1 Si prega di riferirsi al sito web di ACA per ulteriori informazioni sull'organizzazione di ACA e le sue attività (il sito è disponibile solamente in olandese e francese): www.a-c-a.be .

rispetto ad altre fonti. Uno dei risultati è stato un trattamento fiscale favorevole per i servizi delle CT ed i relativi componenti, come le installazioni di allarmi, nella catena del valore.

Recenti sviluppi in Belgio sono focalizzati sulla qualità delle informazioni, e il modo in cui sono trasmesse dalle CT alle guardie specializzate ed alle FF.OO.- Ancora l'intento è quello di incrementare ulteriormente l'efficienza e la sicurezza dell'intervento sul posto.

8. Best Practice Regno Unito (UK)

Il caso di best practice del Regno Unito (UK) è stato fornito dalla BSIA², la British Security Industry Association, che è membro attivo di CoESS.

Nel Regno Unito, se una Centrale di Telesorveglianza desidera attivare la Polizia a seguito di un allarme, deve ottemperare alle condizioni definite dal sistema di norme di Polizia del Regno Unito³ assieme all'installatore/manutentore del sistema (che deve anch'egli ottemperare alle previsioni delle norme di Polizia del Regno Unito) per prevenire/gestire i falsi allarmi.

Il lavoro intrapreso dal settore per ridurre i falsi allarmi causati da sistemi di allarme antintrusione è stato enorme. Nel 2000, c'erano 949.062⁴ sistemi antintrusione con segnalazione remota e questi hanno determinato 921.649 falsi allarmi (quasi un falso allarme per sistema) e ciò era inaccettabile per il servizio della Polizia. Nel 2008, il numero di sistemi antintrusione con segnalazione remota installati è cresciuto a 1.152.475 ed il rateo di falsi allarmi si è abbattuto a 277.873. Il settore e le FF.OO. stanno lavorando assieme per continuare questa tendenza alla diminuzione nell'attivazione delle forze di Polizia.

I maggiori sforzi della Polizia e del settore sono stati indirizzati verso quei sistemi antintrusione che hanno avuto un certo numero di false attivazioni nelle quali la Polizia è intervenuta. E' stato concordato che se un sistema di allarme avesse generato 5 falsi allarmi sarebbe stato rimosso dalla disponibilità dell'intervento e avrebbe potuto essere riabilitato al servizio se il sistema antintrusione di allarme fosse stato aggiornato a "sistema di allarme conforme" (il documento dd 243 del British Standard si riferisce a questo). Questo ha significato che il sistema di allarme antintrusione dovesse mandare due distinte attivazioni di allarme da almeno due distinti (e indipendenti) sensori prima che la CT potesse passare l'allarme alla centrale operativa della Polizia per causare l'intervento della Polizia. Questo provocò una curva di apprendimento per l'intero settore dato che l'installatore ha dovuto imparare come progettare e installare sistemi conformi e la CT ha dovuto gestire sistemi di allarme conformi.

Attualmente, il documento per l'approvazione British Standard DD 243 è stato aggiornato a British Standard BS 8243 e la Polizia ora richiede che le attivazioni per allarme rapina siano "conformi". Questo ha significato che quando un allarme rapina è ricevuto, ci deve essere una qualche forma di verifica che l'allarme sia reale. Questa può essere costituita da una forma di conferma audio o video o altro metodo per ridurre la possibilità di false attivazioni.

E' importante notare come i "sistemi conformi" sono solo richiesti per nuove installazioni antintrusione e per sistemi antintrusione e antirapina che hanno causato falsi allarmi. Le forze di Polizia non hanno richiesto retroattivamente che tutti i vecchi sistemi siano aggiornati finché questi sistemi antintrusione o antirapina causino falsi allarmi.

2 Si prega di riferirsi al sito della BSIA per ulteriori informazioni sull'organizzazione di BSIA e le sue attività (il sito è disponibile solamente in inglese): www.bsia.co.uk.

3 Questo documento è intitolato "APCO Security Systems Policy 2009" ed è disponibile dal seguente sito web: www.securebydesign.com/professionals/pdfs/ssgpolicy.pdf.

4 I numeri citati in questo paragrafo sono tratti dai dati ufficiali della Association of Chief Police Officers (APCO).

Il lavoro che il settore ha intrapreso con la Polizia sta provando a cosa può portare un approccio collaborativo. Affrontare il problema dei falsi allarmi fornisce anche alla Polizia la certezza che quando rispondono ad una chiamata da parte di una CT, c'è un'alta probabilità che un furto o una rapina reale si sta consumando e loro possono comportarsi di conseguenza.

