Oracle Community For Security

SICUREZZA E SOCIAL NETWORK

# La Sicurezza nei

*Guida all'utilizzo sicuro dei Social Media per le aziende del Made in Italy*

BLOG

# INDICE


Indice ..... 3
Management Summary ..... 5
Introduzione ..... 6
PARTE PRIMA: il fenomeno dei Social Media nella prospettiva della sicurezza ..... 8
Made in Italy: la ciliegia dei Social Media. ..... 8
I Social Media nella realtà della media azienda italiana ..... 11
Alcuni casi reali ed una indagine sulla sicurezza. ..... 11
Il fenomeno della Consumerization e la tendenza BYOD ..... 13
Uso aziendale dei Social Network ..... 14
Premessa ..... 14
Uso attivo e uso passivo del Social Network ..... 14
Classificazione dei Social Media ..... 15
Macro catalogazione ..... 15
Tipologie di utilizzo da parte dei consumatori ..... 16
Tipologie di utilizzo da parte delle aziende: obiettivi di progetto e obiettivi di business ..... 16
L'utilizzo da parte delle aziende: tabelle riepilogative ..... 18
Aspetti economici: il ROI dei Social Network ..... 20
Return on Security Investiment ..... 22
PARTE SECONDA: per un progetto Social sicuro ..... 24
I Social Media in azienda: istruzioni per partire ..... 24
Social Media Policy ..... 25
La Social Media Policy ad uso esterno ..... 26
La policy Social Media ad uso interno. ..... 28
Ruoli sui Social Network ..... 29
Il lato oscuro dei Social Media: le nuove minacce ..... 31
Introduzione ..... 31
Le minacce. ..... 31
I rischi ..... 34
Approfondimento: rischi relazionali dei Social Media ..... 37
Approfondimento: Rischi operativi dei Social Media tramite dispositivi mobili ..... 37
Contromisure ..... 39
Le matrici Rischio / Contromisura ..... 39
Aspetti legali ..... 43

Le norme rilevanti ..... 43
I termini di servizio ..... 47
Forme di tutela e raccomandazioni legali ..... 48
Adempimenti in materia di protezione dei dati personali: la profilazione dei dati personali ..... 51
I contenuti, tra copyright e creative commons ..... 53
Come è stato affrontato il tema dalla giurisprudenza ..... 55
Trascurare la sicurezza: esempi di casi critici ..... 55
Trascurare la sicurezza: aspetti economici danni e criminalità ..... 58
PARTE TERZA: I casi aziendali ..... 61
Il caso Bisazza ..... 61
Il caso Bticino ..... 64
Il caso Lugana ..... 67
Il caso Italcementi ..... 68
Chi è ITALCEMENTI ..... 68
Italcementi e i Social Network ..... 69
Il caso Roadrunnerfoot ..... 71
L'azienda ..... 72
Il prodotto ..... 73
Il mercato ..... 73
Linee guida ..... 74
Considerazioni sul caso ..... 76
Il caso Cesari ..... 76
Umberto Cesari e i Social Network ..... 77
APPENDICI ..... 79
Indice delle figure ..... 79
Note e fonti ..... 79
Autori e contributori ..... 81
Team leader ed editor ..... 83
Autori e contributori ..... 83

# MANAGEMENT SUMMARY

Alzi la mano chi non ha un account Facebook o LinkedIn. Alzi la mano chi pensa che la sua azienda non abbia intenzione di fare una pagina sui Social Media per “parlare” con i clienti. L’IT lo sa o il marketing sta andando avanti da solo? Qualcuno si è preoccupato della Sicurezza e della Privacy?

L’evoluzione e la penetrazione dei Social Media come strumento di supporto al Business sta attirando l’attenzione delle aziende. Se fino a pochi anni fa la tendenza predominante era di considerare le piattaforme di comunicazione e di condivisione come un fenomeno prettamente legato alla sfera privata dell’individuo, oggi il mondo dei Social Media rappresenta, di fatto, un fattore differenziante e quindi un’importante opportunità per gran parte delle organizzazioni. Opportunità che si accompagna tuttavia a rischi di diversa natura e alla inevitabile necessità di gestirli.

Intraprendere la strada del Social, dunque, comporta degli obblighi di compliance e dei rischi dei quali è molto importante essere consapevoli. Alcuni rischi, però, si applicano anche alle aziende che non lo vogliono fare, visto che il mondo intorno ad esse cambia ed agisce nonostante la loro inerzia.

Questo documento fornisce delle utili indicazioni per le aziende che vogliono prenderne coscienza e qualche raccomandazione su come comportarsi.

Nella prima parte sono trattati gli aspetti generali dei Social Media, a partire dal fenomeno dirompente che ne ha sancito l’affermazione globale in questi ultimi anni, insieme ad una analisi del contesto e delle nuove tendenze di fruizione dei sistemi informativi.

Su questa base sono state poi classificate e correlate sia le modalità di utilizzo dei Social Media in ambito aziendale che le tipologie di offerta presenti sul mercato.

La seconda parte del documento affronta il tema secondo il punto di vista della sicurezza: sono descritti gli elementi che dovrebbero essere affrontati nella redazione delle Social Media policy e quindi sono trattati in dettaglio i ruoli deputati alla gestione della tecnologia, le minacce, i rischi, le contromisure e gli aspetti legali; la sezione si chiude con la disamina di alcuni incidenti di sicurezza che hanno generato danno reputazionale occorsi ai Social Media ed ai loro utilizzatori.

Nella terza parte il documento si conclude con la descrizione di alcuni case study relativi all’adozione dei Social Media da parte di organizzazioni italiane con l’obiettivo di sfruttarne le potenzialità per migliorare il rapporto con la clientela, i processi interni e sviluppare il business aziendale.

Nota sul logo:

La ciliegia? Il Social Media è per le aziende come una ciliegia. Rossa e matura. Pronta per essere addentata. Ma tutti sanno che le ciliegie hanno il nocciolo e tutti sanno che bisogna morderle con una certa attenzione. Il nocciolo contiene i rischi ed i vincoli di cui questo documento si occupa.

# INTRODUZIONE

L'ambiente in cui si trovano ad operare le aziende odierne è fortemente caratterizzato dalla pervasività e sempre più dall'ubiquità di internet che ormai ci accompagna ovunque grazie alle tecnologie "mobile". Se a questo si aggiunge l'intuizione Aristotelica "l'uomo è per natura un animale sociale" si può iniziare a comprendere come sia nato il fenomeno dei Social Network, comunità virtuali abilitate da tecnologie dell'informazione.

La crescita che ha portato, in pochi anni, alla partecipazione di un miliardo di persone a tali comunità è giustificata dal potere che queste hanno di aumentare le possibilità e l'efficacia relazionale, cognitiva e organizzativa degli individui che le popolano attraverso la fruizione di servizi offerti da una nuova categoria di imprese che operano in genere esclusivamente sul web 2.0.

Questo documento sulla Sicurezza nel Social Network intende contribuire pragmaticamente alla conoscenza delle cose da fare per avvicinarsi a queste nuove realtà.

essi rappresentano una reale opportunità, ma, al contempo, suggeriamo di farlo senza sottovalutarne la complessità e tenendo conto di tutti gli aspetti rilevanti e, tra questi, della sicurezza dell'informazione e della protezione degli asset aziendali materiali ed immateriali.

Non sono aspetti trascurabili: non per niente, si sta affermando una nuova branca dell'Information Security, necessariamente multdisciplinare, che si occupa della prevenzione dei rischi e della gestione degli incidenti che possono colpire le imprese a causa dei Social Network.

Questa nuova disciplina è chiamata, dagli addetti ai lavori, Social Business Security, ed include elementi di ICT Security, di reputation management, di brand protection, di compliance normativa, di tutela legale, di open source intelligence (OSInt), di digital marketing e di altre discipline specifiche nate in ambito Social (per esempio, conversation management). Per brevità, nel proseguo del testo, si farà riferimento a questo ambito di attività utilizzando indifferentemente i termini "Sicurezza Informatica" e "Security".

Nelle pagine seguenti, come anticipato nel management summary, gli autori forniscono una serie di elementi fondamentali per fare dei Social Media un successo per la propria azienda in sicurezza.

In questo caso, ancora più che in altri, abbiamo la consapevolezza che sia necessario operare anche a livello culturale in modo da elevare il livello della sicurezza di cui si dotano le aziende.

L'utilizzo dei Social Media da parte delle imprese è, infatti, un fenomeno molto recente e tuttora poco esplorato sia per quanto riguarda le sue potenzialità di business, sia, a maggior ragione, per le sue relazioni con i sistemi informativi aziendali e per le implicazioni relative alla sicurezza.

In un contesto come l'attuale, caratterizzato da una grande attenzione al contenimento di tutti i costi non direttamente finalizzati ad obiettivi di business, spesso, la forbice tra la sicurezza che serve e quella di cui ci si dota, non tende verso la chiusura, ma si allarga. Il risultato è che, proprio mentre innovazioni come i Social Media aprono la strada a nuove minacce e nuovi rischi, le aziende sono portate a ridurre le risorse disponibili per tutti gli interventi che non appaiono strettamente necessari per cogliere l'obiettivo di business.

Il gruppo di lavoro, invece, raccomanda di effettuare un'attenta valutazione delle minacce, di svolgere l'analisi del rischio, di valutare gli impatti sul business e di sfruttare al meglio le risorse disponibili, nella convinzione che l'attenzione a questi aspetti possa contribuire al successo dei progetti e perfino, ad abilitare dei nuovi modelli di business, a creare dei nuovi prodotti o un nuovo modo di comunicare ed interagire con i propri clienti e partner.

Abbiamo scritto questo documento avendo in mente un lettore che è responsabile della sicurezza delle informazioni in azienda, ma che probabilmente dispone di un tempo limitato e di risorse scarse; che opera trovandosi di fronte i colleghi del "business" che

vogliono “Facebook” senza troppo preoccuparsi del modo in cui questi progetti vanno fatti e dei pericoli che comportano.

Vorremo rivolgerci all’ecosistema della media impresa Italiana, ossia quell’insieme di aziende, pur molto diverse tra loro, che così bene rappresenta l’Italia nel mondo con i propri prodotti e servizi. Per queste aziende, internet ed oggi i Social Media costituiscono una grande opportunità per raggiungere nuovi mercati, stabilire partnership produttive e commerciali e sviluppare nuovi servizi. Social Media e Made in Italy, dunque è l’altra focalizzazione di questo documento. Anzi, in ordine di importanza, Social Media sicuro e Made in Italy.

Nel definire l’ambito del lavoro abbiamo anche molto discusso se includere o meno la Pubblica Amministrazione locale e centrale. Anche se molte delle cose si applicano indifferentemente sia al pubblico sia al privato, alla fine abbiamo preferito, come sempre finora, focalizzarci su una cosa sola per portare un valore più grande.

Il taglio è quindi quello della Security nei Social Network, dal punto di vista di una media azienda privata che lo deve utilizzare verso l’esterno o nei confronti della propria organizzazione estesa, per fare il proprio “business”.

Per certi aspetti parliamo anche di Privacy, ma in questo nostro lavoro essa rimane sullo sfondo. Rispetto alla Pubblica Amministrazione è nostra intenzione fare un approfondimento in seguito. Lo decideremo anche ascoltando i vostri suggerimenti.

Mettiamo a disposizione queste considerazioni tramite una licenza molto aperta (Creative Common – Attribuzione – Condividi allo stesso modo)* nel pieno spirito di collaborazione che da anni ci lega nella Oracle Community for Security e sotto l’ombrello della quale abbiamo prodotto nel tempo numerosi altri contributi per la discussione pubblica come le pubblicazioni “Privacy nel Cloud: Le sfide della tecnologia e la tutela dei dati personali per un'azienda italiana”, “Mobile e Privacy: Adempimenti formali e misure di sicurezza per la compliance dei trattamenti di dati personali in ambito aziendale”, “ROSI Return on Security Investments: un approccio pratico” (un metodo per il calcolo del Ritorno dell’Investimento in Progetti di Sicurezza), “Fascicolo Sanitario Elettronico: il ruolo della tecnologia nella tutela della privacy e della sicurezza”, e infine, prodotto contemporaneamente a questo, una pubblicazione sui “Primi 100 giorni del Responsabile della Sicurezza delle Informazioni”. Per tutti si rimanda al sito web della Community e a quello di Clusit (la nostra associazione di riferimento) o alle pagine dedicate a questo indirizzo http://c4s.clusit.it.

* La licenza permette a chiunque di usare il nostro prodotto anche per crearne una sua evoluzione a condizione che citi gli autori originali e utilizzi a sua volta lo stesso tipo di licenza. Autorizziamo la pubblicazione parziale di testo e immagini non già protette da altri copyright riportando la nostra url http://c4s.clusit.it.

# PARTE PRIMA: IL FENOMENO DEI SOCIAL MEDIA NELLA PROSPETTIVA DELLA SICUREZZA

L'obiettivo di questa prima parte è quello di descrivere il fenomeno dei Social Media, in particolare per quanto attiene all'utilizzo dei Social Media da parte delle imprese.

Descrivere questo fenomeno non è l'obiettivo primario del documento. Abbiamo cercato di farlo nella prospettiva della sicurezza, evidenziando aspetti, concetti, situazioni che saranno utili, nella seconda parte, per affrontare i temi che costituiscono l'obiettivo centrale del documento.

Non solo, abbiamo cercato di ancorare questa ricognizione al contesto tutto italiano della media impresa che, come dichiarato nell'introduzione, costituisce il target a cui il documento è rivolto.

## Made in Italy: la ciliegia dei Social Media.

Nell'affrontare le rilevanti implicazioni di sicurezza connesse all'utilizzo dei Social Media come strumento di promozione per le aziende del Made in Italy, la prima domanda che è necessario porsi è: i Social Media sono una opportunità per il business o se ne può fare tranquillamente a meno?

E' chiaro, infatti, che se stessimo parlando di un fenomeno effimero e superficiale, anche gli aspetti di sicurezza diventerebbero un tema marginale.

Bastano poche tabelle a fugare ogni dubbio, sia per quanto riguarda il mercato americano che spesso segna la tendenza, sia per quanto già oggi emerge dalle analisi disponibili relative al mercato italiano.

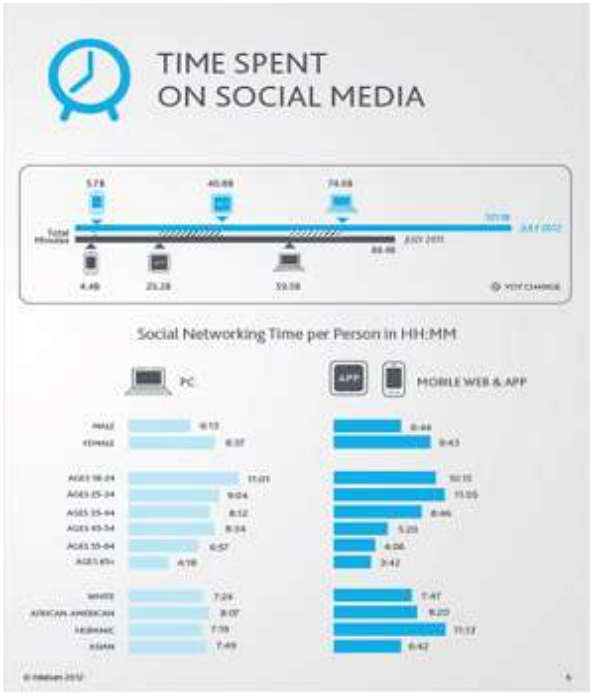



**FIGURA 1 - UTILIZZO DEI SOCIAL MEDIA**

La seconda domanda riguarda la specificità italiana, rispetto al fenomeno Social Media: alle aziende del Made in Italy deve interessare il fenomeno Social?

La risposta a questa domanda ha due facce: deve interessare perché gli italiani sono essi stessi dei grandi consumatori di Social Media e, soprattutto, perché i Social Media con il loro pubblico *miliardario*, sono una finestra sul mercato globale, attivabile senza complesse organizzazioni internazionali e grandi investimenti. Dunque, per un mondo di piccole e medie imprese, spesso sotto capitalizzate e con uno spessore organizzativo inadeguato alla internazionalizzazione, i Social Media se non sono la risposta, certo sono una opportunità

Che poi in rete si faccia business, è qualcosa che ormai nessuno pensa più di mettere in discussione. Anche qui, trovare numeri a supporto non è certo difficile, basta verificare l'andamento dell'e-commerce osservato in un anno in cui i dati sul commercio in generale hanno risentito pesantemente della contrazione dei consumi generata dalla crisi. In

internet si vendono prodotti e servizi in quantità crescente, con percentuali di crescita da anni del boom.

Se dunque internet è ormai una piazza dove si vende e si compra di tutto, popolata da un numero crescente di utenti appartenenti soprattutto alla fascia d'età più predisposta alla spesa e se sempre più il tempo speso in rete passa attraverso i Social Media, allora hanno senso due cose: analizzare meglio il fenomeno e preoccuparsi della sicurezza.

