

## LA SICUREZZA ANTICRIMINE IN BANCA: STRUMENTI E UOMINI

BRUNO AMICI

Segretario Generale A.I.PRO.S.

*La relazione era stata inizialmente predisposta da Giancarlo Guglielmi, Responsabile per circa 14 anni dell'Ufficio Sicurezza della Banca Carige, che nel gennaio 1997 è stato collocato a riposo, su sua richiesta.*

*All'amico Giancarlo, che mi ha autorizzato a prendere spunto e ad utilizzare il suo lavoro, un sincero e cordialissimo ringraziamento, con la speranza di aver saputo rappresentare il suo pensiero e con l'augurio di un lunghissimo, sereno e prospero futuro.*

L'incidenza di fatti criminosi perpetrati nei confronti del mondo bancario continua ad essere significativa, malgrado i cospicui e continui investimenti in strumenti e metodologie che le aziende fanno per cercare di prevenirli o contenerne gli effetti.

L'obiettivo di una difesa accettabilmente efficace contro il crimine è oggi perseguibile contro le intrusioni ed i furti con scasso i quali, in effetti, pur continuando a rappresentare un problema, di norma non impattano pesantemente sulle persone, come invece purtroppo spesso accade con le rapine. Fra gli strumenti e le metodologie che stanno avendo sempre più successo nel contenere questo tipo di attività criminale possiamo elencare:

- continuo sviluppo dei sistemi e delle procedure di gestione degli accessi;
- impianti di allarme evoluti, ben articolati e gestiti centralmente;
- adozione, sempre più diffusa, di strumenti complementari di sorveglianza (TVcc);
- mezziforti di accresciuta affidabilità, in linea con le nuove norme;
- sistemi di chiusura e chiavi più perfezionati ed affidabili;
- maggiore attenzione, migliorata organizzazione e norme procedurali nell'assegnazione, gestione, conservazione ed utilizzo di chiavi e duplicati;

- evoluzione concettuale e normativa nell'uso di strumenti incorporati di sicurezza (combinazioni numeriche segrete, password);
- attrezzature e apparecchiature per rendere indisponibile o inutilizzabile il numerario compendio di reato;
- interventi rapidi, attenti e ben coordinati delle Forze dell'ordine o di guardie giurate degli Istituti di vigilanza.

Per contro, non si può constatare che, in materia di rapine, siano stati perseguiti risultati, non diciamo ottimali, ma quantomeno accettabili in tema di difese e/o di limitazione dei relativi danni, salvo un certo contenimento della media del rapinato che, tuttavia, continua a mantenersi elevata e quindi ancora incentivante per la malavita. In materia di difesa antirapina sembra si debba amaramente constatare come, ancora oggi, ci siano molte soluzioni ed applicazioni interessanti, alcune delle quali indubbiamente utili, ma nessuna che possa dirsi risolutiva.

Probabilmente, stiamo ancora cercando la pietra filosofale, considerato che:

- la rapina è un atto di violenza dell'uomo sull'uomo e, come tale, ben difficilmente contenibile, specie in un contesto come il nostro;
- la sicurezza richiede strumenti e metodologie, ma soprattutto esige che siano messi in campo comportamenti attenti, coordinati ed adeguati a realtà e circostanze anche flessibili nel tempo; condizioni, queste, di non semplice attuazione;
- la sicurezza ha il grave difetto di dimostrare non la sua presenza bensì la sua assenza, come purtroppo molti dei presenti hanno dovuto almeno qualche volta constatare.

Le singolari caratteristiche della sicurezza non agevolano le possibilità di instaurare un corretto rapporto fra chi è fruitore della sicurezza e gli strumenti, fisici e metodologici, a sua disposizione per realizzarla sempre al me-

glio. Su questi aspetti di disagio relazionale, e delle cause che lo determinano, meriterebbe fosse aperto un ampio dibattito-confronto fra produttori, addetti alla sicurezza e fruitori della stessa, magari moderato da un esperto in psicologia del lavoro. Ma non è questa la sede. E' però certo che, alla radice del problema, nel quale gli elementi soggettivi prevalgono su quelli oggettivi, vi sia l'accentuato edonismo che muove e motiva il nostro vivere quotidiano dove, fatte pur salve le sempre presenti e lodevoli eccezioni, l'elementare constatazione che