9. Best Practice Italia

Il caso di best practice italiano è stato fornito da Federsicurezza – A.N.S.S.A.T. Federsicurezza⁵ (Federazione del Settore della Vigilanza e Sicurezza Privata) è l'associazione italiana per i servizi di sicurezza, membro attivo di CoESS. A.N.S.S.A.T.⁶ (Associazione Nazionale Servizi Satellitari e Telematici) è l'associazione italiana per i servizi satellitari e telematici, ed è a sua volta membro di Federsicurezza – Confcommercio.

Il testo originale in italiano è stato fornito dal Sig. Romano Lovison, President di A.N.S.S.A.T. Questo testo è un estratto dell'edizione italiana del rapporto 2009 di Federsicurezza intitolato: "Rapporto 2009 Federsicurezza: realtà e scenari della sicurezza privata italiana nel contesto Europeo"⁷.

Le aziende associate erogano servizi di sicurezza evoluta su oltre l'80% dei mezzi pesanti, dotati di sistemi satellitari, con servizio di sicurezza professionale. Nel corso degli ultimi anni l'attività di controllo su mezzi mobili, svolta dai soci di A.N.S.S.A.T. , ha prodotto un risparmio per le compagnie di assicurazione ovvero per i privati o le imprese di autotrasporti o per i committenti i trasporti, mediamente di circa 55 milioni di Euro annui per furti e rapine sventate.

In questo studio è stata esaminata l'attività di circa 800 veicoli che hanno trasportato merce di analoga tipologia e percorsi omogenei sul territorio italiano. Ciò per fornire un quadro dell'importanza, per la sicurezza dei trasporti, dell'adozione di sistemi di radiolocalizzazione su veicoli pesanti.

La comparazione avviene confrontando i viaggi tra un 50% circa di veicoli con sistema di sicurezza professionale e il 50% circa di veicoli senza alcun sistema di sicurezza.

Nel 2008 si ha una notevole riduzione degli eventi dovuta ad una sempre maggiore azione di contrasto sia per l'organizzazione della sicurezza dei trasporti ma anche per le azioni attuate dalle forze di Polizia che spesso, grazie all'ausilio dei dati forniti dai sistemi di controllo, hanno potuto porre in essere importanti attività di repressione del fenomeno.

La maggior parte degli eventi avviene su veicoli non dotati di sistema di radiolocalizzazione satellitare. In particolar modo si può osservare l'elevato numero di mezzi che hanno subito il furto totale della merce. Per quanto attiene il furto parziale è da sottolineare come l'entità della merce parzialmente sottratta sia diversa.

In ipotesi di veicolo dotato di sistema di radiolocalizzazione satellitare la merce sottratta è poca cosa (qualche pacco) in quanto l'attivazione dei sistemi acustici reca disturbo all'attività dei malviventi mentre in veicoli senza sistemi di sicurezza il danno è maggiore. Le rapine effettuate sono 4 mentre una risulta solamente tentata grazie alla bravura del conducente che con il suo comportamento è riuscito a sventarla. Il furto del mezzo è avvenuto in un'officina, mentre era in manutenzione, ma la presenza del sistema ne ha consentito il recupero.

5 Si prega di riferirsi al sito di Federsicurezza per ulteriori informazioni sull'organizzazione di Federsicurezza e le sue attività (il sito è disponibile solamente in italiano): www.federsicurezza.it .

6 Si prega di riferirsi al sito di A.N.S.S.A.T. per ulteriori informazioni sull'organizzazione di A.N.S.S.A.T. e le sue attività (il sito è disponibile solamente in italiano): www.anssat.it .

7 Il "Rapporto 2009 Federsicurezza: realtà e scenari della sicurezza privata italiana nel contesto Europeo" può essere scaricato dal sito web di Federsicurezza sia in italiano (<http://www.federsicurezza.it/public/documenti/97200913365.pdf>) che in inglese (<http://www.federsicurezza.it/public/documenti/89200915934.pdf>).

Per quanto riguarda la tipologia di evento a cui sono stati soggetti i veicoli dotati di sistema di radiolocalizzazione satellitare: nell'86% il danno è stato evitato totalmente (80%) o parzialmente (6%) grazie alla presenza e al funzionamento del sistema di radiolocalizzazione satellitare. Solo nel 12% dei casi (furto totale 8% e rapina 4%) vi è stato il danno completo.

Analizzando questi casi uno per uno, si evidenzia che ciò è avvenuto per inosservanza da parte dell'autista delle disposizioni impartite, la più frequente delle quali è stata la sosta in aree non sicure.

Si evidenzia come in caso di evento vi è sempre un danno economico. Nel 53% dei casi vi è un evento importante con il furto totale e nel 47% dei casi un danno parziale. In quest'ultima ipotesi, come si è prima osservato, il danno parziale è di entità maggiore rispetto all'analogo danno parziale patito dai veicoli dotati di sistema di radiolocalizzazione satellitare.