

LA CENTRALE OPERATIVA ANTIRAPINA: FILTRO TRA LE SEGNALAZIONI PROVENIENTI DAGLI SPORTELLI BANCARI E LE SALE OPERATIVE DELLE FORZE DELL'ORDINE

DOTT. GIUSEPPE CALABRESE
Istituto di Vigilanza Città di Milano S.p.A.

Buongiorno, sono Giuseppe Calabrese, sono responsabile dell'organizzazione e del coordinamento operativo dell'Istituto di Vigilanza Città di Milano. Provingo da un'esperienza di dieci anni all'interno delle Forze di Polizia, e in particolare ho coordinato la centrale operativa della Questura di Milano ed ho svolto funzioni come dirigente di una sezione investigativa all'interno della Squadra Mobile della Questura di Milano

Questo intervento rappresenta, in pratica, una testimonianza e cercherò di essere breve perché probabilmente il livello di attenzione di tutti noi va scemando.

Abbiamo avuto modo di ascoltare, in precedenti relazioni, concreti accenni alla diversità delle tecnologie che ci consentono di gestire le varie segnalazioni di allarme o comunque le varie necessità di sicurezza all'interno delle agenzie, degli sportelli bancari. Mi soffermerò, in particolare, sulla videosorveglianza in ambito bancario, perché l'Istituto che rappresento da diversi anni ormai ha sviluppato delle strategie e realizzato delle infrastrutture (centrali operative antirapina o di videosorveglianza) che ad oggi hanno superato la fase sperimentale, durata circa tre anni, ma ancora necessitano di alcune implementazioni e di ulteriori sviluppi, non soltanto dal punto di vista tecnologico.

Sappiamo, infatti, che se la tecnologia è in continua evoluzione, sicuramente un dato rilevante è rappresentato dalla gestione, o meglio dal fattore umano rappresentato da coloro che sono chiamati a gestire la tecnologia: è sempre all'Uomo che compete la fase di acquisizione, di rilevazione e di gestione, in termini di intervento e di operatività.

Il servizio di videosorveglianza all'interno delle banche è un servizio alternativo alle tipologie classiche antirapina ed ha finalità che tutti conosciamo: prevenire rapine ed altri atti criminosi.

Cercheremo di analizzare in che termini può essere efficace e quando non lo è, ed è un servizio meno rischioso degli "antirapina" classici, essendo una sorta di "guardiana virtuale", come qualcuno l'ha definita. Una sorta di vigilanza virtuale che può far diventare l'operatore, il gestore all'interno della centrale operativa antirapina, parte integrante della struttura e del sistema di sicurezza dell'agenzia bancaria.

Il sistema di controllo di videosorveglianza è composto da diverse apparecchiature

- postazioni con personal computer
- modem collegato con linea ISDN e SNA della linea dati delle agenzie bancarie
- linea di collegamento
- microfono per comunicazioni
- telecamera di postazione immagini visibili attraverso linea SNA

Nella realtà, tuttavia, possono riscontrarsi diversi tipi di centrali operative di videosorveglianza, che si differenziano e si caratterizzano per una diversa organizzazione, o per strumenti e postazioni diversi.

Esistono centrali operative di videosorveglianza che hanno tuttavia delle caratteristiche diverse. Ci sono centrali operative che si attivano in seguito all'azionamento di un pulsante antirapina, oppure in seguito a una richiesta di comunicazione da parte di un dipendente oppure ancora per l'attività autonoma dell'operatore in stand-by. Vi sono altre centrali operative di videosorveglianza che si caratterizzano per un collegamento costante, che va dall'orario di apertura dell'agenzia bancaria, mattino e pomeriggio: in tali casi si tratta di "postazioni operatore" ed ogni operatore effettua il controllo da un minimo di due ad un massimo di dieci agenzie, ed è in grado di vedere attraverso un monitor, solitamente diviso in quattro parti, anche quattro siti contemporaneamente (con due monitor, fino a otto).

