Intelligence in azienda con risorse interne: il perimetro di legalità

Ing. Alessandro Siazzu

20 settembre 2006, dal quotidiano La Repubblica: *"Si fanno sempre più complicati i contorni dell'inchiesta milanese sull'*affaire *che coinvolge il Settore Security di Telecom... Le manette sono scattate alle prime ore del mattino... Ci sono diversi ex manager [Telecom, ndr], vari pubblici ufficiali... I PM milanesi hanno firmato ordinanze anche per associazione a delinquere, corruzione, violazione della privacy, falso, riciclaggio e appropriazione indebita".*

Con queste scarne righe, il pubblico veniva al corrente, per la prima volta in modo così eclatante, dei problemi di legalità relativi allo svolgimento di attività di *intelligence* all'interno delle aziende italiane. Tali attività, che vanno sotto il nome di *Competitive Intelligence* o *Intelligence* Economica o *Business Intelligence*[1], sono eseguite con finalità di supporto al *business* e al processo decisionale del *management*, ad esempio quando si decide di entrare in una *partnership* industriale strategica o di selezionare un nuovo importante fornitore. Scopo di questo studio è la definizione del perimetro entro il quale queste attività possono essere svolte dai dipendenti senza incorrere nel compimento di reati. In altri termini, si è cercato di stabilire il confine tra l'attività di raccolta delle informazioni, svolta con mezzi leciti, e lo spionaggio industriale vero e proprio. Partendo dall'esperienza di una delle più grandi multinazionali italiane, sono state esaminate due diverse tipologie di report di *intelligence*: una con *focus* sull'analisi di aziende ed organizzazioni (*competitor*, fornitori, altre controparti); l'altra orientata allo *screening* di persone fisiche (es. per collaborazioni di professionisti o candidati all'assunzione). Successivamente, sono stati individuati i rischi connessi alla possibilità di compiere reati nella fase di raccolta delle informazioni. Al fine di mantenere la massima riservatezza sulle operazioni, oltre che per ragioni di convenienza economica, l'ipotesi presa in considerazione è che questa attività sia eseguita da personale interno, senza ricorrere al supporto di società specializzate in materia o investigatori privati muniti di licenza. Per ogni reato, poi, sono state definite una serie di prescrizioni atte a mitigare il rischio di violazione delle normative, che, se messe in atto, consentono alla risorsa interna di operare in condizioni di piena salvaguardia legale. Di seguito, viene illustrata una sintesi delle regole cui attenersi nella fase di raccolta delle informazioni: il dipendente non deve impiegare modalità tipiche della professione di investigatore privato (pedinamento, appostamento, camuffamento, riprese audio-video, tracciamento con localizzatori GPS), per non incorrere nel reato di esercizio abusivo di tale professione; può utilizzare tutte le fonti aperte, inclusi i *social media*, purchè impieghi *account* riconducibili all'azienda, facendo uso eventualmente di funzionalità di navigazione anonima; deve astenersi dall'impiego di tecniche di *hacking* di sistemi informatici protetti e di intercettazione delle comunicazioni (e, naturalmente, evitare di commissionare incarichi ad *hacker* o esperti di intercettazioni); deve evitare il trattamento di informazioni la cui riservatezza è protetta dalle normative sul segreto (segreto di Stato/NATO-UEO, segreto nella corrispondenza e nelle comunicazioni, segreto professionale, scientifico ed industriale, segreto investigativo, segreto amministrativo/d'ufficio); deve astenersi dal corrompere, o comunque coinvolgere, anche tramite terzi, pubblici ufficiali con lo scopo di ottenere informazioni riservate o privilegiate accessibili da questi ultimi in virtù del proprio ruolo. Viene, inoltre, dato risalto agli adempimenti relativi alla normativa sulla *Privacy*, nel caso in cui le informazioni raccolte contengano dati personali riconducibili a singoli individui. Infine, sono state distinte le fonti utilizzabili da quelle non utilizzabili perchè considerate riservate ai sensi della legge italiana. La ricerca ha, dunque, raggiunto l'obiettivo di fornire una definizione chiara, puntuale e pratica del perimetro di legalità nell'esecuzione di attività di intelligence in azienda con risorse interne, riducendo al minimo il rischio legale per i dipendenti e per l'impresa, e consentendo di sfruttare al massimo le potenti tecniche di raccolta delle informazioni da fonti aperte (OSINT) a supporto del *business*.

[1] Da non confondere con *Business Intelligence* intesa come elaborazione, analisi e presentazione di grosse moli di dati interni provenienti dai sistemi informatici aziendali.