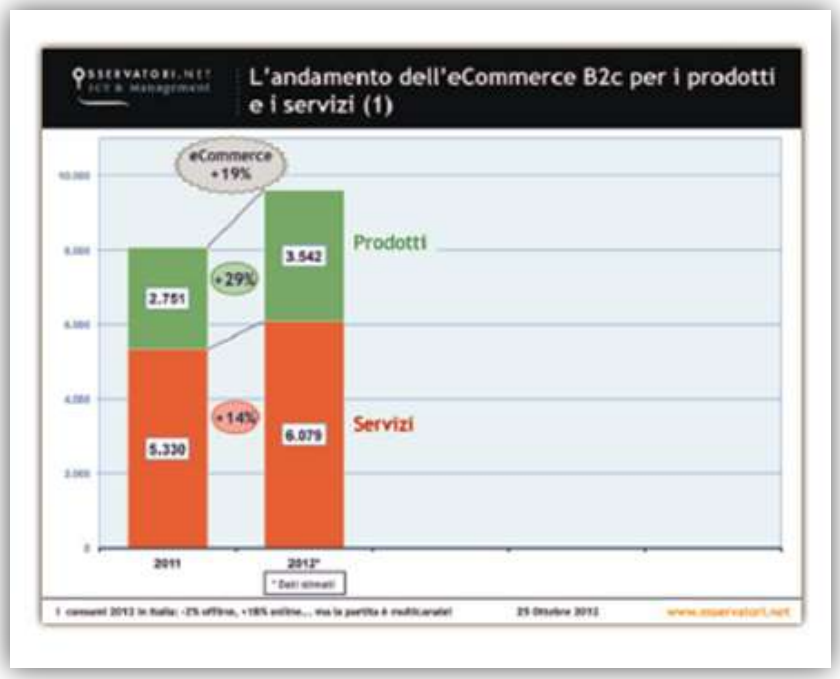



**FIGURA 2 – ANDAMENTO DELL'E-COMMERCE B2C**

Quest'ultima è il cuore di questo documento e viene sviluppata in profondità nei suoi molteplici aspetti, nei capitoli successivi, al contrario della prima che, però, non è l'obiettivo di questa pubblicazione. Ci limitiamo quindi, in questo primo capitolo, a qualche cenno, a qualche piccola provocazione di stimolo per la curiosità del lettore, con l'obiettivo di qualificare, a grandi linee, il fenomeno.

Cerchiamo, allora, di dare qualche indicazione su cosa siano i Social Media in Italia e cosa possano essere per le aziende italiane, prendendo spunti da diverse ricerche.

I sentieri italiani che vanno e vengono dai Social Media sono diventati strade o addirittura autostrade?

"L'Italia ai vertici per penetrazione dei Social Media. Batte gli Stati Uniti per utilizzo da PC 86% a 79%".

Certo non basta per affermare che esista una "via italiana ai Social Media". Forse dice solo di diverse abitudini di consumo e di diverse organizzazioni del lavoro e della vita sociale: più "PC-casa, PC-ufficio" per gli impiegati italiani, più smartphone e tablet negli Usa.

| # | Country | Number of Users | Change | (± %) | Penetration |
|---|---|---|---|---|---|
| 1 | United States | 167 554 700 | +10 320 940 | +6.56% | 54.01% |
| 2 | Brazil | 60 665 740 | +14 326 020 | +30.92% | 30.17% |
| 3 | India | 60 620 620 | +14 846 360 | +32.43% | 5.17% |
| 4 | Indonesia | 50 489 360 | +8 242 360 | +19.51% | 20.78% |
| 5 | Mexico | 39 388 040 | +8 348 080 | +19.21% | 35.02% |
| 6 | United Kingdom | 33 227 180 | +2 443 580 | +7.94% | 53.29% |
| 7 | Turkey | 31 415 080 | +665 620 | +2.16% | 40.38% |
| 8 | Philippines | 29 862 300 | +2 696 040 | +9.93% | 29.89% |
| 9 | France | 25 295 760 | +1 022 660 | +4.21% | 39.06% |
| 10 | Germany | 24 978 600 | +1 456 100 | +6.19% | 30.36% |
| 11 | Italy | 22 829 800 | +1 209 080 | +5.59% | 39.30% |
| 12 | Argentina | 20 411 360 | +2 130 780 | +11.66% | 49.37% |
| 13 | Canada | 18 573 940 | +689 240 | +3.85% | 55.02% |
| 14 | Thailand | 17 469 060 | +3 455 760 | +24.66% | 26.31% |
| 15 | Colombia | 17 455 500 | +1 106 840 | +6.77% | 39.49% |

Fonte: http://www.socialbakers.com/

**FIGURA 3 – UTENTI DEI SOCIAL MEDIA PER PAESE**

Certo, se guardiamo ai Social Media con uno sguardo globale, è interessante notare che, tolti gli Usa, i Paesi con maggiore penetrazione di Facebook siano Paesi emergenti: di nuovo il Brasile e poi India, Messico, Turchia, Indonesia. Chissà cosa può suggerire un dato del genere agli esperti di marketing del Made in Italy.

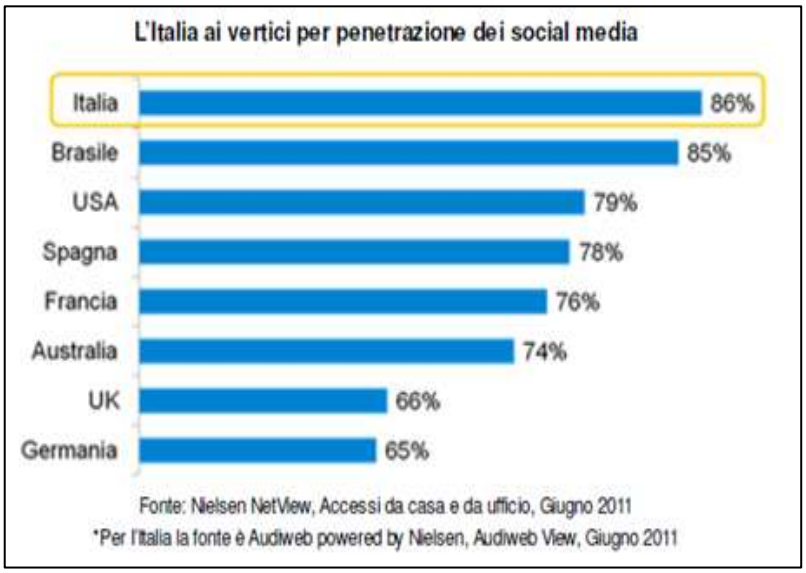



**FIGURA 4 – PENETRAZIONE DEI SOCIAL MEDIA PER PAESE**

Possiamo ovviamente immaginare che le marche italiane che vendono il valore dell'italianità siano impegnate a veicolare per queste strade i loro contenuti.

Il quadro è complesso, mancano ancora modelli interpretativi affidabili e riconosciuti da tutti: generalizzare e fare di tutte le erbe un fascio, può condurre ad errori fatali.

Viene smentito un diffuso pregiudizio: i Social Media non sono esclusiva dei giovanissimi: 35-44 anni è la fascia d'età protagonista con il 24,2%. (*Nielsen 2011*) [8]

Tra i Social Media, come prevedibile, anche in Italia spopola Facebook (FB). Il tempo è prezioso: un minuto su tre on line viene speso su FB. Sono soprattutto donne, mentre l'universo maschile preferisce LinkedIn. FB è essenziale anche per l'e-commerce.

Il 90% circa dei *merchant* online censiti dalla ricerca ha inoltre sviluppato una presenza sui Social Network. L'80% è attivo su almeno due Social diversi, il 60% addirittura su 3. Facebook è lo strumento più adottato (84% dei merchant), seguito da Twitter (70%), YouTube (58%), Google+ (34%) e Pinterest (27%).

Tuttavia, gli utilizzatori non sembrano ancora riporre fiducia nei Social Network dal punto di vista puramente commerciale/transazionale: potenzialità in termini di numero di utenti, engagement, possibilità di supporto pre/post vendita non si sono ancora concretizzate nella capacità di supportare con successo l'acquisto. (Osservatorio eCommerce B2C Netcomm – School of Management del Politecnico di Milano).

Ma su quest'ultimo aspetto qualcosa si muove, in Italia. Tra i dieci vincitori di Ripartiamo dalle idee, il concorso promosso da Corriere della Sera, Intesa San Paolo, Sda Bocconi e Armando Testa troviamo HighstrIT, rete di boutique sul web caratterizzata dall'idea dell'e-shopping ibrido: si compra online, si prova

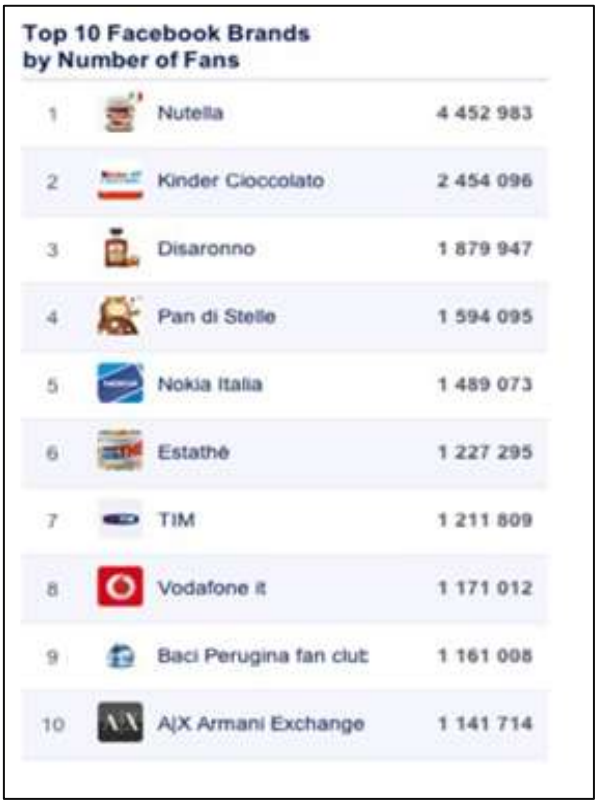



**FIGURA 5 – FAN FACEBOOK DEI MARCHI ITALIANI**

nei negozi. Nel segmento fashion appare poi affascinante l'approccio della toscana Styletrigger.com, capace di e-commercializzare oggi un'antica coniugazione, quella tra letteratura e, appunto, moda.

Dunque non è un caso se il settore moda Made in Italy è più avanzato degli altri comparti industriali italiani impegnati nel Social Media Marketing.

Non c'è gara neppure nel numero dei commenti degli utenti. Peccato che solo il 7% di questi commenti riceva una risposta, per il restante 93% il dialogo è interrotto dal silenzio dell'azienda (*IULM 2012*).

Una contro-lezione di stile, contro-producente in termini, se non altro, di immagine. Inaspettata dai Paladini dell'Italian Style.

Senza voler tirare sintesi approssimative, si può, dunque, dire che la ciliegia dei Social Media si presenta - e inizia ad essere percepita - come assai succosa per il Made in Italy: una buona ragione per addentarla. Con attenzione però: il nocciolo duro della sicurezza si nasconde nella polpa e può provocare seri danni a chi non se ne prendesse adeguatamente cura.

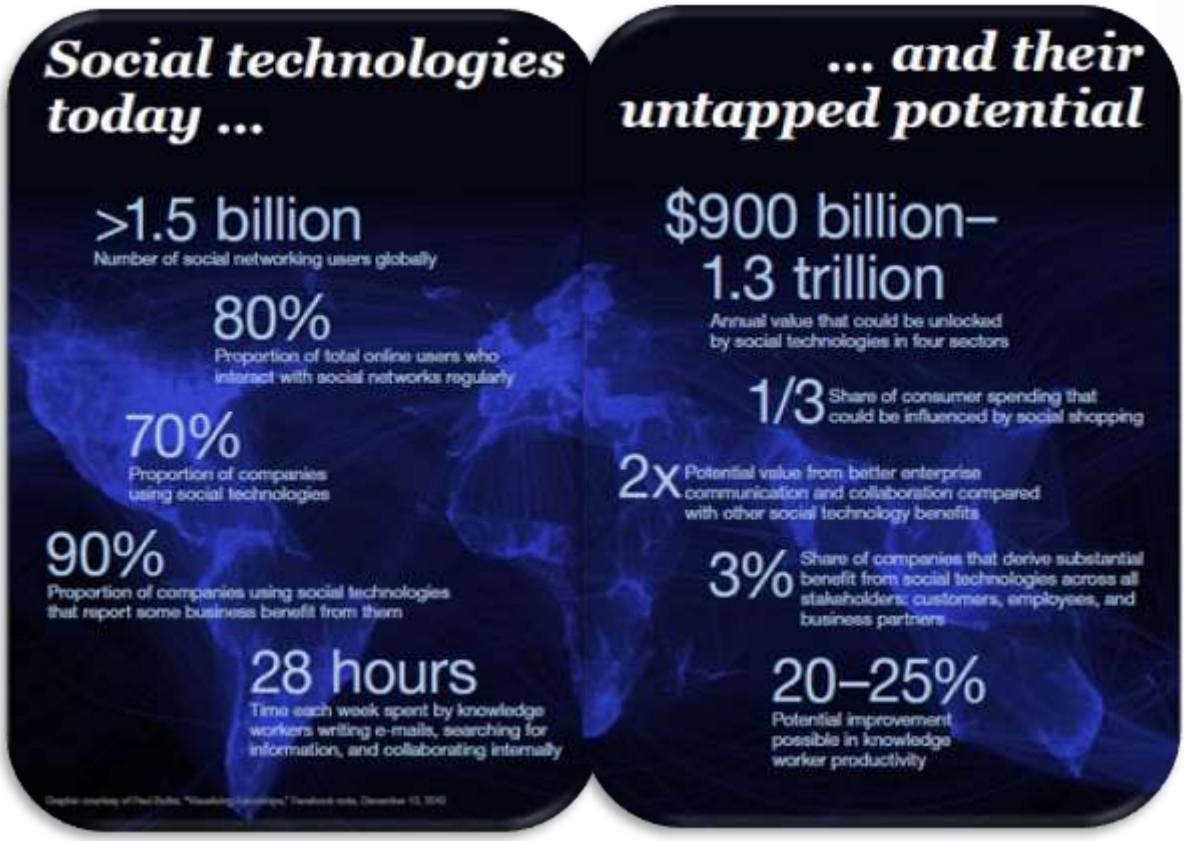



**FIGURA 6 - I SOCIAL MEDIA OGGI E IN PROSPETTIVA (MCKINSEY 2012)**

## I Social Media nella realtà della media azienda italiana

### Alcuni casi reali ed una indagine sulla sicurezza.

Per dare concretezza a questa descrizione introduttiva, inevitabilmente sommaria, dei Social Media in relazione all'utilizzo aziendale degli stessi, nell'ambito dei lavori che hanno condotto alla redazione di questo documento, sono state intervistate alcune

aziende italiane anche molto diverse fra loro per dimensione, storia e settore merceologico.

Innanzitutto è doveroso ringraziare della disponibilità e della qualità del contributo le aziende BTicino, Bisazza, Cesari, Consorzio Lugana, Italcementi e Roadrunnerfoot.

Le interviste hanno riguardato le esperienze che ciascuna azienda ha sviluppato nel corso degli ultimi anni nell'utilizzo dei Social Media.

Le risposte forniscono uno spaccato molto interessante della reazione del Made in Italy alle opportunità offerte dalle nuove forme di comunicazione e di relazione rese disponibili dai Social Media. Costituiscono di per sé un nucleo informativo di rilievo che conferma molte delle considerazioni riportate nei capitoli introduttivi:

- i progetti dedicati all'utilizzo dei Social Media sono guidati e gestiti da funzioni di business; il coinvolgimento dei sistemi informativi rimane sullo sfondo
- l'evoluzione dei progetti contribuisce a rivedere ed aggiustare le funzionalità, i contenuti e le modalità operative
- la sicurezza non è percepita come un aspetto critico del progetto, anche se è oggetto di qualche attenzione

Le interviste sono riportate per intero in appositi riquadri distribuiti nel testo per favorirne la consultazione.

In parallelo alle interviste, nell'ottica di comprendere meglio come le aziende percepivano il problema Security in ambito Social, abbiamo elaborato una serie di 14 domande, ed abbiamo fatto un primissimo e limitato uso del questionario su un campione leggermente più ampio, per capire l'usabilità.

Le domande sono state messe in coda al "Social Media Effectiveness Use Assessment" condotto dal Politecnico di Milano cercando così di correlare l'indagine conoscitiva sull'utilizzo nelle aziende dei Social Media, con la sensibilizzazione e misurazione degli aspetti security.

