

TAVOLA ROTONDA

“Abbiamo parlato della sicurezza sotto vari profili. Possiamo parlare un attimo delle prospettive, viste anche da chi è in contatto con le Istituzioni, il Consumatore, i Giovani?”

I

Chairman:

Ing. Anthony Cecil Wright, Presidente ANSSAIF

Interventi di:

Dott. Fabio Picciolini, Segretario Gen.le ADICONSUM

Dott. Elio Ciaccia, Consigliere CNEL e Presidente

SImpresa

Prof. Michele Crudele, Direttore del Centro ELIS

Dott. Fabio Picciolini

L'intervento del dott. Picciolini focalizza la sua attenzione sulla tipologia di *comunicazione* tra le strutture, quali anche la Banca e il mondo dei consumatori.

In particolare la domanda principale che proviene più frequentemente dal mondo dei consumatori è se *la Banca possa essere considerata effettivamente sicura*.

Considerando che il sistema bancario italiano è uno dei più sicuri, ne deriva che forse esiste un problema di comunicazione tra Banca e Clienti, ovvero c'è discrasia tra l'intermediario e il cliente finale.

Il dott. Picciolini incentra la discussione in particolare su due aspetti:

1. c'è paura che un conto on-line non sia sufficientemente sicuro. Pertanto c'è diffidenza nell'usare la carta di credito anche per fare delle semplici operazioni on - line.
2. esiste un problema assicurativo: nella maggior parte dei casi, in occasione del verificarsi di problemi relativi all'utilizzo della carta di credito da parte di un cliente, ad esempio per smarrimento o clonazione della stessa, per la banca la causa è sempre da ricercare nel cattivo utilizzo da parte del cliente, onde evitare il risarcimento. Si potrebbe immaginare, pertanto, una forma di assicurazione collettiva, finalizzata a tutelare il cliente da eventuali perdite non attribuibili a sue colpe.

Un esempio relativo al problema di comunicazione è relativo al libretto informativo che l'ABI sta predisponendo per la diffusione alla clientela bancaria relativo all'utilizzo del sistema obbligatorio IBAN.

Tale libretto, visualizzato prima della pubblicazione da ADICONSUM, è risultato non del tutto chiaro per il consumatore medio, ma ha evidenziato la possibilità di miglioramenti attraverso rapporti costruttivi tra Associazioni dei Consumatori e ABI.

Le soluzioni, al fine di far sentire il cliente più vicino alla realtà bancaria, sono state di:

1. utilizzare il "tu" al posto del "lei";
2. fornire, già dalle prime pagine del testo informativo, la definizione chiara e dettagliata di alcuni termini che, se posticipata numerose pagine dopo, renderebbero incomprensibile il contenuto del testo ed inefficace la comunicazione.

Dott. Elio Ciaccia

Il dott. Ciaccia porta come testimonianza la sua esperienza di membro del Consiglio Nazionale dell'Economia e del Lavoro.

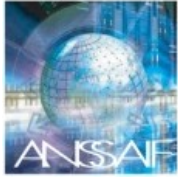
Le attività del Consiglio permettono l'attivazione di tavoli di confronto tra persone di elevata professionalità accomunate da analoghi interessi ed obiettivi.

Alcuni esempi di argomenti trattati riguardano:

1. la globalizzazione della finanza e le relazioni fra questa e le esigenze di sviluppo di aree che interessano il sistema paese;
2. la dematerializzazione nei flussi documentali ed amministrativi (ad esempio per ordini, consegna, fatturazione, pagamenti) in modo tale da ottenere un innalzamento qualitativo dei relativi processi.

L'Italia è un paese formato principalmente da piccole-medie imprese che si pongono sul mercato in forme organizzative di filiera o di distretto. Al fine di sviluppare ulteriormente la loro posizione sul mercato è necessario rafforzare le relazioni tra clienti e fornitori instaurando rapporti basati in misura crescente sulla fiducia e sulla sicurezza.

Gli elementi che danno certezza sull'identità di ogni soggetto che opera sul mercato forniscono fiducia e concorrono allo sviluppo.



Due fattori sono in proposito di rilevante significato:

1. la promozione della cultura della sicurezza tra i soggetti che hanno responsabilità verso e nelle comunità di business e più in generale della collettività;
2. la valutazione di come figure specialistiche quali quelle che si riconoscono nell'associazione ANSAIF possano contribuire alla diffusione del valore della sicurezza come fattore competitivo.

