

ALLE PRESE CON NUOVI RISCHI

di GIACOMO CORVI

L'ATTUALE CONTESTO GLOBALIZZATO INCREMENTA L'INCERTEZZA E LE MINACCE PER LE AZIENDE. FARE IMPRESA OGGI, COME EMERSO NEL CORSO DI UN CONVEGNO DI CINEAS, SIGNIFICA ANCHE CONOSCERE E PRESIDARE TUTTE LE AREE DI RISCHIO CHE POSSONO RIPERCUOTERSI SULL'OPERATIVITÀ AZIENDALE



Tutto connesso, tutto globalizzato. Al punto tale che oggi, come insegna la teoria dell'*effetto farfalla*, anche il più piccolo cambiamento in Asia o America può avere pesanti ripercussioni in Europa. Solo che qui la teoria c'entra poco: tutto è reale e concreto, nella quotidianità di un'impresa che si trova a fronteggiare pericoli che prima potevano essere serenamente trascurati. Rischi nuovi o emergenti, sostanzialmente sconosciuti, che necessitano ora di rigoroso approfondimento per garantire la normale operatività di un'azienda.

Il monito arriva dal convegno *I nuovi rischi e l'impatto sulla governance delle imprese*, promosso da **Cineas** in collaborazione con **Munich Re**. "Il presidio del rischio operativo deve salire di un livello, arrivando all'attenzione dei consigli di amministrazione", ha esordito **Massimo Michaud**, presidente del consorzio universitario, nell'intervento introduttivo della mattinata di dibattito e confronto, che si è tenuta lo scorso aprile nell'aula magna del Politecnico di Milano. "Si tratta – ha aggiunto – di questioni che hanno impatto sull'immagine e sulla reputazione dell'azienda, nonché

sulla responsabilità del management: serve un nuovo modello di gestione del rischio che ridefinisca ruoli e processi per arrivare a un più efficace sistema di prevenzione e mitigazione delle minacce".

BUFALE, FARFALLE E CIGNI NERI

E di minacce, in un mondo connesso e globalizzato, pare esserci abbondanza. A cominciare da un contesto geopolitico in perenne fibrillazione, in cui tutto deve diventare oggetto di presidio perché tutto cambia giorno dopo giorno. A differenza di quello che poteva essere 15 anni fa, ha fatto notare **Paolo Magri**, vice presidente esecutivo dell'**Ispi**, "il rischio geopolitico non è più lontano, contenuto e isolato". E così può capitare che le sanzioni imposte alla Russia per l'annessione della Crimea possano avere ripercussioni sul fatturato dei produttori agricoli australiani. O che ancora, più recentemente, la scelta di introdurre la *sharia* nel sultanato del Brunei possa generare una campagna di boicottaggio contro l'hotel **Principe di Savoia** di Milano. "Dobbiamo imparare a orientarci fra bufale, farfalle

IMPARARE A GESTIRE UNA CRISI

Azzerare il rischio è impossibile. E quando il rischio si trasforma in danno, è bene avere a disposizione strumenti adeguati a gestire la crisi. È il consiglio che arriva da **Lorenza Pigozzi**, direttore comunicazione del gruppo **Mediobanca**, la quale si è focalizzata soprattutto sul danno di immagine e reputazione che può scaturire da una crisi. “Secondo uno studio del **Reputation Institute** – ha affermato – nel 2015 l’84% del valore di Borsa delle imprese è dato da asset intangibili”. Il brand diventa dunque un nuovo elemento di presidio, da salvaguardare con una narrazione che sappia diffondere la filosofia dell’azienda, fidelizzare il cliente e attutire, anche dal punto di vista economico, i contraccolpi di un’eventuale crisi. “Oggi – ha concluso – i risultati economici arrivano anche da investimenti in comunicazione”.

e cigni neri”, ha affermato Magri. “Senza trascurare – ha aggiunto, proseguendo nella metafora zoologica – l’*elefante nella stanza*: il mondo sta cambiando, il primato dell’assetto occidentale sta venendo meno e ciò può in parte spiegare fenomeni nuovi come la diffusione del populismo, l’elezione di **Donald Trump** e il referendum sulla Brexit”.