**LAVORO = FATICA**

induce alla altrettanto correlazione

**MENO SI LAVORA = MENO SI FATICA**

Dobbiamo però, noi tutti, adoprarci affinché, almeno per quanto si riferisce alla sicurezza, ad un siffatto devastante sillogismo si sostituisca una molto più elementare constatazione

**QUEL POCO DI LAVORO IN PIÙ CHE MI VIENE  
RICHIESTO È UN INVESTIMENTO PER LA MIA ED  
ALTRUI SICUREZZA**

Si accennava, anche, ad elementi oggettivi che, spesso, si frappongono all'instaurarsi di un corretto rapporto fra l'uomo e gli strumenti.

Tali elementi sono:

- il prevalente orientamento al prodotto, piuttosto che al mercato, di non pochi operatori della security. Ciò ha permesso che molti prodotti posti in commercio, in sé teoricamente ottimi ai fini proposti, non si siano rivelati altrettanto utili allo scopo, perché nell'uso quotidiano hanno evidenziato carenze strutturali, errori progettuali, disallineamenti di obiettivo a volte piuttosto marcati, tali da creare barriere non agevolmente sormontabili fra uomo e macchina;
- l'azione degli addetti alla sicurezza aziendale, che quasi sempre consiste in una rincorsa dopo gli eventi, piuttosto che sostanziansi in una giusta e meditata attività di ricerca di nuovi presidi atti a migliorare le

difese contro la criminalità ed a contenere le conseguenze delle azioni delittuose.

E questo, perché? Le cause sono diverse e non sempre superabili.

Scartiamo subito la credibilità degli addetti alla security, perché faremmo ingiusto torto alla preparazione ed alla sensibilità dei funzionari bancari ed alle capacità di discernimento dei rispettivi vertici aziendali. Cosa resta? Non poco, anzi la gran parte.

1. Innanzi tutto, la sicurezza ha sempre avuto il grave torto di essere vista come un puro *centro di costo*. Gli investimenti che essa ha richiesto e richiede nel tempo sono di solito molto incisivi e ben difficilmente sono in grado di far apprezzare risultati tangibili e durevoli nel tempo. Se l'uomo della security ha lavorato bene, e pertanto l'impegno delle risorse è stato corretto e ben finalizzato, l'unico risultato tangibile, però ben difficilmente avvertito ed apprezzato da chi di dovere, sarà stato quello di aver stornato il rischio criminale su obiettivi esterni all'azienda. All'interno di questa nessuno (o ben pochi) si sarà accorto di alcunché! Questa condizione di relativa tranquillità tende infatti ad essere attribuita ad una sorta di particolare benevolenza della sorte nei confronti dell'azienda (a Roma, si dice: ci protegge Santa Pupa!) Ecco, allora, che il nostro uomo, qualora ritenesse necessari alcuni investimenti per mantenere elevata nel tempo la prevenzione anticrimine della banca si sentirebbe dire, più o meno: "ma come, non succede mai niente e Lei è di nuovo qui a chiedere altri soldi?"
2. L'attenzione al conto economico delle Aziende si sta rapidamente accentuando e ciò è dovuto:
  - alle trasformazioni in S.p.A. di banche prima operanti nel settore pubblico,
  - all'andamento generale dell'economia del Paese,
  - all'inasprirsi della concorrenza.
3. Il processo di aggregazione, che ormai sta massicciamente investendo il mondo del credito, comporta come ineluttabile conseguenza la ristrutturazione, che spesso di traduce in rilevanti compressioni, di moltis-

sime attività aziendali e, fra queste, anche la security.

4. L'entrata in vigore del D.Lgs. 626/94 ha convogliato, ed ancora convoglia, cospicue risorse, non solo umane, sulla "safety" e ciò rischia di ripercuotersi negativamente sui già magri budget della sicurezza anticrimine, a meno che, come già è avvenuto in altri Paesi, anche in Italia si decida di regolamentare anche la security, oltre alla safety.
5. Gli eventi criminali ed anche sociologici (accentuazione attività della malavita, fenomeni di terrorismo, particolari turbolenze ambientali) possono, a loro volta, stimolare momenti di attenzione particolare all'interno delle aziende; momenti che però, vista la loro stessa natura, non possono che caratterizzarsi per un andamento ondivago (facciamo! stiamo fermi! riduciamo!) e comunque hanno il vizio di origine dell'emotività e sono condizionati dalla estrema urgenza. E la gatta frettolosa fa i gattini ciechi!