In questo momento le risposte raccolte sono relative a un numero limitato di casi ed

**TABELLA 1 - SOCIAL MEDIA E SECURITY: LA PERCEZIONE DELLE IMPRESE**

| Questionario sulla gestione e percezione della security in ambito Social Media. | | | |
|---|---|---|---|
| Nr. | Domanda | SI | % SI |
| 1. | Avete una policy per i dipendenti relativa ai Social Media? | 4 | 44.4% |
| 2. | Avete dei documenti guida per i dipendenti su come comportarsi sui Social Media? | 3 | 33.3% |
| 3. | Avete un sistema di rilevazione degli accessi ai sistemi social? | 4 | 44.4% |
| 4. | Avete una policy BYOD (Bring Your Own Device)? | 2 | 22.2% |
| 5. | E' consentito l'utilizzo di device personali in azienda, per accededere alla rete/applicazioni/web? | 7 | 77.8% |
| 6. | Le persone possono liberamente accedere ai Social Network? | 7 | 77.8% |
| 7. | Alcuni Social Network sono bloccati all'accesso dei dipendenti? | 2 | 22.2% |
| 8. | Esiste un comitato per la sicurezza (che segue le tematice IT)? | 4 | 44.4% |
| 9. | Avete un sistema di Securtiy Assesment dedicato alla navigazione Online? | 6 | 66.7% |
| 10. | Avete un sistema di Securtiy Assesment dedicato ai Social Media? | 0 | 0.0% |
| 11. | Ci sono meeting periodici di allineamento tra marketing, ICT ed HR sulle iniziative Social Media? | 3 | 33.3% |
| 12. | Ci sono integrazioni con i sistemi di Contact Center, Call Center con i Social Media? | 0 | 0.0% |
| 13. | I fornitori di soluzioni marketing Social Media e Web, nel caso di forniture SaaS, sono sottoposti ad un Security Audit? | 1 | 11.1% |
| 14. | Effettuate periodici test di Vulnerability Assessment? | 6 | 66.7% |

hanno perciò solamente un valore di riferimento; quindi è stato deciso di non pubblicare i nomi delle aziende.

Qui di seguito alcune osservazioni, da considerare come indicatori qualitativi e di spunto alla riflessione.

E', innanzitutto, interessante notare che nessuna delle aziende ha un 'Sistema di Security Assessment dedicato ai Social Media', e questo è indicativo della scarsa sensibilità al tema.

Nessuna azienda, poi, ha in essere integrazioni con sistemi core business di Contat/Call Center con i Social Media. Questo denota uno stato ancora non maturo dell'utilizzo nei sistemi di direct marketing tradizionale, e allo stesso tempo indica una sorta di barriera di sicurezza tra sistemi consolidati ICT e strumenti innovativi Social.

Infine, è significativo che quasi la totalità delle aziende non effettua un'analisi delle soluzioni fornite in Saas. Il Software as a Service non è certo una caratteristica dei soli Social Media, ma sicuramente tutti i Social Media sono erogati in modalità SaaS.

## Il fenomeno della Consumerization e la tendenza BYOD

Un altro fenomeno che ha rivoluzionato le logiche di business delle aziende moderne è la consumerization, cioè la tendenza che hanno le nuove tecnologie informative, come i Social Network ma anche gli smartphone, di essere adottate prima dai consumatori (che diventano quindi i driver dell'innovazione di settore) e poi dal mondo del business.

E' una tendenza nuova: tradizionalmente l'industria IT era guidata dalle aziende che fin dal primo apparire dell'informatica, hanno trovato in tali tecnologie uno strumento per esercitare il controllo sulle proprie attività a sostegno del proprio business.

Fino alla affermazione di Internet e della telefonia mobile, per lavorare i dipendenti andavano in azienda; essa era l'unico luogo deputato allo svolgimento delle attività lavorative. Il pc era un terminale collegato ad un server centrale, che abilitava ed autorizzava solo le operazioni inerenti il business. Oggi non è più così. Molte attività lavorative vengono svolte in luoghi esterni al perimetro aziendale ed in tempi differenti rispetto al tradizionale orario di lavoro. Inoltre il progresso tecnologico ha dato la possibilità ai dipendenti di portare dei dispositivi di loro proprietà in grado di accedere ad internet sia attraverso le reti aziendali sia direttamente tramite i servizi di telefonia mobile.

Spesso l'acquisto di tali strumenti, come gli smartphone e i tablet, avviene per una scelta personale del consumatore-lavoratore, ben prima che per una decisione aziendale di innovazione tecnologica. In tali casi, diventa inevitabile la tendenza, da parte del dipendente, a privilegiare, nell'uso quotidiano, lo strumento più innovativo. D'altra parte una decisione di investimento nei nuovi strumenti comporta per le aziende investimenti non marginali.

Nasce così il dilemma amministrativo del BYOD (Bring Your Own Device). Sistemi e infrastrutture aziendali si sovrappongono così a tecnologie e dispositivi personali in una commistione di usi privati ed aziendali che riguarda l'accesso ai dati, alle reti, alle applicazioni: bisogna permettere l'uso di device personali per motivi di lavoro e dentro e fuori le reti aziendali?

La cosa riguarda, naturalmente, la sicurezza e, in generale, la capacità dell'azienda di controllare l'accesso e l'utilizzo del proprio patrimonio informativo.

I Social Media, insieme alla crescente adozione dei dispositivi mobili, sono uno degli aspetti di questo fenomeno: l'uso personale di Facebook o di LinkedIn si sovrappone all'uso aziendale degli stessi strumenti modificando radicalmente e moltiplicando i ruoli e le potenzialità dei soggetti coinvolti.

Si deve stare attenti a giudicare negativamente questo fenomeno che, oltre ad essere difficilmente contrastabile, presenta anche risvolti positivi interessanti, come il potenziamento cognitivo ed organizzativo del personale, che, ad esempio, se si riconosce nell'azienda, ne parlerà bene sui Social Network, creando valore e rappresentando uno stimolo al miglioramento aziendale in generale.

Diventa però essenziale inserire nella complessa equazione del "Social Media sicuro" anche l'utilizzo ibrido privato-aziendale di dispositivi mobili: il cosiddetto BYOD.

# Uso aziendale dei Social Network

## Premessa

I Social Network si configurano come piattaforme online di incontro, discussione, condivisione, lavoro ed espressione della propria identità, e come tali sono arricchiti di una serie di funzionalità che trovano limite solo nella fantasia e creatività degli sviluppatori e amministratori dei vari sistemi. Queste diverse funzionalità e l'uso che ne vogliono fare gli utilizzatori, creano delle piattaforme con loro specifici utilizzi.

I Social Media evolvono velocemente allargando il perimetro funzionale ed ampliando la base di potenziali utenti sia per esigenze commerciali dell'ideatore del Social Media che è portato ad estendere le funzionalità del servizio offerto sovrapponendosi a quelle di altri servizi nati con obiettivi diversi, sia per la creatività degli utilizzatori che talvolta piegano funzionalità nate per uno scopo specifico ad utilizzi del tutto diversi e imprevedibili contribuendo ad estendere le potenzialità dello strumento.

In ogni caso, però, la vocazione originaria di ciascun Social Media tende a caratterizzare il servizio offerto anche quando la gamma delle funzionalità si estende ben al di là dei confini iniziali. Per un'azienda che deve scegliere su quale piattaforma realizzare i propri progetti è importante considerarla con attenzione, infatti normalmente essa mantiene una certa rilevanza e determina parte degli sviluppi futuri.

Per questa ragione, nel seguito, per tracciare una classificazione dei Social Media, facciamo riferimento a questa vocazione originaria e non al profilo funzionale o agli ambiti di effettivo utilizzo affermatisi nel tempo; compito che altrimenti sarebbe anche arduo e produrrebbe un risultato soggetto a rapida obsolescenza.

## Uso attivo e uso passivo del Social Network

I Social Media interferiscono e, sempre più, interferiranno con le strategie di comunicazione e di relazione delle imprese, a prescindere dalla scelta di queste ultime di avviare progetti specifici di presenza e sfruttamento delle loro potenzialità.

Esiste, infatti, un uso passivo dei Social Network che fa riferimento al comportamento di aziende che non sono sui Social Network. Non essere attivamente presenti in questo ambito non comporta l'esserne assenti e dunque non elimina alcuni dei rischi connessi.

Soprattutto le aziende titolari di marchi conosciuti dal grande pubblico, possono essere oggetto di considerazioni, discussioni, suggerimenti ma anche critiche da parte di comunità indipendenti che si possono formare intorno ad un marchio ma anche ad una personalità aziendale particolarmente esposta mediaticamente.

Altri rischi che si presentano anche a fronte di un atteggiamento passivo da parte dell'azienda derivano dalla tendenza alla consumerizzazione e all'utilizzo ibrido privato-aziendale delle nuove tecnologie.

La partecipazione di dipendenti aziendali a comunità verticali che si formano intorno ad interessi particolari può generare nuove opportunità per attacchi alla integrità dei dispositivi e, attraverso questi, dell'infrastruttura informatica aziendale. Si tratta spesso di comunità virtuali che nascono senza un'organizzazione robusta alle spalle e dunque privi di qualsiasi forma di protezione e di sicurezza. In taluni casi, come, ad esempio le comunità virtuali che ruotano intorno a tematiche border line ma di ampia diffusione come la pornografia, è il contesto stesso che genera una propensione alla insicurezza, sia per la natura dei fornitori di contenuti sia per le modalità di fruizione.

Quando il tema oggetto della comunità è affine ai servizi o ai prodotti offerti dall'azienda - molte di queste realtà virtuali sono dedicate a temi come la salute, il cibo, l'ambiente - i rischi di un coinvolgimento passivo sia sul fronte della comunicazione sia su quello del coinvolgimento dei dipendenti ovviamente aumentano.

Non presidiare questo fronte della comunicazione può esporre a rischi anche gravi per l'immagine e questo suggerisce attenzione anche in caso di una scelta aziendale di passività nei confronti del Social Media. I Social Media sono dunque, volenti o nolenti, uno snodo obbligato nelle relazioni con il pubblico, con i consumatori e con i dipendenti e

la necessità di allocare risorse al fine di monitorarli costantemente prescinde, pertanto, dalla decisione di avviare progetti volti a garantire una presenza attiva nel settore.

Per quanto riguarda l'uso attivo dei Social, introduciamo brevemente il lato consumer e poi discutiamo degli usi e delle finalità dei Social Network nel mondo business. In seguito parleremo delle finalità.

### Classificazione dei Social Media

Come si è detto, le sempre maggiori possibilità di accesso alla rete e la proliferazione di dispositivi mobili sono gli elementi abilitanti della crescita continua dei Social Media, in termini di diffusione e tipologia di utilizzo .

Tale proliferazione rende possibile, nonché necessario al fine di facilitarne l'utilizzo da parte delle aziende, la definizione di una tassonomia dei Social Media relativa alle funzionalità offerte. Come accennato precedentemente si è ritenuto di procedere innanzitutto ad una macro-catalogazione che copra in modo esaustivo l'offerta e che ne fornisca una chiave di lettura utile a guidare eventuali scelte di investimento.

### Macro catalogazione

Questa scelta ci obbliga a rinunciare ad una catalogazione analitica, peraltro assai problematica per la costante e velocissima evoluzione dell'offerta (vedi http://en.wikipedia.org/wiki/Social_networking_websites), che viene però indirizzata, in modo indicativo, all'interno di ciascuna delle macro-categorie individuate.

#### *1. Relazione*

Strumenti che permettono all'utente di relazionarsi con altri e per comunicare, raccogliere e divulgare informazioni ai componenti della propria community. Spesso utilizzata dalle aziende per la sola comunicazione. Tale tipologia di Scial Media include:

- portali di blogging e microblogging (Twitter, Tumblr);
- reti sociali (Facebook, Google+);
- reti professionali (LinkedIn);
- portali per l'organizzazione di eventi (Meetup, Evite).

#### *2. Condivisione di interessi*

Strumenti che permettono all'utente di condividere informazioni e dati multimediali (musica, foto, video, etc.) in modo da garantire un'ampia divulgazione delle informazioni condivise. Le informazioni che tale tipologia di Social Media permette di condividere includono:

- foto (Flickr, Instagram, Pinterest);
- video (YouTube);
- musica (Last.fm, Pandora);
- presentazioni (Slideshare);
- geolocalizzazione (Foursquare);
- navigazione (Waze).

#### *3. Collaborazione*

Strumenti che permettono all'utente di collaborare con i membri della community e di coordinarsi. Tale tipologia di Social Media include:

- piattaforme per la condivisione di informazioni (Wikis, Forum);
- strumenti per la gestione documentale (Google Drive);

- media per la gestione di informazioni provenienti da una varietà di fonti differenti (Delicious, Feed aggregator);
- online gaming (World of Warcraft);
- Multi-User Virtual Environment, simulazione di un ambiente interattivo tra più utenti (es. Second Life).

Nel seguito di questo documento faremo riferimento alla catalogazione sopra esposta per cercare di dare dei criteri interpretativi e di utilizzo dello strumento Social Media.

Naturalmente sono possibili, assolutamente lecite oltre che utili altre tipologie di classificazione.

### Tipologie di utilizzo da parte dei consumatori

I consumatori usano i Social Network principalmente per interagire, informarsi, condividere, discutere, intrattenersi, coltivare interessi e trovare lavoro ma la moderna economia dei servizi ha fatto sì che, con queste piattaforme, possano anche fruire di prodotti o servizi digitali molto diversi fra loro: acquistare o ascoltare musica, giocare, guardare video, ottenere finanziamenti, videochiamare, mandare messaggi, geolocalizzarsi, etc.

Riportiamo qui i risultati di una ricerca di NM Incite [4] che riporta una lista degli usi più frequenti dei Social da parte di consumatori:

- Tenersi aggiornati e in contatto con famiglia e amici
- Trovare nuovi amici / appuntamenti
- Trovare recensioni di prodotti e fornire feedback / Informarsi su prodotti
- Accedere a forme di intrattenimento
- Trovare offerte convenienti / Ottenere coupon
- Trovare lavoro

### Tipologie di utilizzo da parte delle aziende: obiettivi di progetto e obiettivi di business

La prospettiva da cui le aziende guardano ai Social Media è diversa ma la diversità di obiettivi non impedisce l'utilizzo degli stessi strumenti ed il ricorso ad approcci in gran parte speculari.

Social Media Marketing è un termine che raggruppa un insieme di usi dei Social Network, da parte di aziende, volti a raggiungere il mercato e conquistarlo con una varietà di tecniche di marketing. I Social Network stanno diventando anche palcoscenico dell'e-commerce, nonché un importante hub per il mercato del lavoro.

A questo proposito, occorre ricordare che, così come i Social Network sono estremamente utili per individuare nuovi talenti e per svolgere attività di recruitment, lo sono anche per i concorrenti. In questo senso dal momento che i collaboratori sono asset aziendali preziosi, andranno posti in essere gli opportuni strumenti contrattuali a tutela dell'azienda

**FIGURA 7 - SOCIAL MEDIA E VALORE AGGIUNTO ALLE IMPRESE**

Secondo l'analisi del McKinsey Global Institute [5] gli usi principali dei Social Network da parte delle imprese per creare valore sono:

- Co-creare prodotti
- Stimare, prevedere e monitorare
- Distribuire processi di business
- Ottenere pareri dai consumatori
- Marketing volto a comunicare/interagire
- Generare e potenziare le vendite
- Social Commerce
- Fornire assistenza ai consumatori
- Migliorare la collaborazione e comunicazione dell'organizzazione
- Associare talenti ai lavori

Queste diverse possibilità di sfruttamento delle potenzialità dei Social Media da parte delle imprese, finiscono per costituire gli obiettivi dei singoli progetti che vengono attivati.

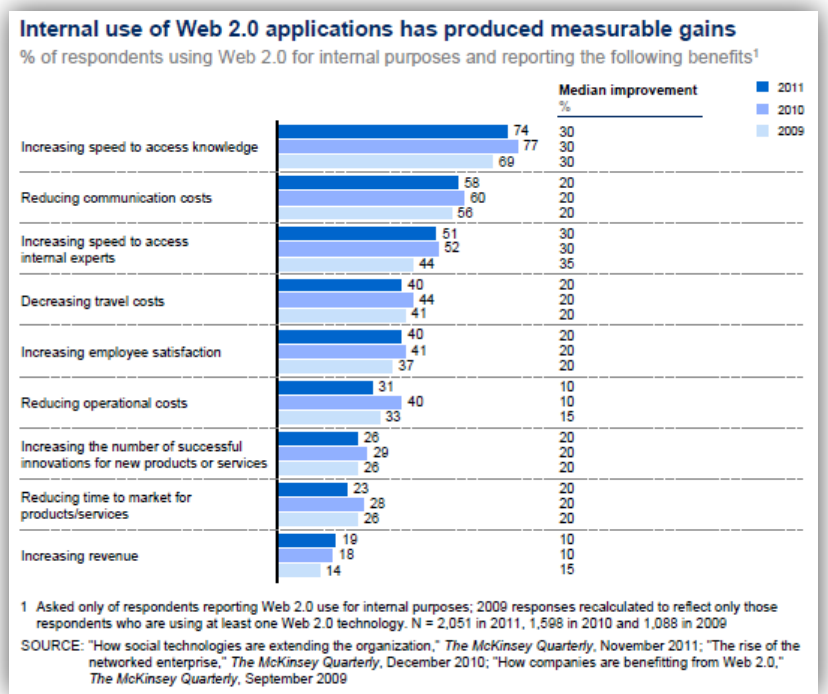



**FIGURA 8 - BENEFICI OTTENUTI DALL'USO DI SOCIAL MEDIA**

E' però altrettanto utile ricondurre questi obiettivi di progetto ad obiettivi di business più generali di grande interesse anche per il top management preposto alla allocazione delle risorse disponibili, al di là delle tecnicalità specifiche di ciascuna realizzazione progettuale.