L'attività dell'operatore viene documentata da una serie di funzioni, ed alla base ci colloca il primo contatto all'apertura, con una verifica del funzionamento degli impianti, una verifica audio, una verifica telecamere, una verifica immagini all'interno dell'agenzia. Questo controllo viene poi reiterato durante tutta la fascia oraria del collegamento.

L'operatore, quindi, documenta queste attività attraverso la redazione di un documento che quotidianamente viene custodito all'interno delle centrali operative antirapina di videosorveglianza, come riscontro continuo dell'attività che viene svolta.

Prima di passare alla fase della gestione, la considerazione che tutti noi facciamo appena entriamo in una centrale operativa di videosorveglianza è: ma un operatore è veramente in grado di seguire contestualmente quello che accade in otto agenzie in videosorveglianza?

Effettivamente c'è margine per questa riflessione, c'è una grande perplessità sulla effettiva capacità di un singolo operatore, di una guardia giurata, di un addetto ad una centrale operativa antirapina, di riuscire a restare otto ore davanti al monitor e captare, comprendere, quello che accade, anticipatamente, al fine poi di prevenire o comunque di garantire un intervento immediato al verificarsi di tali elementi.

A mio avviso, e la nostra esperienza si sta muovendo in questo senso, il percorso è quello di creare anziché un semplice collegamento virtuale, anche se tale resterà tecnicamente, un rapporto costante tra l'operatore della centrale di videosorveglianza e l'agenzia bancaria, intensificando i momenti di controllo audio ed i momenti di contatto tra l'agenzia bancaria e l'operatore e scansionando in tempi ben definiti l'effettuazione di tutta una serie di procedure di contatto tra l'operatore e l'agenzia bancaria.

Si tratta di un momento che può garantire l'efficienza e l'efficacia del servizio e tenere all'erta l'operatore su quanto avviene all'interno dell'agenzia. Si innescano anche dei meccanismi "virtuosi" da parte dell'operatore, che arriva a "riconoscere" i clienti della banca, diventando con ciò parte della struttura agenzia bancaria.

La perplessità che tutti noi abbiamo quando vediamo o parliamo di una centrale operativa di videosorveglianza, è una perplessità reale. Il sistema, tuttavia, realizza i risultati attesi, nel senso che può effettivamente riscontrarsi, come rilevato dalla nostra esperienza, una riduzione del fenomeno delle rapine per le agenzie bancarie coperte da un sistema di videosorveglianza.

Comportamenti dell'operatore a seguito di eventi	
Acquisizione	<i>Momento in cui la rilevazione dell'evento giunge al personale della Centrale operativa antirapina</i>
Verifica	<i>Momento in cui l'operatore accerta la reale causa dell'evento</i>
Gestione	<i>Momento in cui l'operatore reagisce al verificarsi dell'evento</i>

Veniamo, con ciò, alla seconda fase, che è appunto quella della gestione, cioè il comportamento dell'operatore a seguito di eventi, che è una procedura complessa. Possiamo suddividere il comportamento dell'operatore in fasi o momenti:

acquisizione, il momento in cui la rilevazione dell'evento giunge al personale della centrale operativa antirapina, e questa fase si distingue e si differenzia in ragione del tipo di centrale operativa di videosorveglianza. Il collegamento continuo dell'operatore con l'agenzia bancaria, un operatore attento, un operatore partecipe di quello che avviene all'interno dell'agenzia, determina l'immediata percezione di un evento che sta per iniziare, quindi l'acquisizione dell'evento è un momento rilevante nella gestione di una centrale operativa antirapina e di una postazione di videosorveglianza in una centrale operativa antirapina;

verifica, cioè il momento in cui l'operatore accerta la reale causa dell'evento, cioè inizia ad avere la certezza che qualcosa si sta verificando;

gestione, che è il momento in cui l'operatore reagisce al verificarsi dell'evento, attivando le procedure di intervento e/o di emergenza. La gestione di un evento possiamo dire, mutuando poi quella che è la dottrina sulle varie tecniche di prevenzione anticrimine, è efficace allorché i tempi di segnalazione, di acquisizione e di verifica si sviluppano e si concludono quando è ancora in corso la prima fase dell'evento, cioè l'attacco.