CYBER, RISCHIO SENZA REGOLE

Altro fronte caldo è quello del cyber risk. E lo è soprattutto perché, a differenza di quello che avviene in scenari più tradizionali, qui mancano codici e regole che possano istruire il confronto in un assetto regolato. “Lo spazio cibernetico è diventato talmente importante da essere diventato luogo di presidio e di scontro”, ha osservato **Fabio Rugge**, responsabile del centro di ricerca sulla cybersecurity dell’Ispi. La mancanza di codici comunemente accettati sta portando al paradosso per cui, come illustrato da Rugge, “la mia sicurezza è data dall’insicurezza dell’altro, in un contesto di *consistent engagement*”.

Un assetto siffatto, che può anche ricordare la guerra fredda, non può per sua natura essere stabile. E rischia continuamente di sfociare in un conflitto vero e proprio o, senza andare troppo in là, in episodi che possono comunque avere ripercussioni sulle imprese: alla fine, anche violazioni delle libertà civili o segmentazioni della rete non fanno bene al business.

UNA QUESTIONE DI SICUREZZA

Sullo sfondo resta poi il tema della sicurezza, salita ai vertici delle priorità imprenditoriali in Italia negli anni

del terrorismo. E oggi allargatasi a tutto ciò che può recar danno a un’azienda. “Dietro a ogni rischio c’è sempre la mano di qualcuno: le cose accadono perché qualcuno l’ha voluto”, ha osservato **Riccardo Balotta**, amministratore delegato di **Agatòs Agger**. La consapevolezza negli anni è cresciuta, arrivando anche all’attenzione del legislatore che, a seguito di alcuni interventi, ha posto la questione anche in un’ottica di *compliance*. “Le norme sulla *travel security* – ha affermato – sono un esempio calzante: oggi c’è un obbligo di legge che impone al datore di lavoro di garantire la sicurezza del proprio personale in viaggio”.

Per fare sicurezza, tuttavia, non basta una legge. “La sicurezza deve essere una condizione diffusa, non trincerata in un fortino all’interno dell’azienda”, ha spiegato. “È sicurezza – ha chiosato – anche disporre in maniera agevole gli estintori o, ancora, evitare di tenere sul monitor del computer un post-it con le password di accesso”.

CONOSCERE PER AGIRE

Su un punto hanno convenuto tutti i relatori: l’analisi del rischio deve diventare parte integrante dell’operatività aziendale. Il tema è stato al centro della tavola rotonda conclusiva, dove è emerso il punto di vista delle imprese. Per **Anna Gervasoni**, direttore generale dell’**Aifi**, “il tema è culturale”. Il vertice dell’associazione che riunisce società di private equity, private debt e venture capital, ha evidenziato come diventare azionisti comporti una riflessione preliminare sulla solidità dell’impresa. “Siamo portati – ha osservato – a escludere inizialmente tutte le aree e tutti i settori a rischio, poi interveniamo per fare un iniziale perimetro delle minacce e prendere le dovute contromisure”. Contromisure che, nell’era della *compliance*, si traducono in una gestione del rischio rivolta anche all’ambiente circostante. “In questa fase – ha osservato **Margherita Bianchini**, vice direttore generale di **Assonime** – anche il rispetto della normativa va visto come una sorta di rischio: bisogna individuare le singole cautele, dobbiamo rispondere di tutele ulteriori verso l’ambiente e gli stakeholder”.

Elemento centrale resta comunque la conoscenza e il presidio del rischio. **Gianmarco Capannini**, head of cyber di Munich Re, ha parlato a tal proposito del cyber risk. “La penetrazione delle polizze informatiche in ambito corporate resta marginale”, ha affermato. Pensano senz’altro il costo e la complessità della soluzione, nonché la difficoltà di trasferire il rischio che grava su un bene intangibile. Forse, anche l’impossibilità di coprirsi contro un rischio che non viene percepito. “Molte aziende – ha chiosato Capannini con una provocazione – non trasferiscono il rischio perché semplicemente non lo governano”.