Comunque sia, oggi più che mai, appare sempre più arduo chiedere risorse all'Azienda al fine di sostenere azioni puramente preventive in tema di security. Generalmente ci si muove soltanto, per dirla in termini calcistici, di rimessa. Succede un qualcosa che ha determinato un danno ed ecco che l'uomo della sicurezza, di solito, è chiamato a "relazionare in merito" e, al più presto, proporre *qualcosa* che metta al riparo l'azienda da ulteriori incidenti del genere.

Però attenzione, quanto proposto dovrà:

- essere scovato in fretta (magari per ieri),
- costare poco (meglio se niente),
- dimostrarsi innovativo ed efficace.

\* \* \*

Dopo queste riflessioni, è opportuno affrontare il problema **rapine**, con un rapido excursus su quanto storicamente fatto per prevenirle o contenerne gli effetti. Per molti dei miei ex colleghi bancari, professionisti ben sperimentati nel settore, sarà una trita e ritrita materia, ed a costoro vanno le scuse più sentite per l'inutile perdita di tempo. Ma, oltre che "repetita .... juvant", può tornare utile una rapida ricognizione storico-critica su cosa è

stato sinora realizzato in materia di sicurezza antirapina in ambito bancario per coloro che alla materia si sono affacciati da poco o per coloro che la vivono dal di fuori e, per ciò stesso, non avendo di fronte quotidianamente questo tipo di problematiche, e tutte le problematiche, potrebbero non averne colto il giusto significato.

La prima difesa "storica" che le banche hanno adottato contro le rapine è stato il ricorso al presidio di guardie giurate. Siamo all'inizio degli anni settanta e subito dopo sono arrivate le bussole. Penso che tra i bancari presenti non ce ne sia uno che non le abbia viste e sperimentate pressoché tutte: girevoli, scorrevoli, a battente, con e senza metal detector, ad uno o più varchi, manuali, gestite ed autogestite! E mi scuso se ho dimenticato qualche tipologia.

Il metal detector (specie nelle prime generazioni) ha sollevato problemi di gestione e di taratura, di influenza di campi magnetici interni ed esterni; ma l'errore stava nel considerare il metal detector come sistema antirapina, e non lo è mai stato! Ma per diversi anni ha facilitato le difese: ma non da solo!

Per oltre un quinquennio (1982-1988) ci eravamo illusi di aver imboccato la strada giusta, dal momento che, statisticamente, gli eventi diminuivano. Sono, però, arrivati (guarda caso, in coincidenza con alcuni provvedimenti legislativi) i rapinatori privi di armi da fuoco ed allora il metal, per siffatte tipologie di evento, poteva anche non esserci. Ma per la sua presenza, almeno, contiamo meno feriti e vittime tra clientela e personale.

Sul finire degli anni ottanta e negli anni novanta si sono prepotentemente affermati i sistemi di contenimento del danno. Oltre ai sistemi di inchiostrazione o colorazione dei valori asportati, anche ai fini antirapina sono stati maggiormente utilizzati temporizzatori e ritardatori, per altre applicazioni già presenti da tempo, ed ha preso piede l'adozione di sistemi di custodia per cassieri che, al giorno d'oggi, hanno sì una vasta diffusione ma incontrano ancora una scarsa accettazione, anche ad onta di normative aziendali più o meno rigidamente impostate, da parte del-

l'operatore di sportello. Ciò, fondamentale per ragioni

- *oggettive*: il flusso di contante allo sportello a volte ha un andamento esasperato per cui i tempi di ritardo programmati, specie se elevati, costituiscono un indubbio ostacolo all'operatività;
- *soggettive*: il cassiere sente la necessità di avere un contatto diretto e continuo con il denaro di cui ha la responsabilità. L'uso di tempi di ritardo costituisce un ostacolo a detti fini e, pertanto, egli non lo accetta facilmente.