Prof. Michele Crudele

L'intervento del prof. Crudele focalizza l'attenzione sul tema relativo alla consapevolezza, da parte dei giovani, sulla sicurezza.

È necessario nell'analisi della situazione distinguere gli adolescenti dai bambini.

I primi sono ragazzi che utilizzano le tecnologie senza freni e non danno importanza alla sicurezza, se non quando vedono rischi immediati di perdere soldi. Non percepiscono il valore economico dei beni immateriali (documenti, musica, film) ai quali accedono con strumenti leciti e illeciti. Il problema deriva anche dal cattivo esempio dei genitori, che non esitano a utilizzare Internet per scaricare canzoni e film.

A suo avviso non è più possibile recuperare il livello di legalità di questa categoria di ragazzi (salvo casi personali), in quanto troppo esposta alla negatività (pirateria, violenza, erotismo). L'esposizione continua alla negatività porta alla perdita di sensibilità, a tal punto da non far percepire più il fatto di fare qualcosa di non corretto o illegale.

I bambini, invece, hanno ancora la possibilità di essere educati alla legalità informatica, in modo tale da far capire loro la differenza tra cose "buone" e cose "cattive". È necessario farla percepire come valore etico e non come semplice rispetto di regole stabilite da un'autorità civile, visto che le norme cambiano da Paese a Paese.

La proposta che ne deriva è quella di effettuare una "campagna di educazione alla legalità informatica" rivolta ai maestri delle scuole primarie per arrivare ai bambini. Infatti questo processo educativo non può condotto dai genitori di oggi, che non sono in grado di insegnare il retto uso dell'informatica e delle telecomunicazioni, sia per ignoranza, che per cattiva abitudine.

Il rischio è che anche i genitori di domani (attuali adolescenti) siano cattivi maestri, perché abituati alla negatività di oggi. Perciò le energie formative dovrebbero essere concentrate sui maestri.

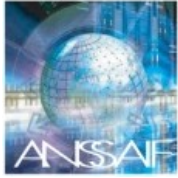
Interventi

- Si potrebbe allargare il discorso della legalità non solo agli aspetti informatici, ma anche al resto. Ci sono troppi comportamenti illegali da parte degli adulti.

- Con riguardo ai sistemi di pagamento, va detto che molte cose stanno cambiando in senso positivo, anche per effetto degli incisivi interventi normativi e delle Autorità di controllo. Nel rapporto banca/cliente, va sicuramente migliorato il sistema di comunicazione, rendendolo più semplice e trasparente; le stesse banche ne trarrebbero benefici sul piano dell'efficienza operativa attraverso la riduzione degli oneri connessi alla gestione dei reclami e del relativo contenzioso (al riguardo pesano anche inadeguati comportamenti e/o inadempienze da parte delle associazioni dei consumatori, come, ad esempio, sull'applicazione della normativa sui bonifici cross-border). La trasparenza è prevalentemente come un adempimento normativo (compliance alle leggi e alle normative di Vigilanza), mentre sono ancora deboli i passi verso la sua attivazione come efficace leva per la fidelizzazione della clientela e il miglioramento dei servizi offerti.

- In tema di singoli strumenti di pagamento, è in atto un'intensa azione tesa a elevare la qualità dei servizi resi, ancorata ad approcci end-to-end e a uno stretto monitoraggio dei risultati finali del funzionamento dei diversi circuiti. Significativi gli interventi attuati, o in corso, in materia di assegni e bonifici. Sui primi rileva la fissazione di un limite massimo di 7 giorni alla loro "disponibilità" (destinato a ulteriori abbassamenti), che ha eliminato l'ampia e ingiustificata disparità tra banche (con punte vicine ai 20 giorni). Sui bonifici, la SEPA e la recente Direttiva comunitaria sui sistemi di pagamento spingono verso l'applicazione di condizioni di maggiore certezza e tempestività sulla loro esecuzione, fissando in tre giorni il termine di esecuzione (da ridurre gradualmente a uno) e regolando in modo trasparente adempimenti e responsabilità dei diversi partecipanti al servizio (con formalità prossime al riconoscimento di una "responsabilità oggettiva" in capo all'intermediario ordinante).