In questo senso possono essere individuati i seguenti obiettivi di business:

- Aumentare la velocità di accesso al sapere
- Ridurre i costi di comunicazione
- Velocizzare l'accesso ad esperti interni
- Ridurre i costi di trasporto
- Aumentare la soddisfazione dei dipendenti
- Ridurre costi operativi
- Aumentare il numero di innovazioni di successo
- Ridurre il time-to-market
- Aumentare i ricavi

E' utile sottolineare che questi obiettivi di business possono essere suddivisi in due grandi categorie:

- obiettivi di business finalizzati a migliorare le relazioni esterne all'azienda, ad esempio nei confronti della clientela: iniziative di marketing, promozione del branding, supporto delle relazioni pubbliche, miglioramento del processo di lead generation, supporto alle vendite
- obiettivi di business finalizzati al miglioramento dell'organizzazione e dei processi aziendali, ad esempio mediante la migliore condivisione delle informazioni, l'utilizzo di tool di collaboration e di messaging che incrementino la produttività o riducano i costi operativi.

## L'utilizzo da parte delle aziende: tabelle riepilogative

L'insieme delle considerazioni esposte sono sintetizzate in due tabelle riportate nel seguito.

In esse ritroviamo la macro-catalogazione dei Social Media incrociata con le finalità dei progetti attivabili in ambito Social Media da parte delle imprese e gli obiettivi di business che possono essere così perseguiti.

Nelle celle ritroviamo le tipologie di Social Media rilevanti per quella specifica combinazione con il tipo di piattaforma utilizzabile riportata a scopo esemplificativo.

In ogni cella è poi inserito un numero che costituisce un tentativo di misurazione della rispondenza dello strumento con l'obiettivo. In pratica, ad ogni casella viene assegnato un valore da 0 a 10 che indica quanto sia alta l'opportunità di utilizzare la categoria di Social Network individuata per le funzionalità indicate.

Questa misurazione effettuata in relazione alle caratteristiche specifiche del Made in Italy, è frutto della riflessione collettiva del Gruppo di Lavoro ed è tratta dall'esperienza professionale acquisita sul campo insieme all'approccio metodologico e di mercato delle aziende di appartenenza dei componenti del Gruppo.

Si tratta, dunque, di una misura empirica in assenza di altri metodi di misurazione consolidati e accettati e di serie storiche di dati omogenei e confrontabili. Inoltre è soggetta al rischio di una rapida obsolescenza a causa della velocità di evoluzione dei Social Media.

Abbiamo ritenuto di inserirla comunque, per fornire al lettore un elemento sintetico di raffronto dialettico rispetto alle proprie aspettative e ai propri orientamenti, nella convinzione che, in un ambito ancora così poco consolidato come l'utilizzo dei Social Media da parte delle imprese, la possibilità di confrontarsi ed, eventualmente, dissentire sia un elemento di grande importanza per ridurre i margini di rischio nelle scelte di investimento.

**TABELLA 2 - PRIMA MATRICE DI FINALITÀ**

| Utilizzo dei social media da parte delle imprese **Matrice tipologia-finalità** | **Uso interno: B2B/B2E** | | | | | | **Uso esterno: B2C** | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Comunicazione Tipol. - Rilevanza** | | **Condivisione Tipol. - Rilevanza** | | **Collaborazione Tipol. - Rilevanza** | | **Comunicazione Tipol. - Rilevanza** | | **Condivisione Tipol. - Rilevanza** | | **Collaborazione Tipol. - Rilevanza** | |
| Co-creare prodotti | Microblogging | 6 | Microblogging | 6 | Design<br>Tech | 10<br>8 | | | Microblogging | 6 | Design<br>Tech | 8<br>6 |
| stimare, prevedere e monitorare | Blogging | 5 | Blogging | 5 | | | | | | | | |
| Distribuire processi di business | | | Community<br>Business | 8<br>8 | Community<br>Business | 8<br>8 | | | | | | |
| Ottenere pareri dai consumatori | | | | | | | Microblogging | 9 | Blogging<br>Microblogging | 7<br>8 | Community | 8 |
| Marketing volto a comunicare/interagire | Business<br>Video<br>Blogging | 8<br>7<br>6 | Community | 8 | | | Business<br>News<br>Video | 8<br>6<br>8 | Blogging<br>Microblogging | 8<br>6 | | |
| Selezionare personale | Business<br>Video | 8<br>6 | | | | | Business 8,<br>News 6,<br>Video 8 | 8<br>6<br>8 | | | | |
| Lead generation | Business | 6 | | | | | Business 7 | 7 | | | | |
| Social Commerce | Business | 6 | | | | | Business 8,<br>News 6,<br>Video 8 | 8<br>6<br>8 | | | | |
| Fornire assistenza ai consumatori | | | | | | | Community<br>Microblogging<br>Tech | 10<br>8<br>9 | Bookmarking<br>Information | 6<br>6 | Community | 6 |
| Migliorare la collaborazione e comunicazione dell'organizzazione | Video<br>Blogging | 9<br>7 | | | Community | 8 | Tech<br>Video | 7<br>8 | Blogging<br>Tech | 6<br>7 | | |
| Associare talenti ai lavori (crowd sourcing) | Business | 7 | | | Tech | 8 | Business 7 | | | | Design<br>Tech | 8<br>8 |

**TABELLA 3 - SECONDA MATRICE DI FINALITÀ**

| Utilizzo dei social media da parte delle imprese **Matrice tipologia-obiettivi di business** | | **Uso interno: B2B/B2E** | | | | | | **Uso esterno: B2C** | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | **Comunicazione Tipol. - Rilevanza** | | **Condivisione Tipol. - Rilevanza** | | **Collaborazione Tipol. - Rilevanza** | | **Comunicazione Tipol. - Rilevanza** | | **Condivisione Tipol. - Rilevanza** | | **Collaborazione Tipol. - Rilevanza** | |
| Ridurre i costi | Aumentare la velocità di accesso al sapere | | | Bookmarking | 8 | | | | | Information | 6 | | |
| | Ridurre i costi di comunicazione | Video | 8 | | | | | Community Microblogging | 8 6 | | | | |
| | Velocizzare l'accesso ad esperti/interni | Video | 7 | | | Tech | 8 | Community | 7 | | | Design Tech | 8 8 |
| | Ridurre i costi di trasporto | Video | 9 | Travel | 7 | | | | | Travel | 5 | | |
| | Aumentare la soddisfazione dei dipendenti | | | Community | 8 | | | | | | | | |
| Aumentare i ricavi | Merchandising | | | | | | | Video | 7 | | | | |
| | Aumentare il numero di innovazioni di successo | | | Community | 8 | Tech | 8 | | | | | Design Tech | 8 8 |
| | Ridurre il time-to-market | | | | | Tech | 9 | | | | | Tech | 9 |

Dal punto di vista della Sicurezza i Social Media veicolano diversi tipi di minacce, in conseguenza della loro funzione prevalente.

Questo fenomeno deve essere attentamente considerato in sede di adozione di una particolare piattaforma di Social Networking, in modo da poter approntare le opportune contromisure fin dal principio, ottimizzando gli investimenti in sicurezza conseguenti. Per un approfondimento di questo tema si rimanda alla sezione dedicata ai rischi connessi con l'uso dei Social Media.

## Aspetti economici: il ROI dei Social Network

Calcolare il ROI (Return on Investment) implica l'individuazione dei costi e dei ricavi derivanti dalle proprie attività Social, compito difficile che presenta non poche criticità, legate alla necessità di selezionare informazioni significative all'interno di un "chiasso" altissimo e perdurante, alla loro possibile manipolazione, alla difficoltà di stabilirne la rilevanza ed alla assenza di modelli interpretativi.

Questo tema è molto caldo in quanto le società hanno bisogno di sapere quali effetti sortiscono le loro iniziative "Social" in modo da poter prendere decisioni informate e perseguire strategie strutturate. Tuttavia i Social Network sono piattaforme molto fluide, dove le informazioni provenienti da diverse fonti e di diversa natura si sovrappongono e appaiono come una indistricabile matassa. Dunque molti ricercatori si sono dedicati all'individuazione di una metodologia che restituisca informazioni e dati quantitativi utilizzabili, ma l'obiettivo non è facile da raggiungere e generalizzare una tale pratica risulta ancora più sfidante in virtù dei diversi usi e contesti con i quali le (diverse) aziende si confrontano nell'affrontare il mondo dei Social Network.

Nonostante le difficoltà di misurazione e i problemi relativi alla trasparenza dei risultati ottenuti, è bene che ogni azienda faccia del proprio meglio per valutare in termini economico-reddituali, e dove possibile finanziari, i propri sforzi in rete, con particolare riferimento ai risultati derivanti dai Social Network che oggigiorno rappresentano un' inestimabile fonte di dati/informazioni.

Prima di entrare più in profondità nel tema oggetto di questo capitolo, è opportuno riprendere e valutare anche sotto questo profilo, le considerazioni sopra riportate a proposito dell'utilizzo passivo dei Social Media da parte delle aziende.

Vi è infatti un onere indotto sulle aziende derivante dalla semplice esistenza dei Social Media e dalla possibilità di esservi citati - positivamente o negativamente - a propria insaputa, in relazione a decisioni aziendali critiche come l'attivazione di procedure di cassa integrazione o la delocalizzazione di stabilimenti produttivi, o il cambiamento di prodotti o servizi. Oppure causati dalla frequentazione dei Social Media da parte di

dipendenti, magari con l'utilizzo di dispositivi di loro proprietà ad uso ibrido aziendale-personale.

L'entità dell'onere varia in funzione della tipologia del business aziendale: la proprietà di marchi consumer molto conosciuti porta inevitabilmente ad una maggiore esposizione rispetto ad attività di produzione di beni rivolti all'industria; un operatore turistico è inevitabilmente esposto ai giudizi ex post dei propri clienti e anche, come si è visto in alcuni casi, al tentativo dei concorrenti sleali di deprimere artatamente l'immagine aziendale.

Quando ci si riferirà, dunque, al ritorno degli investimenti, nel valutare i costi sostenuti bisognerà considerare solo quelli aggiuntivi rispetto allo sforzo comunque necessario per raggiungere quella che può essere definita la "Social Media Neutrality" applicando metodologie e strumenti di Reputation Management.

Per stimare i costi e ricavi alla base del calcolo del ROI, si devono necessariamente quantificare gli sforzi volti a raggiungere obiettivi esplicitati nel piano di Social Media Marketing, o altri obiettivi che l'organizzazione si è posta, e i relativi risultati, attraverso attività di monitoraggio, raccolta dati, analisi comparative e statistiche.

Bisogna considerare che ci sono elementi di rischio connessi alla relazione con terzi che devono essere valutati caso per caso (ad esempio quando tramite la propria iniziativa vengono coinvolti i minori o viene propagato da terzi del malware ai propri fans). Questi rischi per essere contrastati comportano dei costi aggiuntivi specifici di ciascun progetto, che non possono rientrare in questa trattazione di carattere generale.

Menzioniamo di seguito, a titolo esemplificativo, alcuni aspetti utili a valutare il ritorno "marketing" dell'uso del Social Media in azienda, con l'osservazione che spesso appare più utile effettuare tali misurazioni in termini relativi, esprimendo i valori in percentuali e tassi: il valore sta crescendo? Rispetto ai concorrenti come va? Ecc…

Cosa misurare:

- Livello di customer engagement
- La natura dei dialoghi che ti riguardano da parte dei consumatori, o "sentiment"
- La reputazione del brand sui Social Network
- La qualità delle relazioni col mercato target
- Il livello di partecipazione alle conversazioni online
- Il posizionamento rispetto ai concorrenti

Misure quantitative:

- Misurazione di performance interna
  - Traffico alle tue pagine Social o sul sito
  - Click-through rate dei tuoi post Social
  - Quali prodotti sono più venduti/apprezzati
  - Conversion rate: gente che diventa acquirente o contatto commerciale valido
- Misurazione economica
  - Costo per ottenere un consumatore o contatto commerciale in più
  - Valore relativo di ciascun contatto commerciale
  - Break-even point
  - ROI

## Return on Security Investiment

Questa community negli anni scorsi, ha anche lavorato sul ROSI ovvero il ROI dei progetti di sicurezza (http://rosi.clusit.it). A tal proposito si rimanda al relativo documento per maggiori dettagli, ma qui di seguito si danno alcune indicazioni su come valutare la bontà economica di alcune misure tecnologiche ed organizzative relative alla sicurezza dei progetti Social Media.

Ecco, dunque, alcune indicazioni pratiche sul ROSI, visto che il management spesso richiede decisioni razionali sostenute numericamente.

- Nel calcolare i costi e i ritorni del Social Media (ROI) non dimenticarsi dei costi della mancanza di sicurezza o di implementazione delle misure compensative. Solo includendo anche questi ultimi il quadro è davvero completo. E', infatti, necessario che l'azienda finanzi il progetto Social nella sua interezza. Rimandare gli aspetti di sicurezza ad una seconda fase è più costoso e deleterio. Può compromettere il successo del progetto.
- Non imputare ad uno specifico progetto Social Media ed alle misure di sicurezza ad esso collegate i costi necessari a raggiungere la Social Media Neutrality sopra spiegata. Tali costi devono far parte dell'impianto aziendale base, così come l'edificio dove lavorano le persone.
- Valutare il ritorno degli investimenti tecnici ed organizzativi (le misure) considerando da una parte i costi necessari (tempo, risorse, denaro) fissi e variabili in maniera consueta e dall'altra il ritorno inteso come riduzione economica dell'impatto degli eventi avversi.

In merito a quest'ultimo aspetto, nella valutazione degli investimenti in sicurezza, è prassi, con tutte le difficoltà del caso, valutarli economicamente tramite formule che legano la probabilità di un incidente con il danno causato dallo stesso.

In tale danno si considerano tutti i costi diretti ed indiretti relativi alla scoperta, analisi e remediation. In linea generale è necessario considerare:

- Il rischio operativo
- La perdita di immagine aziendale
- Il rischio di compliance.

La probabilità viene stimata tramite l'ausilio di fonti esterne di tipo statistico oppure basandosi sul giudizio degli esperti e in rarissimi casi a partire dallo storico dei sistemi aziendali di tracciatura degli incidenti.

Nel caso in cui alcune misure portino all'automazione dei processi di controllo si può considerare il risparmio dovuto alla diversa distribuzione dei costi le diverse voci.

Affidandosi ad esperti è possibile fornire valutazioni numeriche anche per quegli eventi rari ma possibili e a carattere disastroso (il cosidetto cigno nero).

Un ultimo punto riguarda l'interdisciplinarità delle misure e dei relativi "stakeholder". Molte delle misure ipotizzabili impattano su diversi attori aziendali: spesso quelli interessati al fatto che le misure siano realizzate e sono diversi da quelli su cui ricade l'onere della implementazione della misura. E' importante quindi che colui che valuta il ROSI di un investimento di Social Media Security abbia bene in mente queste relazioni.

Ad esempio:

- Compliance. Usare attivamente o permettere l'uso di un Social Network ha dei risvolti di compliance. Ad esempio per la privacy il "principio di necessità nel trattamento nei dati" di cui all'art. 3 della legge 196/03 oppure per le misure di controllo l'art. 4 dello statuto dei lavoratori (si veda, nello specifico il parere 1/2010 del gruppo di lavoro Articolo 29). La compliance interessa all'ufficio legale.
- Protezione dell'immagine aziendale. Usare i Social attivamente dà voce ai propri fans e anche ai propri avversari, oltre che al personale autorizzato dall'azienda a rappresentarla nel Social. Ad esempio c'è e qual è l'impatto del Social Network usato come veicolo per screditare un brand concorrente? L'immagine aziendale interessa al marketing.

- Protezione dei propri clienti. Qual è la responsabilità dell'azienda quando un attaccante abusi della relazione fiduciaria per propagare malware sui computer e device dei propri clienti? La protezione dei clienti interessa al direttore vendite.
- Attacchi alla proprietà intellettuale propria ed altrui. Può capitare nelle pieghe del Social network, incrociando le clausole contrattuali del fornitore del Social Network, le leggi di diversi stati nazionali e il comportamento degli utilizzatori siano essi clienti finali oppure dipendenti o collaboratori aziendali. Questi aspetti interessano a diversi: almeno al legale e alla ricerca e sviluppo.
- Protezione dell'investimento. Per esempio in ragione del fatto che un servizio concepito in un certo modo e concesso dal fornitore del Social Network può cambiare o essere cancellato e non soddisfare più le esigenze aziendali e il patrimonio informativo inserito in esso corre il rischio di essere perso. Buttar via il denaro non piace a nessuno, in questo caso indichiamo il direttore finanziario oppure colui che ha speso in azienda la sua credibilità per realizzare il progetto Social.