Un diverso impatto nel personale, in genere positivo, ha invece trovato la videoregistrazione, in uso da molti anni, una volta superata e chiarita l'assoluta estraneità di tale soluzione per il controllo del lavoratore. Anche perché l'impegno gestionale è mediamente contenuto e perché l'effetto rassicurante sulle persone è piuttosto alto. Alla ricostruzione dell'evento, infatti non si ricorre soltanto in caso di rapina, ma anche a seguito di altri "minori" eventi, quali furti e truffe allo sportello (anche a danno della clientela), frodi a mezzo bancomat, ricorsi della clientela (presunti errori contabili e/o scambio di contante allo sportello).

Sembra però necessario rimeditare su alcune "certezze" che, per diverso tempo, hanno imperato all'interno delle banche, visto che gli attacchi della criminalità, e nello specifico le rapine, non diminuiscono, tutt'altro. E quelle "certezze" si stanno ormai velocemente sgretolando. Le cause del cambiamento sono molteplici, ma fra le più accreditate o accreditabili troviamo:

- a) il lavoro di sportello tenderà sempre più a svolgersi in ambiente "aperto", invitante, ospitale, quasi familiare, nel quale sia stimolante entrare e piacevole intrattenersi; caratteristiche queste in stridente antitesi con talune concezioni fin qui prevalse, basate sull'arroccamento, sulle blindature interne, sugli accessi controllati. Strumenti e metodologie che, come tutti ben sappiamo, si sono dimostrati utili per un certo tempo, per essere poi ben presto superati e neutralizzati dall'inventiva, dalla determinazione e dalla violenza messe in campo dai malviventi, a fronte delle quali non è stato e non sarà mai verosimilmente pos-

sibile contare su altrettanto efficaci iniziative di contrasto da parte del personale delle banche, per ragioni che tutti noi ben conosciamo;

- b) ogni proposta che l'addetto alla sicurezza di una banca fa per aumentare i livelli di sicurezza della propria azienda deve, e dovrà, sempre più caratterizzarsi per
- concreta efficacia nel perseguimento dell'obiettivo;
  - semplicità dei comportamenti attesi dal personale in genere e richiesti a chi sarà chiamato a gestire le soluzioni adottate. In altri termini, l'incidenza dei comportamenti per la security dovrà essere la più moderata possibile;
  - contenimento dei costi (di acquisto, installazione, gestione e manutenzione);
  - "pay back" molto accentuato; si deve cioè poter dimostrare ai vertici aziendali che gli investimenti richiesti per la security andranno ad eliminare altre spese per cui, non appena ammortizzati, l'azienda, oltre a vedere aumentato il proprio livello di sicurezza, ne ricaverà un concreto beneficio;
  - corretta impostazione delle relazioni interne con i vertici aziendali, evitando, nella richiesta di risorse, l'uso di particolari accentuazioni, sottolineature e, men che mai, il ricorso a vaticini catastrofici in caso di riconsolazione.
- c) l'attuale incidenza delle difese umano-metodologiche consistenti, in prevalenza, nei servizi offerti da Istituti di vigilanza (presidi fissi e/o saltuari, trasporto valori, interventi su allarme, ronde e pattugliamenti, ecc.) tenderà ad attenuarsi, evolvendosi peraltro verso forme di collaborazione tecnologicamente e professionalmente più avanzate.

\* \* \*

Dopo la storia "critica" sugli strumenti, pensiamo agli uomini, ai nostri uomini, per vedere cosa sia ancora possibile e doveroso fare per migliorare il loro rapporto con gli strumenti che potremmo mettere a loro disposizione, per garantire la loro sicurezza nonché quella dell'Azienda nel suo complesso.

E' indispensabile, anzitutto, demolire concetti quali quello della "sicurezza assoluta", da

considerarsi devastanti e di cui spesso i media si fanno portavoce. E' importante far capire che, quando si parla di sicurezza, ci si riferisce **sempre** ad una condizione mediata fra rischio, o pericolo, temuto e la possibilità che esso si traduca in danno. Quindi, la sicurezza è un compromesso; il migliore possibile o ottenibile, ma pur sempre un compromesso.