- Un cenno a parte merita il problema delle frodi sulle carte di pagamento, in aumento specie in quelle di debito. Raramente esse si sono tradotte in perdite per il possessore della carta; la chiara emersione di punti di vulnerabilità presso i merchant sono alla base di recenti interventi, incentrati sul potenziamento e sull'incentivazione dei meccanismi di sicurezza (eliminazione dei terminali più a rischio e adozione di nuove specifiche di sicurezza) e sulla connessa revisione delle regole di attribuzione delle responsabilità e delle perdite subite (attivazione della liability shift e revisione del sistema di autoassicurazione); decisiva, al riguardo, si prospetta una più rapida e regolare migra -



zione al microcircuito, che impegna sia le Autorità sia i diversi partecipanti al circuito. Da ultimo, è assai significativa, al riguardo, l'istituzione presso il Ministero dell'Economia – Ufficio Centrale Antifrode sulle carte di pagamento (UCAMP) di un archivio per la prevenzione delle frodi su carte di pagamento.

Un aspetto particolare attiene alla funzionalità del circuito POS, la cui resiliency si è fatta cruciale a seguito della concentrazione dei punti di acquisto e del rapido sviluppo dei pagamenti via Pagobancomat. Ripetuti incidenti di fermo del circuito e talune criticità legate al complesso sistema autorizzativo inducono ormai a considerare attentamente il problema della continuità di servizio del circuito, valutando i necessari interventi tecnico-operativi atti a isolare i punti di crisi e a circoscrivere al massimo gli effetti sistemici di eventuali malfunzionamenti (tra cui l'introduzione, in uno con l'attivazione del "microcircuito", di sistemi di autorizzazioni off-line).

- Forse esiste un problema nella multicanalità, anche se questo fa parte della concorrenza dei prodotti. Le tecnologie stanno evolvendo, ma non sempre sono riconosciute e usate dai consumatori. Il problema pertanto, consiste nella mancanza di garanzie sul rispetto di certi standard di sicurezza da parte dei fornitori di servizio. La soluzione da parte delle banche, potrebbe trovarsi nell'informare il pubblico sull'esistenza di un livello minimo di sicurezza al di sopra del quale il cliente dovrebbe sentirsi sicuro e stare tranquillo. L'incremento del livello di sicurezza potrebbe innalzare il livello di fiducia riposta dal cliente nella banca, anche supportato dal fatto che, in caso di inefficienze, dovrebbe essere la banca stessa a risponderne.

Intervento prof. Marco Strano - ICAA

"Attacchi dall'esterno e dell'interno dell'Azienda: profili criminali, rischi e possibili contromisure"

L'intervento del Prof. Strano pone l'attenzione sugli attacchi all'azienda, che possono essere distinti in due categorie, esterni ed interni.

Ad oggi, l'analisi degli attacchi esterni è costituita da due filoni di ricerca:

1. **Preventivo**, che prevede l'osservazione e lo studio di un campione di soggetti sui quali viene applicata una strategia di analisi per comprendere il livello della percezione del crimine e della sicurezza che questi soggetti hanno; tale livello viene poi misurato per poter intervenire con formazione mirata seguita da possibili verifiche sull'effettiva diminuzione del rischio di un crimine.
2. **Consuntivo**, ovvero cosa fare nel momento in cui è già successo il crimine, vale a dire se la prevenzione non è stata efficace. Tale filone si chiama CRIMINAL PROFILING. Attualmente, però, sul tema dei crimini informatici c'è poco materiale anche perché in Italia sono gli unici psicologi ad occuparsi di tale argomento.

Quando si parla di scienze forensi in campo digitale servono comunque metodi standard per l'acquisizione di prove che, insieme a studi e procedure, rappresentano una prassi che tutto il mondo sta percorrendo.

Prove, studi e procedure sono competenze che si trovano sempre.

A questi elementi di analisi, poi, ne andrebbe aggiunto anche un quarto: il Criminal Profiling.

In particolare, nel momento in cui si chiede una prima opinione sul possibile autore del crimine, il gruppo ICAA offre, a chi non è psicologo ma solo un forense, degli strumenti di supporto per il loro lavoro.

La filosofia del profiling prevede che si cerchi di individuare le persone che più di altre hanno le caratteristiche del possibile autore del crimine. Proprio in quanto ipotesi, non vengono eliminati gli altri sospetti, ma si parla di "gerarchizzazione dei sospetti".

Su tale argomento esistono due scuole di pensiero:

1. *offender profiling*: in caso di reato, cerca di capire il profilo di chi ha commesso il crimine. Si parla pertanto di "analisi del comportamento", svolta mediante la creazione di indicatori di comportamento. Ad esempio, nel caso di un dipendente con un