Queste considerazioni, anticipando altre conclusioni di questo documento, suggeriscono di raccogliere periodicamente intorno ad un tavolo tutte le funzioni aziendali interessate al Social, formalizzando questi momenti con l'istituzione di un Social Media Governance Board. In questo modo anche la valutazione dei rischi e dei costi per contrastarli potrà essere correttamente condivisa da tutti gli interessati.

# PARTE SECONDA: PER UN PROGETTO SOCIAL SICURO

I capitoli precedenti hanno introdotto, descritto e provato a catalogare secondo una logica funzionale alle finalità di questo documento il fenomeno dei Social Media. In questa seconda parte si affrontano i temi che ne sono invece l'obiettivo centrale, quel nocciolo duro che, come si diceva all'inizio, si annida nella polpa succosa della ciliegia e che, se ignorato, può provocare molti danni.

Non ci sono regole che risolvono a priori tutti i problemi. Quelle contenute nei capitoli che seguono sono osservazioni, indicazioni, suggerimenti utili a mettere a fuoco, a non sottovalutare aspetti che, considerati opportunamente in sede di impostazione e progettazione, non comportano oneri rilevanti mentre, se trascurati, possono obbligare a faticose rincorse per recuperare situazioni sfuggite dal controllo.

Ci auguriamo, anche, di fornire argomenti utili ad ottenere la giusta attenzione per la sicurezza da parte di chi deve decidere sull'allocazione delle risorse, spesso giustamente distante dagli aspetti tecnici delle diverse tecnologie.

## I Social Media in azienda: istruzioni per partire

Come accennato, la sicurezza nei progetti Social Media ha molte e diverse implicazioni ma ci sono alcune regole di base, in alcuni casi forse perfino ovvie, che è opportuno considerare per partire con il piede giusto.

Nella pagina dell'impresa all'interno del Social Network deve essere caricato il **logo aziendale** e devono essere riportati il link del sito web aziendale e l'indicazione dei contatti aziendali (sede fisica, telefono, fax, orari di apertura uffici) in modo tale da rappresentare ai terzi il carattere istituzionale ed ufficiale della pagina ed individuare in maniera univoca l'identità: è preferibile non inserire e riportare dati, valutazioni riconducibili alle singole persone.

Nelle informazioni generali occorre descrivere la mission aziendale e riportare il link al codice etico aziendale che stabilisce i principi e regole nelle relazioni con clienti, fornitori, colleghi e stakeholders. È utile riportare i link delle pagine ufficiali delle imprese sui diversi Social Network.

Si consiglia in un'ottica di economicità ed efficienza di riportare nella pagina del Social alcuni indirizzi di posta elettronica dedicati, per segnalazioni e reclami in materia di violazione di copyright, privacy, furti di identità, reati informatici ed eventuali disservizi. In alcuni casi l'esplicitazione di queste informazioni è richiesto da specifiche normative.

Si consiglia inoltre di nominare gli amministratori della pagina ed i moderatori dello spazio aziendale sul Social Network e di specificare che la voce ufficiale della azienda sulla pagina del Social viene espressa unicamente dal moderatore / admin e non può essere rappresentata da altri soggetti, dipendenti o collaboratori dell'azienda che dovessero intervenire sulla pagina.

Gli amministratori e moderatori devono attenersi a precise regole ed istruzioni nel rigoroso rispetto della normativa privacy. Occorre ribadire la natura istituzionale e

aziendale dello spazio sul Social Network anche attraverso le modalità di linguaggio e di intervento e di ingaggio utilizzate dal moderatore.

Al fine di ottimizzare la presenza sul Social Network e di gestire il processo di condivisione di informazioni e contenuti, risulta utile per l'impresa elaborare **due preziosi documenti: la policy Social Media ad uso esterno e quella relativa all'ad uso interno.**

## Social Media Policy

L'adozione di una Social Media Policy è utile per regolare il comportamento dell'impresa nei seguenti casi:

1. utilizzo dei Social Media da parte di dipendenti o collaboratori durante l'orario di lavoro e/o con l'eventuale utilizzo degli strumenti aziendali
2. utilizzo dei Social Media da parte dell'azienda stessa per finalità di natura interna (ad es. comunicazione con i dipendenti, condivisione di informazione all'interno di gruppi di lavoro, etc.)
3. utilizzo dei Social Media da parte dell'azienda stessa per finalità di business rivolte al mercato.

Le misure che comunemente le aziende adottano per cercare di controllare l'utilizzo dei Social Media da parte dei dipendenti, con interventi tecnici puramente restrittivi come sistemi di web filtering, finalizzati a inibire l'accesso a tali piattaforme dalla rete aziendale, non rappresentano certamente il modus operandi più produttivo ed efficace e soprattutto non esauriscono il tema in quanto riguardano solo uno dei tre casi di cui sopra.

Peraltro, il ricorso, assai diffuso, a strategie di BYOD ("Bring Your Own Device"), che consentono ai dipendenti l'utilizzo a fini lavorativi dei propri device mobili personali (smartphone e tablet), rende questo approccio inefficace anche rispetto ad obiettivi di controllo sull'uso del tempo da parte dei dipendenti e sulla sicurezza delle informazioni e degli asset aziendali.

Un processo evoluto di individuazione, gestione e mitigazione dei rischi correlati all'utilizzo dei Social Media deve iniziare con la delimitazione dell'ambito di interesse. Quest'ultimo non può non considerare almeno i tre casi sopra riportati, rispetto ai quali deve essere valutato il livello di adeguatezza e di allineamento delle policy vigenti di Information Security, comunicazione e marketing rispetto al perimetro individuato.

L'esclusione di uno dei tre casi dall'ambito di interesse deve essere considerata con grande attenzione: a questo proposito si rimanda alle considerazioni svolte in altre parti di questo documento sul coinvolgimento passivo e involontario che può interessare le aziende e generare comunque la necessità di una risposta.

La definizione di policy adeguate alla complessità ed alla rilevanza del tema relativo alla gestione dei Social Media in azienda è la base per una gestione corretta dell'impatto dei Social Media sulle relazioni con i dipendenti ed i collaboratori in genere da un lato e con tutti i soggetti terzi interessati dai processi di business dall'altro: clienti, agenti, manutentori, fornitori in genere.

Naturalmente la definizione di tali policy e la loro effettiva attuazione sono l'atto terminale di un processo che, almeno per ciascuno dei tre casi indicati, consideri:

- rischi da presidiare;
- policy e procedure in essere;
- capacità di gestione del rischio delle policy in essere;
- necessità di aggiornamento delle policy;
- sistemi di monitoraggio del livello di applicazione delle policy;
- efficacia e applicazione delle policy in essere.

In generale ciascuna policy dovrà affrontare e definire alcuni temi fra cui:

1. Finalità
2. Perimetro di applicazione
3. Valori chiave
4. Misure di sicurezza da implementare
5. Implicazioni di compliance a normative
6. Identificazione di ruoli e di responsabilità
7. Formazione e commitment del Management
8. Revisioni
9. Sanzioni disciplinari
10. Destinatari

Non sempre si tratta di affrontare tematiche radicalmente innovative quanto di ripensare, in un contesto diverso, temi già affrontati in ambito aziendale. Certamente le modifiche indotte da questo cambiamento di prospettiva possono comportare una radicale trasformazione degli approcci tradizionali e questo deve riflettersi nelle policy in modo chiaro.

Le politiche di sicurezza in particolare sono pesantemente impattate mentre i ruoli aziendali necessari per gestire questo fenomeno riflettono la novità del tema, come si può evincere dalla trattazione dei capitoli a questo dedicati.

In base alle considerazioni presentate nel paragrafo precedente si possono quindi articolare due diverse policy relative all'utilizzo dei Social Media che vengono di seguito trattate.

### La Social Media Policy ad uso esterno

In questo caso occorre individuare le regole di netiquette da seguire all'interno del prezioso spazio di interazione e dialogo del Social Network in linea con le condizioni generali di utilizzo dello stesso (ad esempio: https://www.facebook.com/legal/terms).

Nella policy conviene precisare che l'azienda non è responsabile dei commenti e dei contenuti pubblicati sulla pagina Social aziendale dagli utenti. Naturalmente occorre specificare che l'azienda si riserva il diritto di rimuovere, anche senza preavviso e a propria discrezione, dalla pagina aziendale del Social Media qualunque commento, in particolare i commenti ed i materiali offensivi, volgari, classificabili come istigazione alla violenza, all'intolleranza e alla discriminazione ovvero in violazione del diritto alla protezione di dati personali (privacy), copyright, marchi, diritto all'immagine e della relativa Social Media policy adottata.

Occorre specificare che l'azienda può bloccare e segnalare al Social Media interessato gli utenti che hanno infranto la policy e nei casi più gravi ricorrere alla Polizia Postale (le aziende devono considerare che la omessa rimozione di contenuti illeciti od offensivi può comportare il rischio di corresponsabilità).

Di seguito i link ad alcune Social Media policy aziendali per l'ambiente Facebook:

- http://www.fiat.it/it/policy/fb-policy
- https://www.facebook.com/legal/terms#!/UniCreditItalia/app_208195102528120
- https://www.facebook.com/BusinessInsieme/app_453135061368613

In riferimento al diritto alla protezione dei dati personali occorre specificare e avvertire gli utenti in modo semplice e diretto della possibilità che i dati, le informazioni, i commenti postati possono essere indicizzati dai motori di ricerca generalisti ed essere conosciuti senza limiti di tempo e di spazio dalla generalità degli utenti di internet e non dai soli iscritti alla pagina aziendale.

Occorre richiamare la propria privacy policy del sito aziendale ed illustrare agli utenti l'utilizzo o meno di cookies e specificare che l'azienda tratterà i dati visibili degli utenti sulla piattaforma on line esclusivamente al fine di rispondere a quesiti e commenti sui propri prodotti e servizi dagli stessi inviati e per il tempo strettamente necessario per il perseguimento di tale finalità. Nel caso di promozione di concorsi on line o questionari tramite Social sui servizi erogati dall'azienda, occorre specificare che i dati saranno raccolti direttamente dalla società e non dalle piattaforme ospitanti.

Nel caso di spazi virtuali dedicati alla salute, all'interno della pagina blog e forum, occorre inserire una specifica "avvertenza di rischio", il cui scopo è quello di richiamare l'attenzione degli utenti sui rischi connessi al fatto di rendersi identificabili sul web in relazione alla propria patologia [6]. Occorre inserire alcune regole di comportamento nelle operazioni di caricamento di fotografie e video da parte degli utenti e specificare che gli stessi devono acquisire il consenso delle persone ritratte.

In riferimento al diritto di autore, occorrerebbe specificare che i materiali pubblicati dall'azienda, all'interno dello spazio Social, qualora non diversamente indicato, sono di proprietà dell'impresa e coperti da copyright; occorrerebbe inoltre richiedere agli utenti di prestare molta attenzione all'utilizzo dei contenuti, video, musica, foto, materiali di terzi soggetti coperti dal copyright e segnalare agli stessi di non pubblicare materiali coperti da copyright senza la relativa autorizzazione e raccomandare agli utenti di caricare i contenuti, musiche, video rilasciati con licenze creative commons, in quanto utilizzabili liberamente e gratuitamente al fine di non esporre l'azienda ad eventuale contenzioso (es. chiusura dello stesso profilo sul Social Network).

Occorre specificare che l'azienda compie ogni sforzo possibile per migliorare il livello di completezza e aggiornamento delle informazioni e dei contenuti, è possibile per gli utenti segnalare all'impresa in modo rapido e gratuito eventuali abusi attraverso uno specifico form.

La policy esterna deve inoltre specificare agli utenti in modo semplice e trasparente quali soggetti aziendali all'interno dell'azienda (administrator; moderatore) siano autorizzati a rispondere in via ufficiale ai commenti postati on line (principio dell'affidamento esterno). La policy esterna deve inoltre rappresentare agli utenti che l'azienda non è in alcun modo responsabile della mancata fruizione della piattaforma on line o dei relativi collegamenti alla piattaforma on line.

## La policy Social Media ad uso interno.

La Social Media policy interna ha la funzione di illustrare le regole di utilizzo del Social Network da parte del personale aziendale e dei collaboratori e i vari livelli di responsabilità all'interno dell'impresa. Rientrano in questo ambito sia l'utilizzo privato di Social Media da parte di dipendenti o collaboratori sia l'utilizzo da parte dell'azienda per esigenze organizzative interne (piattaforme di collaborazione, condivisione di contenuti, etc.) che possono coinvolgere oltre a dipendenti anche soggetti esterni coinvolti nei processi organizzativi (agenti, manutentori, …)

Il dipendente deve utilizzare il Social Network nel rispetto del disciplinare in materia di posta elettronica ed internet (Provvedimento Garante Privacy del 1/3/2007) - che deve essere adeguato se necessario - e delle regole aziendali sull'utilizzo del marchio aziendale e deve conformare la propria attività ai principi del codice etico aziendale e ai principi di correttezza e all'eventuale piano di comunicazione aziendale.

Deve essere chiarito che ogni qualvolta l'utilizzo personale di Social Media, per le modalità di accesso o per le informazioni scambiate, consenta di correlare il dipendente alla propria azienda, questi deve adottare un comportamento corretto in quanto la sua attività potrebbe essere comunque associata a quella dell'organizzazione.

I dipendenti devono essere consapevoli che un commento inappropriato sui Social anche per finalità private può avere un effetto negativo sul brand e sulla reputazione della società datrice di lavoro o essere sfruttato da terzi per un attacco all'azienda stessa..

I dipendenti devono essere informati che l'uso di strumenti aziendali per accedere ai Social Media o l'uso promiscuo, aziendale-privato, di strumenti privati può comportare rischi per la sicurezza delle informazioni e degli asset aziendali. A loro devono essere quindi fornite delle linee guida sul comportamento da tenere per minimizzare tali rischi e procedure operative in caso di situazioni sospette.

Alcune società richiedono ai dipendenti di rappresentare anche negli account privati l'appartenenza all'azienda. Tale opzione deve essere valutata con attenzione, sia sotto il profilo della legittimità che della opportunità ed, eventualmente, limitata a figure particolari.

Occorre adottare e attestare il rispetto della policy da parte anche di consulenti esterni, collaboratori, stagisti ed ex collaboratori e fare siglare specifici accordi di riservatezza.

Nel caso di violazioni della policy Social Media interna, occorre specificare che si applicheranno le sanzioni disciplinari previste dal contratto collettivo di settore e le sanzioni previste dal codice etico aziendale, quando non si configurino violazioni più gravi.

In considerazione del continuo flusso di dati veicolati dai Social Media, in funzione dei rischi associabili all'esposizione aziendale e nell'ottica di assicurare continuità di servizio, occorre valutare l'opportunità di garantire, una reperibilità di 24 ore dell'amministratore e dei moderatori e prevedere specifici incentivi alla luce dei risultati dell'attività svolta.

Nell'ottica di assicurare un presidio efficace occorre valutare l'opportunità di creare, all'interno dell'azienda, un piccolo staff interdisciplinare (informatici e legali) a tutela della presenza dell'azienda sui Social, con la funzione di verificare costantemente le condizioni generali di utilizzo dei Social Network ed in particolare i canali dei centri servizi per segnalare violazioni di diritto di autore e privacy.

Uno dei compiti principali dello staff dovrebbe essere la redazione di un protocollo per la gestione di una criticità (ad esempio contenuto diffamatorio, accuse all'azienda di avere

commesso dei reati o di violazione della privacy, copyright, diritto all'immagine etc.) con indicazioni, in particolare, della catena di custodia delle prove informatiche; altro compito dello staff dovrebbe essere la promozione di attività di informazione e incontri di formazione in materia in considerazione dell'aspetto virale del web e delle potenzialità dei Social Media.

## Ruoli sui Social Network

Per adottare un processo sistematico di **Social Media Management**, le Aziende devono essere in grado di definire strategie, obiettivi, policy, livelli di rischio accettabili e strumenti utili a misurare l'efficacia dei propri investimenti.

Non solo la moderazione e la gestione della "***real time conversation***" sono processi chiave per sostenere una strategia efficace ed un posizionamento sostenibile nell'ecosistema Social, ma, dal momento che i Social Media sono per loro natura terreno fertile per azioni di Competitive Intelligence da parte di concorrenti, Social Engineering, truffe e furti di dati da parte della criminalità informatica, occorre anche proteggere il Brand e le informazioni che sono alla base del core business aziendale, tanto dagli attacchi esterni, quanto da quelli provenienti dall'interno.