Dobbiamo, poi, spiegare e far recepire che la sicurezza è un modo di essere e di pensare che riguarda tutti; e **tutti** devono contribuire a raggiungere o soprattutto a mantenere.

Cosa mettere in campo a tale riguardo, a parte la normativa scritta che è certamente utile per coloro che la conoscono e la osservano, ma che purtroppo sono un'esigua minoranza, a fronte della generalità dei soggetti che non ne sospetta neppure l'esistenza? Occorre qualcosa di più e di diverso di quanto è stato fatto finora per riuscire nell'intento, almeno in gran parte delle banche. La risposta non può essere che una: **formare ed informare il personale.**

### **Formazione**

Presso alcune banche, da qualche anno, nei corsi di formazione, o di orientamento, per neo assunti sono state inserite anche tematiche di sicurezza. Si tratta, per lo più di mezza o una giornata dedicata alla trattazione di tutti o alcuni degli aspetti di *safety* (D.Lgs. 626/94, precedente normativa e successiva integrazione) e di elementi di *security*.

Soffermandoci sulla *security*, cosa illustrare nel poco tempo messo a disposizione? Dopo un rapido cenno ai substrati del concetto "sicurezza", esplicitando il significato di rischio e pericolo, si deve passare a concetti più specifici, quali la sicurezza integrata, il rischio marginale, i limiti (ed i costi) della sicurezza.

Facendo ricorso ad indispensabili sussidi audiovisivi, andranno descritte:

- a) le varie (o almeno le principali) applicazioni di sicurezza, motivandone (quando e perché) l'adozione ed evidenziando i limiti applicativi ed i rischi in caso di utilizzo improprio;
- b) le speciali metodologie ed i comportamenti richiesti ed attesi a seconda

- dei momenti della giornata lavorativa,
  - del tipo di operatività svolta,
  - del manifestarsi di particolari esigenze (gestione valori, rapporti con gli addetti degli Istituti di Vigilanza, attenzioni e cautele da adottare in caso di presenze sospette, ecc.)
- c) le norme fondamentali che regolano e disciplinano la *security* nell'azienda;
  - d) quali siano i servizi svolti dalle guardie giurate ed il loro "status";
  - e) i rapporti che devono essere tenuti con le Forze dell'ordine.

In questa stessa fase di formazione non dovrebbe mancare la visione di un filmato che rappresenti lo svolgimento una rapina in banca. Analizzando e commentando le varie fasi sarà possibile trasmettere un'informazione appropriata sulla dinamica-tipo di un simile evento ed evidenziare i comportamenti errati, inesatti o controproducenti, illustrando invece quali siano gli atteggiamenti consigliati durante l'evento e quelli da tenere successivamente allo stesso, anche nei rapporti con le Forze dell'ordine e con gli organi centrali della banca.

Ma la formazione non sarà completa se non integrata con un dibattito aperto, e libero, ed alle domande non sarà possibile sottrarsi con risposte generiche o elusive e, men che meno, con imposizioni!

### **Informazione**

E' bene distinguere l'informazione urgente da quella non urgente. La prima è, ovviamente, tanto più efficace quanto più rapidamente viene portata a conoscenza di tutti gli interessati. Perché questa distinzione? Per un aspetto non secondario di legittimazione nell'assunzione di iniziative dirette da parte dell'uomo della *security*, che in ciò dovrebbe essere facoltizzato dalla Direzione.

L'uomo della *security*, infatti, mentre ha il compito di ispirare atti normativi formali e non urgenti, quali ad esempio le disposizioni di servizio, le circolari, i manuali relativi all'uso di sistemi, impianti ed apparecchiature, la prestazione di servizi, il ricorso a determinate procedure e/o metodologie di lavoro, di norma non può redigere e rendere cogenti

tali atti, il cui "imprimatur" è riservato alla Direzione, o alla funzione organizzativa. Queste tipologie del sistema di comunicazione aziendale, quindi, non possono sottrarsi all'iter procedurale ed alle formalità che ne discendono in quanto a:

- modalità e percorsi di emanazione;
- autorità dalle quali promanano;
- strutture o soggetti ai quali si rivolgono;
- materia trattata;
- decorrenza e periodo di validità.