L'operatore della centrale operativa di videosorveglianza può attivarsi, e quindi avere la percezione del verificarsi dell'evento, a seguito di specifica segnalazione dallo sportello bancario che determina l'attivazione immediata del collegamento video, ed in questo caso ci troviamo ad operare in una centrale operativa che non ha un collegamento video costante. Il momento, quindi, è determinato da una segnalazione che crea l'allerta dell'operatore, ed aziona il collegamento video e, quindi, la possibilità per l'operatore di seguire immediatamente quanto accade all'interno dell'agenzia.

Ma il momento della segnalazione può anche derivare dalla percezione dell'operatore che, verificato uno stato di allerta ed accertata l'esistenza di una situazione anomala all'interno dell'agenzia, acquisisce l'evento ed effettua una verifica tempestiva, immediata.

La gestione, quindi la reazione all'evento, si sviluppa quando è ancora in corso la seconda fase dell'azione, cioè quando la rapina non è conclusa, per parlare di un esempio tradizionale. Potremmo indicarne molti altri, con riferimento ad eventi che si verificano all'interno degli sportelli bancari perché la casistica, per la nostra esperienza, ci indica che la videosorveglianza non è soltanto uno strumento antirapina, ma è uno strumento finalizzato ad evitare tutti quegli eventi criminosi che tradizionalmente si verificano all'interno delle agenzie bancarie.

Gestione efficace	Gestione inefficace
I tempi di segnalazione, acquisizione e verifica si sviluppano quando è ancora in corso la prima fase dell'evento (<i>attacco</i>) La gestione e quindi la reazione all'evento si sviluppa quando è ancora in corso la seconda fase (<i>azione</i>)	La segnalazione, acquisizione e verifica si sviluppano quando è in corso la seconda fase dell'evento (<i>azione</i>) La gestione e quindi la reazione all'evento si sviluppa quando è ancora in corso la terza fase (<i>fuga</i>)

Una gestione inefficace dell'evento si determina quando la segnalazione, l'acquisizione e la verifica si sviluppano quando è ancora in corso la seconda fase dell'evento, cioè quando l'azione è già in atto. Siamo, perciò in ritardo e non saremo in grado di attuare una reazione adeguata.

Occorre poi prestare attenzione alle procedure che, al verificarsi dell'evento, determinano e stabiliscono la condotta dell'operatore.

L'operatore della centrale operativa di videosorveglianza, in presenza di una situazione anomala o di una segnalazione che giunga dall'agenzia, in alcun modo deve attivare il canale audio. E' una considerazione abbastanza banale, ma è una riflessione che penso venga a tutti noi. Cosa da l'operatore? Comunica con l'agenzia?

La procedura di massima solitamente seguita è quella di ripetere, al verificarsi di una segnalazione di allarme, una frase convenzionale ("siamo collegati"; "è in atto il collegamento audio video"); una frase banale che serve soltanto a "notificare", per colui che vuole compiere un'azione criminosa all'interno dell'agenzia, la presenza di un collegamento audio video.

Anche su questo potremmo disquisire, perché le teorie possono anche essere diverse e si potrebbe obiettare che questo tipo di segnalazione o questo tipo di comunicazione, comunque convenzionale, comunque non affidata alla discrezionalità dell'operatore della centrale di videosorveglianza, ma affidata appunto ad una procedura operativa concordata, prestabilita con l'agenzia, deve essere evitato. Qualcuno sostiene che sarebbe opportuno non mantenere nessun tipo di comunicazione con l'agenzia bancaria, al verificarsi di eventi che possono in qualche modo creare una reazione scomposta da parte del malintenzionato.