Risulta dunque di fondamentale importanza adottare un insieme di attività di **analisi**, **moderazione**, **monitoraggio**, **tutela legale**, **prevenzione delle minacce** e **gestione degli incidenti**, sia per ottimizzare il ROI dei Social Media sia per evitare danni economici o d'immagine (anche importanti e complessi da sanare), o per rimediare ove si siano già verificati.

La gestione dei Social Media non può quindi essere considerata un problema esclusivamente del Marketing né (solo) dell'IT, ma si deve prevedere un approccio multidisciplinare che includa un legale con conoscenze specifiche e un esperto di Sicurezza dei Social Media.

Solo in questo modo l'attività di Social Media Management potrà essere esplicata lungo le tre dimensioni:

- il piano della Comunicazione, in ottica di gestione e protezione del Brand , di definizione del Mix e di misurazione dei risultati tramite opportuni KPI
- quello relativo alla Protezione Legale, alla compliance normativa, all'allineamento con le best practice internazionali e con le leggi nazionali
- il piano dell'ICT Security, sotto i profili della formazione, organizzativo, della gestione del rischio, della sicurezza dei dati e dell'infrastruttura tecnologica.

Di seguito una breve descrizione dei principali ruoli e delle relative funzioni utili alla gestione della presenza di un Brand sui Social Media.

### 1. Social Media Manager

Il Social Media Manager ha il compito di gestire la presenza di un'azienda sui Social Network.

Sempre aggiornato sugli ultimi trend della comunicazione, favorisce l'interazione con i follower/fan di un determinato prodotto, evitando una promozione troppo esplicita del brand.

Oltre ad avere un'approfondita conoscenza dei Social Network, è in grado di applicare efficacemente le strategie di web marketing e di conoscere, sapendoli sfruttare al meglio, i meccanismi dei nuovi media (search engine marketing, web analytics, geolocalization, ..) e le peculiarità di ciascun Social Network.

### 2. Moderatore

Il Moderatore è una figura nata originariamente nell'ambito dei forum di discussione su Internet.

I compiti del moderatore nell'ambito dei Social Network includono la gestione della conversazione nel rispetto della Social Media Policy aziendale, il monitoraggio, la modifica e, se necessario e fattibile, l'eliminazione di post o commenti inadeguati oltre a bandire (ove possibile) o a segnalare utenti inopportuni.

**3. Social Media Ambassador**

Il Social Media Ambassador pubblicizza gratuitamente il brand di un'azienda tramite i Social Network.

Naturalmente fedele al brand che rappresenta, ama condividere esperienze su prodotti e/o servizi personalmente utilizzati raccomandandoli ad amici e contatti della propria rete sociale.

Il SMA diffonde molte informazioni sul brand, utilizzando siti con buona visibilità e molto frequentati, creando contenuti di qualità in grado di influenzare gli acquisti altrui.

**4. Brand Reputation Manager**

Il Brand Reputation Manager ha il compito di gestire la reputazione online di un'azienda.

Il principale compito del BRM riguarda il monitoraggio delle discussioni online allo scopo di comprendere come viene percepito il Brand, in particolar modo dagli utenti più attivi. Tramite tale monitoraggio è infatti possibile trarre informazioni sulle possibili azioni da compiere per attenuare eventuali percezioni negative o per enfatizzare quelle positive.

Infine, il BRM si occupa di condividere contenuti di qualità e partecipare attivamente alla conversazione.

**5. Privacy Officer**

Il Privacy Officer ha il ruolo di osservare, valutare e organizzare la gestione del trattamento di dati personali e della loro protezione all'interno di un'azienda, nel rispetto delle normative vigenti.

Deve possedere un'adeguata conoscenza della normativa sulla gestione dei dati personali del paese in cui opera, curando l'adozione di misure minime di sicurezza finalizzate alla tutela dei dati che soddisfino i requisiti di legge e assicurino sicurezza e riservatezza.

Infine il PO affianca i responsabili del trattamento dei dati in materia di protezione dei dati personali e verifica che il regolamento relativo venga debitamente seguito, fungendo, se necessario, da punto di contatto per l'autorità di controllo.

**6. Community Manager**

Il Community Manager gestisce una comunità virtuale, ne progetta la struttura e coordina le attività, selezionando strumenti e servizi adatti e avvalendosi, se necessario, di moderatori, promotori o di altre figure che lo affianchino.

Essendo a tutti gli effetti il volto e la voce del Brand nelle community, è necessario che conosca perfettamente le caratteristiche del prodotto e/o servizio dell'azienda che rappresenta.

Deve essere in grado di comprendere e supportare le esigenze dei partecipanti alla community, stimolare la conversazione e gestire le varie tipologie di utenti (dai *lurkers*, che leggono ma non intervengono, agli iperattivi), definendo le regole di comportamento.

Tramite la valutazione dei feedback e dei livelli di brand advocacy (l'atto spontaneo di un consumatore che raccomanda un Brand) è in grado di operare per determinare il successo della campagna promozionale effettuata sul Web.

**7. Social Media Policy Maker**

Il Social Media Policy Maker ha il compito di formalizzare un framework di regole (Social Media Policy) per dipendenti, collaboratori e fornitori atte a regolamentare l'utilizzo in ambito aziendale dei nuovi media, minimizzando i rischi e chiarendo le opportunità offerte da un uso sensato.

Infine il Social Media Policy Maker deve ideare apposite linee guida per i casi di abuso e attacchi informatici.

Si noti che la nostra raccomandazione è estensiva rispetto alla concezione normalmente riscontrata sul mercato.

# Il lato oscuro dei Social Media: le nuove minacce

## Introduzione

In questo capitolo si analizzeranno i rischi per la sicurezza dei Social Media, degli strumenti e dei mezzi che fanno già da tempo parte della nostra quotidianità e che, ultimamente, si stanno sempre più muovendo verso l'integrazione con il mondo business.

I Social Network sono diventati, a causa della loro forte espansione, oggetto di malware, attacchi di tipo Social Engineering, spam, phishing, furti di identità, diffamazione e frodi di ogni tipo. Se si considera l'ambito business in particolare, si aggiungono anche ulteriori minacce come, furto, perdita o diffusione incontrollata di dati riservati, di proprietà intellettuale e di informazioni sensibili (protette da normative) o informazioni strettamente private dell'azienda, ma anche danni all'immagine e reputazionali e possibilità di essere oggetto di spionaggio industriale da parte di competitor.

Nel seguito riportiamo un elenco delle principali aree di rischio che acquisiscono con l'utilizzo di Social Media una rilevanza ancora maggiore o, in taluni casi, che si sono sviluppate in stretta associazione con l'affermarsi dei Social Media.

Si tratta di minacce rivolte in generale agli utilizzatori dei Social Media, che siano aziende o utilizzatori privati ma, certamente si tratta di tematiche di cui una azienda deve tenere conto per sé stessa e per i propri interlocutori nel momento in cui decide una strategia di presenza su un Social Media.

E' infatti interesse dell'azienda che i propri interlocutori Social siano consapevoli delle loro azioni e ne possano valutare con serenità le conseguenze a priori, sia in riferimento al proprietario del Social Media sia per quanto riguarda i possibili attacchi di cui, attraverso la rete Social e, in particolare anche attraverso la relazione con l'azienda, può essere vittima.

Infatti, quello che sembra essere un contatto più diretto con i consumatori o con i dipendenti è, in realtà, un contatto mediato da soggetti terzi che detengono diritti materiali sulle informazioni trattate e da strati tecnologici molto spessi sui quali l'azienda non ha alcuna capacità di influenza.

## Le minacce.

### *Identity assurance inadeguata*

L'Identity Assurance (IDA) è la possibilità di determinare con un certo livello di sicurezza, l'attendibilità delle credenziali di comunicazione affidati ad un'entità attesa. "Trust is often assumed but not always verified" (ovvero "Si ripone spesso fiducia senza mai verificarla") è una frase che racchiude in maniera appropriata un insieme di politiche della "non-cultura" sull'uso e sulla pericolosità dei Social Media e del mondo internet in generale. La natura di internet è, infatti, basata sull'autocertificazione di identità e non sulla verifica della stessa. La totale inattendibilità delle fonti è spesso veicolo per attacchi fraudolenti, diversamente da quanto succede nella vita quotidiana "off-line" dove, per operazioni considerate "critiche" o "rilevanti" ci si serve di metodi di identificazione e registrazione puntuale del soggetto interessato.

### *Profilazione utenti*

Ogni qual volta si parla di Social Network si fa inevitabilmente riferimento al concetto di profilazione utenti, caratteristica molto utile per aziende che investono in pubblicità su queste piattaforme, in quanto permette loro di capire e conoscere più dettagliatamente la propria clientela e quindi migliorare l'offerta.

Molti utenti non sono coscienti del fatto che ogni loro pubblicazione, ogni loro commento ed ogni pagina visualizzata sui Social Network è un input per i motori di profilazione che costruiscono a insaputa degli utenti un profilo virtuale molto dettagliato per offrire loro contenuti adeguati ai loro interessi. Uno degli aspetti negativi della profilazione è che l'utente profilato è inconsapevolmente indotto dal Social Network a seguire percorsi di navigazione coerenti con il profilo e non quelli determinati da un'interazione casuale. A questo si aggiunge la vendita dei dati dei profili ad aziende esterne.

### *Acquisizione di informazioni sui contatti*

La natura dei Social Network consente senza particolari difficoltà di acquisire, da parte di un utente malintenzionato, delle informazioni preziose sui contatti che vengono posti, spesso inconsapevolmente, a fattor comune tra i partecipanti al network.

Un gruppo di utenti condiviso rappresenta una vera miniera d'oro per una persona intenzionata a perpetrare un attacco: è facile trovare nel profilo di un utente le informazioni relative alla sua sfera familiare, al luogo in cui vive, alle sue abitudini, ai suoi gusti personali ed al suo ambiente lavorativo, nonché al suo sistema relazionale. Facendo correlazione tra le informazioni provenienti da più Social Network, incrociate con le tracce indelebili che ogni utente lascia su Internet è possibile, per un attaccante, avere un ritratto preciso dell'individuo bersaglio dell'attacco, che si potrà poi declinare in vari tipi di attacchi (es.: Social Engineering oppure di furto di identità) a seconda della tipologia di risultato che si vuole ottenere e dalle capacità o dalle possibili tecniche che si possono adottare.

### *Il tasto like*

Nel corso degli ultimi anni i Social Network si sono arricchiti di una nuova funzionalità tanto utilizzata e richiesta dagli utenti quanto potenzialmente pericolosa: un tasto che consente di manifestare l'apprezzamento su un post di un utente oppure l'utilità di una risorsa, come un articolo oppure un URL; nel caso di Facebook e LinkedIn il tasto che avvia l'esecuzione del programma si chiama "like", nel caso Google+ è denominato +1, mentre altri Social Media stanno adottando simili meccanismi.

Lo scopo dichiarato di questa funzionalità è stato quello di aumentare l'interazione della comunità degli utenti con il Social Network, permettendo così, al contempo, agli inserzionisti pubblicitari, di proporre delle pubblicità mirate; questo nobile obiettivo non è stato purtroppo accompagnato da un corrispondente sforzo per garantire la privacy dell'utente: utilizzando la funzione like si dà implicitamente il consenso al tracciamento di tutte le interazione dell'utente per un periodo di due anni ad uso del gestore del Social Network.

### *Data leakage*

Come accennato nei paragrafi precedenti, nella maggioranza dei casi, gli utenti dei Social network, siano essi di tipo consumer oppure aziendali non hanno in genere la percezione di quali tipologie di informazioni possano essere pubblicate e di quelle che, se pubblicate, potrebbero arrecare un danno o essere utilizzate come punto di partenza per attacchi di tipo Social Engineering. Nel contesto delle applicazioni web 2.0 contraddistinte da un elevato grado di interattività e da un aggiornamento continuo dei contenuti vengono spesso rese pubbliche informazioni inerenti l'appartenenza ad un team di progetto, la realizzazione di attività, gli spostamenti che si fanno per motivi di lavoro ecc.

La diffusione inconsapevole di informazioni, unita ad altre forme di perdita di controllo delle informazioni (data leakage), può facilitare l'iniziativa un gruppo di attaccanti , mettendoli in una posizione di netto vantaggio rispetto alle vittime potenziali.

La scarsa consapevolezza di questi rischi che si riscontra negli utilizzatori dei Social Media ma anche nelle aziende, insieme alla diffusione esponenziale del fenomeno Social

Media a cui abbiamo assistito in questi ultimi anni, contribuisce ad aumentare i rischi di perdita di controllo sulle informazioni aziendali critiche e sugli asset aziendali.

### *Social Engineering*

Per Social Engineering si intende lo studio del comportamento individuale di una persona al fine di ottenere informazioni utili e confidenziali riguardo la realtà aziendale presso la quale la vittima lavora, questo avviene di solito attraverso l'impersonificazione di un collega o di una persona in possesso delle credenziali necessarie ad accedere alle informazioni richieste. La tecnica del Social Engineering è spesso preferita alle canoniche tecniche di raccolta informazioni perché permette un immediato feedback dei risultati, minori costi e tempi di risposta e minor necessità di competenze specialistiche. La buona riuscita di un attacco di Social Engineering si basa sulla fiducia degli utenti medi e su quanto l'attaccante sia convincente e aderente alla realtà.

### *Cybercrime*

Il fenomeno del Cybercrime, che si basa sull'utilizzo mirato delle tecnologie informatiche per commettere crimini e perpetrare attacchi di tipo terroristico, è in costante aumento come testimoniano alcuni dati statistici tratti dal "Rapporto Clusit 2012 sulla sicurezza ICT in Italia":

- Oggi è possibile acquistare con un solo euro i dati di una carta di credito, con 140 euro una carta di credito contraffatta e con appena 60 euro si possono ottenere le coordinate bancarie.
- Ogni giorno vengono bloccati fino a 600.000 account di Facebook a seguito di vari tentativi di accesso abusivo e nel 2009 oltre 6.700.000 computer sono stati infettati da applicazioni maligne.

A questo vanno poi aggiunte le dichiarazioni rese il 28 marzo scorso da Cecilia Malmstrom, Commissario EU per gli affari interni sul fatto che ogni giorno circa 1 milione di cittadini a livello mondiale è soggetto ad attacchi di tipo informatico: in tale occasione è stata annunciata l'apertura di una struttura dedicata "European Cybercrime Centre" per aiutare i cittadini e le organizzazioni a contrastare questo fenomeno in continua crescita.

### *Sostituzione e furto di identità*

La natura libera e non controllata di Internet, la mancanza di un riscontro sulla effettiva identità di chi apre un profilo sui Social Network ed il fatto che una percentuale significativa della popolazione mondiale non ha gli strumenti per verificare di persona la sua presenza su Internet, sono fattori che consentono ad un malintenzionato di sostituirsi con facilità ad una persona terza. Incrociando le informazioni personali diffuse sui Social con il furto delle credenziali (accessi bancari, numero carte di credito ecc.) disponibili sul mercato nero di Internet è quindi possibile sostituirsi ad una persona fornendo informazioni che risultano del tutto credibili potendo in tutto e per tutto sostituirsi in maniera facile e assolutamente anonima e irrintracciabile.

Oltre a questo occorre citare il fenomeno della creazione dei falsi profili che, per stessa ammissione di Facebook in occasione della sua recente quotazione in borsa, tocca almeno il 10% (ovviamente la fonte aziendale è molto conservativa) sul numero di utenti attivi: questo numero rapportato all'attuale bacino di utenza rappresenta oltre 100.000.000 di persone.

### *Stalking*

I Social Media stanno diventando sempre più un mezzo per veicolare attacchi di tipo personale come il cyber stalking grazie sopratutto alla mancanza di identificazione e alla scarsa consapevolezza dei rischi che il web e i Social Network portano con sé. La creazione di un account su un qualsiasi Social Network, per esempio, può essere fatta da chiunque e senza che ci sia un controllo effettivo del richiedente da parte delle Social Network company. Infatti, sempre più spesso si sente parlare di utenti che, fidandosi di falsi profili, vengono contattati da utenti malintenzionati e che, sfruttando le debolezze della vittima, possono renderli facili vittime di stalking, minacce ed estorsioni.

Tutto ciò può portare a seri rischi ad un'organizzazione se il target dell'attacco è un dipendente o qualcuno che ha accesso a informazioni critiche e che potrà essere poi usato come vettore d'attacco verso l'azienda. Quando il malintenzionato utilizza un Social network di incontri per instaurare una relazione fisica con la vittima e successivamente perpetrare attacchi sfruttando la sua debolezza, si parla di "honey trap".

### *Geolocalizzazione*

L'identificazione della posizione geografica nel mondo reale di un dato oggetto, nota come geolocalizzazione, è una caratteristica che offre molti vantaggi sia per l'utente sia per il provider del servizio. Allo stesso tempo però, esso pone l'utente sotto una serie di pericoli non solo dal punto di vista dello stalking tracciando movimenti ma anche perché conoscere la posizione dei una persona vuol dire anche sapere dove la persona stessa non è (foto e video da posti dove si stanno trascorrendo le vacanze sono utilissime a eventuali ladri, che hanno l'informazione della assenza da casa).