Nel campo della prevenzione anticrimine ci sono però momenti "critici" che richiedono il massimo di attenzione e l'immediata mobilitazione di risorse, per poter essere positivamente superati. E' perciò di tutta evidenza che la conseguente reazione, per essere della massima efficacia, non debba soggiacere a formalità procedurali di alcun genere, pena l'insuccesso. Ecco, allora, che all'uomo della security debbono essere attribuiti poteri autonomi di informazione tali da poter efficacemente contrastare le iniziative criminali al loro manifestarsi.

E' questo il tipo di informazione nel quale la sostanza e l'immediatezza della diffusione possono e devono prescindere da aspetti di rigore formale e d'impronta gerarchica della sua connotazione. L'essenziale è che queste comunicazioni siano rapidamente diffuse alla rete di uffici e sportelli potenzialmente interessati ai problemi che, tempo per tempo e caso per caso, vengono ad evidenziarsi. Di solito, può trattarsi di segnalazioni riguardanti:

- accesso nei locali di soggetti presuntivamente mossi da intenti criminosi (preparazione di rapine, tentativi di truffe e/o furti con destrezza)
- movimenti sul territorio di soggetti dei quali è provata o nota l'attività criminale (furti e/o truffe ricostruiti grazie alla videoregistrazione)
- necessità di richiamare l'attenzione su aspetti di "criticità" generica spazio-temporale (giornate e/o orari e/o aree territoriali a rischio, flussi eccezionali di contante da tenere sotto accentuato controllo, particolari ed estemporanee cautele, temuti eventi catastrofici, ecc.)

- interventi sul territorio, per esigenze tecniche di carattere estemporaneo, da parte di soggetti diversi per espletamento di attività quali il controllo e la verifica di apparecchiature ed impianti, l'attività di manutenzione a chiamata su impianti e sistemi, l'attività di manutenzione programmata su impianti e sistemi.

Per la divulgazione delle comunicazioni di questo tipo ci si potrà avvalere, in relazione ai diversi sistemi di comunicazione esistenti nella banca, di posta elettronica (o similare) se il messaggio investe la generalità o un buon numero di uffici o sportelli; di telefono o telefax per comunicazioni destinate ad un limitato numero di interessati.

\* \* \*

Ma non è tutto, per quanto concerne l'uomo. Abbiamo visto gli aspetti interni al nostro sistema, non anche quelli esterni. Su un'ipotetica bilancia, questi ultimi hanno il maggior peso e sarà sempre molto difficile far bilanciare i due piatti.

Non è in questo momento che possiamo analizzare tutti gli aspetti esterni (consulenza, progettazione, fornitura, installazione, manutenzione, vigilanza, ecc.). Tuttavia, in questo stesso Convegno ne verranno affrontati diversi, a cominciare da quello attinente alla progettazione, argomento trattato dall'ing. del Conte nell'intervento subito successivo.

A mio avviso, per concludere, fra di noi possiamo discutere ed approfondire tutti gli apporti dei diversi attori elencati, tranne uno: il malvivente, per assenza dell'interessato!

Vorrei chiudere con una parabola, rubata all'amico Tomeo della Banca Antoniana Popolare Veneta.

Se in un'ipotetica città si verificasse un'eruzione o una fuoruscita di sostanze magnetiche o gassose, molto verosimilmente l'intervento che verrebbe attuato sarebbe quello di impedire l'eruzione del magma o la fuoruscita del gas, "tappando" il buco. L'eruzione si ripete a qualche metro (o chilometro) di distanza e viene chiusa anche la seconda bocca. E così di seguito. Ma perché non intervenire sulle cause che determinano l'eruzione?

Trasponendo l'esempio, occorrerebbe intervenire sul contesto sociale, si da far venir meno l'evento "rapina", rimuovendo le cause socio-economiche che lo determinano; ma noi non abbiamo certamente questo potere. Possiamo solo cercare di contrastare

l'evento, di contenerlo, attuando al meglio le difese e per far ciò non possiamo che fare affidamento sull'efficace apporto dell'**Uomo**. Elemento essenziale di qualsiasi sistema di sicurezza.