Ma la procedura che noi seguiamo è questa, e devo dire, per l'esperienza che abbiamo, che dà dei risultati, è efficace, non crea allarme all'interno dell'agenzia, perché c'è consapevolezza. Molto spesso, anzi, determina tranquillità all'interno dello sportello perché si ha la conferma che l'operatore sta seguendo, ha visto quello che è successo e che sono state attivate le procedure poi di intervento, di reazione, di gestione dell'evento.

I sistemi di videosorveglianza quindi hanno dei vantaggi: segnalazioni anticipate, immediata percezione dell'attacco, bassa percentuale di falsi allarmi (certezza dell'attacco, efficaci procedure di verifica contestuale).

Certamente possono emergere delle considerazioni. Segnalazioni anticipate: ma riesce sempre l'operatore ad avere "in anticipo" la percezione di quanto sta accadendo? Questo ci riconduce a quanto detto prima, cioè la necessità di rendere l'operatore stesso una presenza virtuale all'interno della banca, una parte dell'agenzia, parte della struttura nella quale svolge la sua attività. In tal senso, stiamo anche sperimentando che i nostri operatori una volta vadano a visitare l'agenzia con la

quale sono collegati per avere anche loro una percezione fisica diretta dell'ambiente con cui quotidianamente interagiscono.

E' noto come una delle problematiche più complesse che le centrali operative in genere debbono affrontare sia quella dei falsi allarmi. Esperienze all'estero, anglosassoni ad esempio, hanno ovviato al reiterarsi di falsi allarmi con una procedura di selezione dei clienti, per cui il cliente che genera un certo numero di falsi allarmi ha una minore possibilità di essere seguito dalla centrale operativa. Si determina, quindi, una discriminante nella gestione.

Il sistema di videosorveglianza azzeri i falsi allarmi, perché ha implicita una procedura di verifica immediata, sicuramente diretta, e quindi la segnalazione che perviene da una centrale operativa di videosorveglianza ha un'attendibilità fortissima e determina un'immediata attivazione della gestione e quindi dell'attivazione delle Forze dell'Ordine.

Ho vissuto personalmente alcuni di questi momenti e di queste esperienze e posso assicurare che il poter dare alle Forze dell'ordine che stanno intervenendo, ed alle strutture di pronto intervento della vigilanza privata in generale, un aggiornamento costante su quanto avviene all'interno della banca è effettivamente determinante. Si possono fornire particolari sulla descrizione dei rapinatori; si possono fornire particolari sulle armi che utilizzate, su quello che stanno facendo, sul clima che c'è all'interno dell'agenzia, cioè sul livello di tensione, quindi dare dei suggerimenti poi nell'approccio operativo e nella gestione dell'intervento.

Si è in grado, in definitiva, di fornire delle indicazioni "certe" rispetto ai tradizionali sistemi d'allarme e di segnalazione antirapina che indubbiamente presentano dei limiti ed inevitabilmente determinano una gestione "al buio" dell'intervento, in base di una telefonata che non si sa se è arrivata o se non è arrivata, di un allarme che non si sa quanto sia vero.

Progettare la gestione, la reazione agli eventi criminosi, significa rendere un sistema efficace, e qui torno al titolo di questo intervento, di questa testimonianza: individuare i collegamenti diretti e sinergie tra centrali operative antirapina e sale operative delle Forze dell'ordine, riducendo contestualmente l'incidenza dei falsi allarmi, significa concorrere alla reazione. Ci muoviamo sempre più verso un sistema di sicurezza integrato, che vuole vedere le Forze dell'ordine deputate alla cosiddetta sicurezza primaria e vuole vedere attribuite invece alle strutture di sicurezza privata un ruolo di sicurezza secondaria, di prevenzione ed avviso.

Gli eventi di questi ultimi tempi ce lo confermano, basti pensare alle evoluzioni che sono avvenute e che stanno avvenendo nella gestione della sicurezza negli ambiti aeroportuali. Il passaggio obbligato è quello di creare delle sinergie, dei collegamenti diretti, filtrando le segnalazioni come con le centrali di videosorveglianza, in modo da ottimizzare strategicamente gli interventi, per un più elevato coefficiente di efficienza e, quindi, di efficacia.