Questi rischi assumono una criticità particolare e sono da valutare con grande attenzione per il coinvolgimento, di fatto inevitabile, anche di minori.

## I rischi

Le caratteristiche dei Social Media che offrono alle aziende le maggiori opportunità e, dunque, esercitano la maggiore attrattiva sono spesso i medesimi elementi che danno luogo ai maggiori rischi tecnologici.

Un approccio strutturato alla gestione dei rischi, richiede innanzitutto una catalogazione dei rischi specifici, derivanti dall'utilizzo dei Social Media.

I rischi individuati dovranno essere poi valutati nel contesto applicativo di riferimento per determinarne l'applicabilità. Il piano di mitigazione dei rischi terrà, infine, conto della propensione al rischio dell'azienda, per quello specifico progetto ed in generale, e di altre valutazioni di contesto, come ad esempio la notorietà del marchio o la tipologia di utenza o l'area geografica: è infatti molto diverso il profilo di rischio di un progetto rivolto ad una utenza interna alla azienda rispetto ad uno dedicato ad una utenza esterna indistinta.

Non si tratta di una attività di natura strettamente tecnologica e, pertanto, le valutazioni dei rischi, della propensione ad accettarli, delle strategie di mitigazione deve coinvolgere tutti gli attori aziendali interessati: la funzione legale, le risorse umane, le relazioni esterne, il management, oltre, naturalmente alle funzioni tecniche e di settore come i sistemi informativi e la sicurezza.

Questo esercizio, effettuato nella fase di impostazione di un progetto Social Media aziendale, può risultare poco costoso ma molto produttivo. Non esaurisce il tema, però.

Come si vede, infatti, in questa sede vengono spesso assunte delle ipotesi sulla base della conoscenza dello strumento e sulle aspettative relative alle reazioni degi destinatari del progetto, per quanto queste informazioni sono disponibili in quel momento.

Durante la vita del progetto sarà necessario verificare periodicamente il perdurare della validità delle ipotesi poste a base della strategia di sicurezza e, se richiesto, procedere ad integrazioni o variazioni. Spesso, soprattutto in questo settore, le reazioni degli utenti sono del tutto differenti da quelle attese, come si evince anche da alcuni esempi di criticità riportati nel seguito.

Come detto, nella valutazione dei rischi, molte sono le considerazioni che derivano dal contesto e dal progetto specifico e queste non possono essere generalizzate.

Come nella classificazione dei Social Media (si veda il capitolo dedicato), il contributo di questo documento consiste nel fornire alcuni criteri di classificazione generale dei rischi in modo che l'analisi di ogni singolo caso si possa confrontare con un quadro generale di riferimento ragionevolmente esaustivo.

I rischi generati dall'utilizzo dei Social Media in azienda sono molteplici ma possono essere classificati secondo i seguenti cluster principali: rischio di conformità, operativo e relazionale.

Riportiamo di seguito, per ciascun cluster, un esempio dei rischi associati.

Tale rappresentazione ha uno scopo esemplificativo e, pertanto, potrebbe non risultare esaustiva con riferimento alle peculiarità di un settore di business e/o di un particolare scenario di utilizzo del Social Media in azienda. Nei capitoli successivi sono riportati esempi di fatti accaduti che corrispondono ad alcuni dei rischi descritti.

### *Rischio di Conformità*

- Trattamento dei dati non conforme alla normativa vigente

  Un trattamento dei dati non conforme alla normativa vigente, ad esempio al d.lgs. 196/03 relativo alla Privacy, potrebbe essere causato dalla diffusione di informazioni personali/sensibili a personale non autorizzato al trattamento dei dati dell'interessato. Analogamente potrebbero essere considerati casi relativi all'applicazione del d.lgs. 231/2001 sulla responsabilità amministrativa d'impresa. Il mancato rispetto della normativa potrebbe dar luogo a potenziali azioni legali, contenziosi e conseguenti sanzioni di carattere penale e/o amministrativo.

- Trattamento dei dati non conforme alle politiche aziendali

  L'introduzione dei Social Media in azienda comporta la necessità di prevedere un processo di conformità rispetto alle politiche/procedure aziendali. Oltre alla possibile redazione di una policy ad-hoc che indirizzi il corretto uso dei Social Media, dovrebbero essere aggiornate, contestualizzandole, le procedure già esistenti in azienda.

  Le policy che richiedono aggiornamento sono, tipicamente, quelle che toccano aspetti particolarmente critici per l'azienda, ad esempio, la documentazione relativa alla compliance esterna, alle attività di marketing, alla proprietà intellettuale, al risk management ed all'area legale.

- Rapporti con dipendenti e candidati

  L'utilizzo dei Social Media, sia da parte del datore di lavoro sia da parte del dipendente, è sempre maggiormente influenzato da tematiche di diritto del lavoro. Le potenziali problematiche interessano le attività di selezione, le pratiche di assunzione, oltre alla gestione di comportamenti scorretti sul posto di lavoro.

  Le risorse umane della società potrebbero, ad esempio, venire a conoscenza di informazioni potenzialmente inappropriate che potrebbero influenzare la decisione riguardo all'assunzione (stato civile, stato di famiglia, condizioni mediche, etc.); potrebbero inoltre verificarsi comportamenti scorretti in ambito lavorativo (ad esempio diffamazione dell'azienda) o personale (ad esempio molestie).

- Commistione tra dati personali e dati aziendali

  L'utilizzo dei Social Media per scopi sia personali sia professionali aumenta il rischio di utilizzare un account aziendale per comunicazioni personali o per esprimere opinioni personali. E' da notare che questo può riguardare comportamenti che prevedano sia il ruolo attivo sia passivo di un dipendente.

  Possibili aggravi possono essere originati dalle condizioni di utilizzo di alcuni Social Network, ad esempio Facebook che permette la creazione di pagine ufficiali per le aziende, richiedendo però l'utilizzo del proprio account personale, aumentando l'esposizione dell'azienda a potenziali rischi reputazionali.

### *Rischio Operativo*

- Diffusione di malware

  I Social Media rappresentano un ulteriore punto di ingresso per possibili rischi legati alla diffusione di software malevolo quale, ad esempio, malware e virus.

  L'infezione su un dispositivo potrebbe estendersi all'intera rete aziendale con conseguenti possibili perdite/furti di informazioni confidenziali e rallentamenti dei sistemi. I dispositivi infetti potrebbero inoltre essere utilizzati come zombie per effettuare ulteriori attacchi verso l'esterno.

- Furto d'identità

  La condivisione di informazioni tra i membri di una stessa community rende possibile ad un malintenzionato di sottrarre informazioni potenzialmente critiche. Sono infatti presenti date di nascita, indirizzi, contatti telefonici e telematici ed una serie di altre informazioni che possono essere utilizzate per commettere furti d'identità ed altri crimini informatici.

  Molti dei metodi di autenticazione attualmente in uso sono basati sulla conoscenza di un'informazione segreta per il recupero delle password in caso queste vengano dimenticate (cognome della madre da nubile, nome dell'animale domestico, etc.): in molti casi queste informazioni sono reperibili da post, fotografie e profili pubblicati sui Social Media. Il furto di un'identità digitale potrebbe essere utilizzato in seguito per ottenere le credenziali aziendali dell'utente e violare poi la rete aziendale.

- Phishing e Social Engineering

  Le tecnologie informatiche sono soggette ad un processo di costante evoluzione e miglioramento dei bug di sicurezza ma gli aspetti non tecnologici possono non essere inclusi in tale processo evolutivo.

  Le tecniche di Social Engineering risultano essere utilizzate sempre più spesso per circuire le persone ed ottenere accesso a privilegi di accesso ed informazioni che dovrebbero invece rimanere riservate.

- Perdita di produttività

  Un utilizzo eccessivo dei Social Media può condurre ad una diminuzione delle performance dell'infrastruttura e ad una diminuzione della produttività. La prolungata durata delle connessioni incrementa inoltre il rischio di esposizione a potenziali software malevoli.

- Perdita di controllo sui contenuti

  La pubblicazione indiscriminata di contenuti sui portali di Social Media potrebbe condurre la società alla perdita dei diritti legali relativi alle informazioni condivise.

  Il rischio maggiore è dovuto alla divulgazione, accidentale o intenzionale, di informazioni aziendali sensibili (piano strategico, piani di acquisizione di competitor, etc.) o di informazioni private sui clienti o altre parti terze interessate, causando così un potenziale svantaggio competitivo.

  Possibili esempi possono essere la formula di un particolare prodotto, il codice sorgente di un software, il progetto di un nuovo prodotto da lanciare sul mercato.

### *Rischio relazionale*

- Danneggiamento del brand (danni all'immagine verso l'esterno)

  Il verificarsi di eventi dannosi può incidere sull'immagine e sulla credibilità dell'azienda nei confronti di clienti, partner e fornitori, comportando, in prospettiva, possibili perdite economiche.

  La società potrebbe essere soggetta ad attacchi di tipo hijacking tramite l'esposizione fraudolenta del brand su portali di Social Media. Potrebbero essere costruite pagine ad-hoc con lo scopo di apportare un danno reputazionale alla società stessa. Un dipendente della società potrebbe, infine, utilizzare il proprio account personale per la comunicazione di informazioni concernenti la sfera lavorativa.

- Danni all'immagine verso l'interno

  Una non corretta gestione dei Social Media o eventuali perdite/alterazione dei dati da parte dell'azienda possono comportare tensioni interne con riflessi negativi indiretti anche sulla produttività del personale e sul possibile aumento delle controversie legali.

- Insoddisfazione dei clienti

  Un passaggio ad un modello di business digitale potrebbe aumentare le aspettative dei clienti. Il mancato raggiungimento del livello di servizio atteso potrebbe comportare un danno d'immagine verso i clienti ed il Social Media stesso potrebbe diventare il canale per una immediata propagazione della criticità.

  Il verificarsi di eventi dannosi potrebbe inoltre determinare un degrado dei servizi offerti alla clientela con conseguenti riflessi negativi sulla capacità dell'azienda di mantenere o migliorare le posizioni di mercato acquisite.

Rispetto a questa catalogazione possono risultare utili alcuni approfondimenti.

### Approfondimento: rischi relazionali dei Social Media

A differenza del rischio reputazionale tradizionale, una gestione efficace del rischio reputazionale derivante dall'utilizzo di Social Media richiede il presidio, il monitoraggio e la misurazione costante di una serie di fonti informative, che altrimenti potrebbero moltiplicare le minacce alla reputazione aziendale e amplificare sia la probabilità che l'impatto del rischio associato.

I rischi relazionali con impatto reputazionale derivanti dai Social Media possono manifestarsi a fronte di:

- Partecipazione attiva dell'azienda in ambito Social Media

  Il rischio in questo caso si configura in relazione a un utilizzo non regolamentato o adeguatamente gestito dei Social Media, in quanto strumenti di comunicazione e di business aziendale. Rientrano in tale categoria tutte le attività di comunicazione effettuate dall'organizzazione o dai suoi rappresentanti, per le quali la mancanza di linee guida, di coordinamento o di processo decisionale possono comportare il manifestarsi di rischi.

- Partecipazione passiva dell'azienda in ambito Social Media

  In questo caso l'organizzazione è inconsapevolmente esposta a rischi di natura relazionale e reputazionale, a seguito di un utilizzo improprio dei Social Media parte di terzi.

Questa considerazione relativa all'uso passivo dei Social Media si aggiunge a quelle già svolte in merito al ROI. Per la loro natura, i Social Media diventano sempre più un'arena comunicativa che tende a coinvolgere l'azienda indipendentemente dalla propria volontà, secondo logiche riconducibili invece alla notorietà del marchio, alla tipologia dei servizi o a particolari criticità o peculiarità del momento storico o organizzativo (delocalizzazioni, licenziamenti oppure, al contrario, grande leadership di mercato).

Rischi e, conseguentemente, costi connessi alla presenza passiva in questa arena tenderanno, pertanto, ad entrare nei rischi e nei costi operativi standard. La decisione di avviare progetti specifici, introdurrà rischi e costi incrementali ma trarrà beneficio dalle iniziative poste in essere per cautelarsi rispetto alla presenza passiva, ottimizzando così i costi già sostenuti.

### Approfondimento: Rischi operativi dei Social Media tramite dispositivi mobili

Come già sottolineato, l'adozione di dispositivi mobili, in ambito business, oltre alla possibilità di diversificare, agevolare, aggiornare e innovare il business, espone

contestualmente l'azienda ad un insieme di nuovi rischi che fino ad ora non doveva considerare.

L'adozione del mobile introduce specifici rischi, specialmente se sui dispositivi vengono trattati dati personali di clienti, dipendenti, partner e fornitori.

La fruizione di Social Media attraverso dispositivi mobili, introduce, di conseguenza, ulteriori rischi specifici.

Ad esempio, una delle principali tecniche di attacco utilizzate sui siti di Social Network ha riguardato l'utilizzo di Url abbreviati, che, in normali circostanze, sono utilizzati per condividere, in una e-mail o su una pagina web, un link a un indirizzo web troppo complesso. Le caratteristiche fisiche del dispositivo mobile tendono a estremizzare l'uso di questa modalità operativa ed a ridurre la propensione e la facilità del controllo.

Uno degli ultimi trend di attacco è sicuramente l'utilizzo dei news feed rss per lanciare attacchi su larga scala: effettuando il login da un falso account e postando un link abbreviato a un sito pericoloso sulla bacheca della vittima. Il Social Network potrebbe distribuire successivamente in automatico il link ai news feed degli amici della vittima, inoltrandolo a centinaia o migliaia di utenti in pochi minuti.

Si tratta, in questo caso, di un rischio che prescinde dalla tipologia di dispositivo, mobile o meno, ma che certo con l'uso di smartphone tende ad aggravarsi.

Abbiamo, inoltre, già introdotto l'acronimo BYOD che individua la tendenza ad utilizzare dispositivi mobili di proprietà del dipendente anche per utilizzi di natura aziendale. Rispetto agli scenari sopra descritti, il BYOD costituisce un moltiplicatore di rischi che impone di rileggere l'intera analisi in riferimento ad alcune sue criticità distintive:

- Il device, non facendo parte degli asset aziendali, è difficilmente governabile e presidiabile con la stessa facilità di un dispositivo di proprietà dell'azienda (sia dal punto di vista tecnico sia burocratico/organizzativo);
- si perde ancora di più il concetto di "perimetro", dando la possibilità ai dati aziendali (siano essi pubblici, sensibili o critici) di essere divulgati senza uno stretto controllo da parte delle figure preposte.

Con riferimento ai cluster identificati per i rischi generati dall'utilizzo dei Social Media in azienda, l'adozione di dispositivi mobili quali supporto per la fruizione dei Social Media, introduce rilevanti aspetti di rischio per quanto riguarda il cluster operativo, in virtù delle caratteristiche intrinseche dei dispositivi stessi e delle peculiari modalità di utilizzo dei media in mobilità. Tra i principali rischi relativi a tale scenario si evidenziano i seguenti:

- Furto o smarrimento del dispositivo

  Il furto o lo smarrimento del dispositivo può portare alla conseguente perdita e/o diffusione di dati aziendali contenuti in esso in assenza di un backup e se non opportunamente cifrati.

- Servizi caratteristici per l'utilizzo dei Social Media via mobile

  Per quanto riguarda la modalità di utilizzo delle app dei Social Network, non bisogna tralasciare il fattore "geolocalizzazione" e "profilazione" che assumono particolare rilevanza in una modalità di fruizione mobile.

- Negazione totale o parziale di servizio

  Un denial of service totale o parziale può essere perpetrato sfruttando le vulnerabilità delle altre app presenti sullo smartphone (es whatsapp) che sfruttando canali di comunicazione e metodi di autenticazione non sicuri possono comportare il blocco del dispositivo.

- Usability vs Security by design

  Il concetto di "Usability vs Security" è sicuramente un fattore chiave parlando di applicazioni mobile. Spesso nella fase di progettazione e sviluppo si tende a ragionare in maniera più accurata sull'usabilità del prodotto che sulle sue caratteristiche di sicurezza, esponendo l'applicazione ed il device a dei rischi relativamente ad attacchi informatici mirati. E' quindi opportuno adottare una strategia di tipo Security by design.

# Contromisure

Una strategia per affrontare i rischi relativi ai Social Media deve concentrarsi, innanzitutto, sugli aspetti organizzativi e di processo, connessi alla gestione della presenza dell'azienda sulle piattaforme Social Media, sia in un ruolo passivo che attivo.

Poi è necessario concentrarsi sul comportamento degli utenti.

L'accesso alle pagine aziendali sui Social Media da parte dei dipendenti, dei collaboratori o dei partner - di tutti quei soggetti, cioè, che sono legati contrattualmente all'azienda e che accedono alla pagina aziendale in virtù di quel rapporto - deve essere regolato da apposite policy, come indicato nei capitoli a questo dedicati e supportate da training per la sensibilizzazione del personale. Naturalmente le policy devono prevedere tutti i diversi casi d'uso rilevanti, in riferimento ai luoghi da cui si accede, ai dispositivi utilizzati ed al ruolo con cui si accede.

La formazione dovrebbe essere effettuata regolarmente e dovrebbe focalizzarsi su benefici, opportunità e potenziali rischi connessi all'utilizzo dei Social Media. Particolare enfasi dovrebbe essere posta sui metodi di Social Engineering, sugli exploit più comuni e sulle minacce alla privacy che presentano i Social Media, in modo di aumentare la consapevolezza dei rischi diffusa in azienda. Questa consapevolezza è, in sé stessa, una contromisura assai importante, soprattutto se si estende anche alle figure apicali dell'organizzazione.

Le relazioni con gli utenti esterni - clienti o potenziali clienti - devono essere considerate senza escludere a priori nessuno scenario tra quelli possibili: a questo scopo la catalogazione dei rischi specifici riportata nel capitolo dedicato, consente di avere un riferimento, seppur molto generale, con cui confrontarsi.

Al fine di mitigare i rischi dovuti all'introduzione dei Social Media in azienda devono inoltre essere sfruttate soluzioni tecnologiche atte a prevenire, individuare ed eventualmente bloccare potenziali incidenti. Le soluzioni implementabili includono, ad esempio, i sistemi di content filtering (per limitare o bloccare particolari accessi) e antivirus (per fornire protezione da malware) ed altre soluzioni per la protezione dei sistemi operativi.

Nella matrice che segue, per ciascuno dei cluster di rischio individuati nel capitolo dedicato al Rischio, sono state individuate possibili contromisure al fine di mitigare i rischi associati.

Sulla base del paradigma individuato dalle leading practice di settore, le contromisure sono state catalogate in tre macrocategorie:

- people (soluzioni di carattere organizzativo);
- process (soluzioni di carattere processuale/procedurale);
- technology (soluzioni di carattere tecnologico).

## Le matrici Rischio / Contromisura

Riassumendo i concetti esposti nei capitoli e nei paragrafi precedenti, è possibile costruire una matrice di correlazione che consenta al lettore di disporre di un quadro sintetico d'insieme.

Nel seguito sono riportate queste matrici suddivise in funzione del cluster di rischio di riferimento per facilitare la lettura.

**TABELLA 4 - MATRICE RISCHIO-CONTROMISURA: CLUSER "RISCHIO CONFORMITÀ"**

| *Matrice di corrispondenza Rischio/Contromisura - Cluster "Rischio di Conformità"* | | | | |
|---|---|---|---|---|
| ***Rischio*** | ***Contromisure*** | ***Categorie contromisure*** | | |
| Trattamento dei dati non conforme alla normativa | Definizione di ruoli e responsabilità per la gestione della privacy | PEOPLE | PROCESS | |
| | Stabilire appropriate politiche, processi e tecnologie atte a garantire la protezione dei dati personali | PEOPLE | PROCESS | TECHNOLOGY |
| Trattamento dei dati non conforme alle politiche aziendali | Definizione di un'apposita social media policy, che disciplini chiaramente gli ambiti di applicazione e le potenziali azioni disciplinari | PEOPLE | PROCESS | |
| | Implementazione di un sistema per il monitoraggio e l'individuazione di azioni non conformi alle policy aziendali | | | TECHNOLOGY |
| | Conduzione di un programma formativo per la sensibilizzazione del personale | PEOPLE | | |
| Rapporti con dipendenti e candidati | Definizione di un'apposita social media policy, che disciplini chiaramente gli ambiti di applicazione e le potenziali azioni disciplinari | PEOPLE | PROCESS | |
| | Creazione di un processo congiunto con la funzione Legale per la continua interpretazione della disciplina del lavoro | PEOPLE | PROCESS | |
| | Revisione delle coperture assicurative concernenti la responsabilità civile, al fine di assicurarsi la copertura finanziaria in caso di citazioni in giudizio | PEOPLE | PROCESS | |
| Commistione tra dati personali e dati aziendali | Differenziare l'account personale da quello aziendale (ad esempio, le notifiche legate ad un account aziendale dovrebbero essere inoltrate ad un indirizzo di posta elettronica aziendale, ipotizzare un messaggio/disclaimer sui messaggi personali in cui si dichiari che il messaggio in questione non riflette la posizione dell'azienda) | PEOPLE | PROCESS | |
| | Sensibilizzare i dipendenti ad utilizzare una prassi corretta:<br>• utilizzare gli account aziendali solamente sul posto di lavoro e solamente utilizzando risorse aziendali<br>• redigere i messaggi su un elaboratore di testi, in modo da poterlo valutare attentamente prima di pubblicarlo su portali di social media | PEOPLE | | |
| | Limitazione dell'accesso ai siti di social media ai soli dipendenti con una condivisa ed approvata necessità a fini lavorativi | | | TECHNOLOGY |

**TABELLA 5 - MATRICE RISCHIO-CONTROMISURA: CLUSTER "RISCHIO OPERATIVO".**

| *Matrice di corrispondenza Rischio/Contromisura - Cluster "Rischio Operativo"* | | | | |
|---|---|---|---|---|
| ***Rischio*** | ***Contromisure*** | ***Categorie contromisure*** | | |
| Diffusione di malware | Implementazione di sistemi antivirus/antimalware ed aggiornamento degli stessi | | PROCESS | TECHNOLOGY |
| | Utilizzo di tecnologie di content filtering | | | TECHNOLOGY |
| | Sistemi di monitoraggio (es. MDM) installati sui device mobili | | | TECHNOLOGY |
| | Utilizzare tecniche di full disk encryption al fine di proteggere l'accesso ai solo utenti autorizzati | | | TECHNOLOGY |
| | Aggiornamento delle policy esistenti e/o definizione di policy specifiche | | PROCESS | |
| | Conduzione di campagne di sensibilizzazione verso i dipendenti | PEOPLE | | |
| Furto d'identità | Restringere gli accessi alle proprie pagine a gruppi di persone selezionati | PEOPLE | | |
| | Non pubblicare indiscriminatamente informazioni personali sui Social Media | PEOPLE | | |
| | Utilizzo di sistemi anti-phishing | | | TECHNOLOGY |
| | Definire una chiara politica per la gestione delle password, che sensibilizzi i dipendenti all'utilizzo di password complesse | PEOPLE | PROCESS | |
| | Implementazione di tecniche di autenticazione multi-factor | | | TECHNOLOGY |
| Social Engineering | Conduzione di corsi di formazione specifici: una formazione adeguata dovrebbe comprendere aspetti di sicurezza e di conformità alle policy aziendali | PEOPLE | PROCESS | |
| | Implementazione di tecniche di autenticazione multi-factor | | | TECHNOLOGY |
| | Implementazione di una soluzione DLP (Data Loss Prevention) sul traffic web al fine di bloccare la diffusione di informazioni classificate come critiche | | | TECHNOLOGY |
| Perdita di produttività | Definizione di un'apposita social media policy, che disciplini chiaramente gli ambiti di applicazione e le potenziali azioni disciplinari | PEOPLE | PROCESS | |
| | Monitoraggio dell'utilizzo dei social media | | | TECHNOLOGY |
| | Identificare un limite alla capacità di banda per le connessioni dirette verso i social media | | | TECHNOLOGY |
| Perdita di controllo sui contenuti | Revisione, da parte delle funzioni Legale e Comunicazione, degli user agreement specifici per i Social Media | PEOPLE | PROCESS | |
| | Stabilire policy che definiscano chiaramente quali informazioni possono essere pubblicate | PEOPLE | PROCESS | |
| | Implementazione di una soluzione DLP (Data Loss Prevention) sul traffic web al fine di bloccare la diffusione di informazioni classificate come critiche | | | TECHNOLOGY |
| | Implementazione di un sistema per il log delle comunicazioni avvenute | | | TECHNOLOGY |

**TABELLA 6 - MATRICE RISCHIO/CONTROMISURA: CLUSTER "RISCHIO RELAZIONALE"**

| *Matrice di corrispondenza Rischio/Contromisura - Cluster "Rischio Relazionale"* | | | | |
|---|---|---|---|---|
| ***Rischio*** | ***Rischio*** | ***Categoria contromisura*** | | |
| Danneggiamento del brand (danni all'immagine verso l'esterno) | Verifica, anche mediante l'utilizzo di società esterne, degli utilizzi impropri del brand aziendale | PEOPLE | PROCESS | |
| | Divulgazione di informative periodiche per rendere consapevoli i clienti di potenziali frodi | PEOPLE | | |
| | Definire chiare linee guida riguardo alla tipologia di informazioni che possono essere divulgate | PEOPLE | PROCESS | |
| | Utilizzare tool specifici per il monitoraggio del brand sui social media (piattaforme di Online Reputation Management). | | | TECHNOLOGY |
| | Definire un piano di gestione della crisi che definisca il processo di escalation nel caso di danni all'immagine aziendale | | PROCESS | |
| Danni all'immagine verso l'interno | Definizione di un'apposita social media policy, che disciplini chiaramente gli ambiti di applicazione e le potenziali azioni disciplinari | PEOPLE | PROCESS | |
| | Utilizzare tool specifici per il monitoraggio del brand sui social media (piattaforme di Online Reputation Management). | | | TECHNOLOGY |
| | Definire un piano di gestione della crisi che definisca il processo di escalation nel caso di danni all'immagine aziendale | | PROCESS | |
| Insoddisfazione dei clienti | Assicurarsi che la struttura individuata e le tecnologie a supporto siano adeguati per gestire la quantità di traffico generata dalla presenza sui Social Media | PEOPLE | | TECHNOLOGY |
| | Garantire una comunicazione trasparente coi clienti | PEOPLE | | |

# Aspetti legali

L'utilizzo dei Social Media in ambito aziendale ha molteplici implicazioni sotto il profilo giuridico, legate in parte al rapporto tra l'azienda e gli utenti dei profili Social ed in parte al rapporto tra l'azienda stessa e i propri dipendenti e collaboratori.

Tale complessità è potenzialmente pericolosa nella misura in cui le aziende che usano questi nuovi strumenti non sono sempre pienamente consapevoli di tali profili e dell'esistenza delle leggi che governano le attività intraprese nel Web: questo può portare a commettere errori, a volte gravi, che potrebbero essere opportunamente evitati.

Il problema dell'adattamento e della complessità delle leggi esistenti e talvolta la loro in appropriatezza per il perseguimento di obiettivi di protezione e tutela degli interessi in gioco non è un problema solo italiano: è un problema globale, acuito dal contrasto tra la velocità con cui evolvono i servizi del c.d. "Web 2.0" e la lentezza con cui mutano le norme vigenti e l'eterogeneità dei sistemi normativi.

In questo contesto, quindi, la differenza tra una presenza, efficace o meno, in Rete è legata anche alla consapevolezza degli aspetti giuridici (per definire la differenza di sensibilità tra i diversi attori, si può parlare di "*legal divide*").

Basti pensare, che secondo un'indagine di Symantec[1], in USA nel corso del 2011, soltanto la diffusione di notizie riservate attraverso i Social Media ha causato alle imprese danni per circa 4 milioni di dollari.

Si tratta, quindi, di temi di centrale importanza per il futuro sviluppo nell'uso degli strumenti del Web sociale, perché le aziende - seppure attratte dai benefici - potrebbero essere frenate dalle preoccupazioni relative ai rischi in termini di reputazione e contenzioso; nelle aule giudiziarie, infatti, ci si occupa con sempre maggiore frequenza (e consapevolezza) della Rete e dei Social Media.

Tuttavia, non si può lasciare che la complessità degli argomenti e dei diversi riferimenti legislativi, interpretati non sempre in modo evoluto dai Tribunali, scoraggi e stronchi le strategie aziendali.

Nonostante la gran parte delle norme applicabili al Web sociale siano precedenti al fenomeno dei Social Media, attraverso le opportune interpretazioni è possibile evitare una serie di comportamenti - assai diffusi in ambito aziendale - che sono scorretti e potrebbero comportare l'applicazione di ingenti sanzioni economiche oltre al divieto di proseguire la specifica attività che si era intrapresa.

Per questo motivo, appare utile evidenziare le disposizioni maggiormente rilevanti in materia di uso dei Social Media in ambito aziendale.

## Le norme rilevanti

Nel caso in cui un'azienda decida di fare ricorso agli strumenti del Web sociale, dovrà necessariamente tenere nella giusta considerazione alcuni atti normativi per assicurare correttezza e legittimità alla propria presenza sui Social Network.

Di seguito, riassumendo, sono indicati i principali provvedimenti normativi rilevanti cui si farà riferimento nel seguito.

**TABELLA 7 – RIFERIMENTI NORMATIVI RILEVANTI**

| Norma Rilevante | Descrizione |
|---|---|
| Costituzione della Repubblica italiana - in particolare articoli: 21, 41 | Libertà di manifestazione del pensiero e libertà di iniziativa economica privata. |
| Legge n. 633/1941 - Legge a protezione del diritto d'autore e di altri diritti connessi al suo esercizio | Copyright, Diritto d'autore, Titolarità dei contenuti e dei dati |
| D. Lgs. n. 196/2003 - Codice in materia di protezione dei dati personali | Privacy, Sicurezza |
| Legge n. 300/1970 - in particolare articoli: 1, 4, 8 | Controllo del lavoratore, Opinioni del lavoratore |
| D. Lgs. n. 231/2001 - Responsabilità amministrativa degli Enti | Delitti informatici e trattamento illecito di dati, Reati societari, Violazioni diritto d'autore |
| Codice civile | Reati societari, Responsabilità civile, Danno |
| Codice penale - in particolare articoli: 494, 595, ... | Diffamazione, Sostituzione di persona, ... |

Ricollegandoci ora ai temi trattati nel capitolo precedente e, cioè, ai rischi connessi all'utilizzo di Social Media, la tabella che segue mette in relazione i principali rischi individuati con le normative rilevanti in relazione ad essi. Le norme sono raggruppate sotto titoli ampi per semplicità di rappresentazione.

**TABELLA 8 - MATRICE DI CORRELAZIONE COMPORTAMENTI-IMPATTI LEGALI**

| Matrice, comportamenti/ impatti legali | | | | | | |
|---|---|---|---|---|---|---|
| **Rischio / comportamento illecito** | **D. Lgs. 231 del 2001** | **D. Lgs.196 del 2003** | **Reati informatici (profilo penalistico)** | **Norme a tutela della Proprietà immateriale (proprietà industriale e proprietà intel.)** | **Statuto dei lavoratori (legge 300/1970)** | **Responsabilità civile** |
| Trattamento dei dati non conforme alla normativa | ▪ | ▪ | ▪ | | | ▪ |
| Trattamento dei dati non conforme alle politiche aziendali | | | | ▪ | ▪ | ▪ |
| Diffusione di Malware | | | ▪ | | | ▪ |
| Furto d'identità | | ▪ | ▪ | | | ▪ |
| Social Engineering | | ▪ | ▪ | | | ▪ |
| Perdita di controllo sui contenuti | | | | ▪ | | ▪ |
| Danneggiamento del brand, danni all'immagine aziendale | | | | ▪ | ▪ | ▪ |

Tra i profili giuridici maggiormente rilevanti in materia di Social Media è opportuno segnalare e approfondire i seguenti:

## *A. LIBERTA' DI MANIFESTAZIONE DEL PENSIERO*

I Social Media rappresentano, innanzitutto, un potentissimo strumento per esprimere e far circolare idee, opinioni e messaggi di ogni genere (non solo di ordine personale, ma anche, ad esempio, di tipo promozionale e politico). Sotto questo profilo, viene innanzitutto in rilievo la libertà di manifestazione del pensiero che ha ricevuto garanzia costituzionale nell'art. 21 della Costituzione; tale norma sancisce che:

«*Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione.*»

Il dettato costituzionale coniuga insieme il diritto di esprimersi liberamente ("di manifestare liberamente il proprio pensiero") e il diritto di utilizzare ogni mezzo allo scopo di portare l'espressione del pensiero a conoscenza del massimo numero di persone ("con la parola, lo scritto e ogni altro mezzo di diffusione").

Pur non esistendo dubbi riguardo al fatto che la libertà di manifestazione del pensiero faccia parte delle libertà fondamentali dell'individuo, è corretto per la generalità dei cittadini che questa libertà abbia dei limiti. Questi sono posti dalla legge e devono trovare fondamento in precetti e principi costituzionali siano essi espressamente dichiarati ovvero implicitamente riconducibili alla Carta costituzionale (ad esempio, la sicurezza pubblica o l'altrui reputazione).

Il rischio che gli utenti eccedano nell'esercizio di questa libertà utilizzando i Social Media è acuito dal fatto che, spesso, l'utilizzo del Web 2.0 è percepito come un ambiente privato (si accede a Internet in solitudine e sulle bacheche ci sono gli "amici" dell'utente): ciò tende a nascondere o fare passare in secondo piano la dimensione assolutamente pubblica delle azioni intraprese (ad es. in caso di diffamazione).

Nell'ambito dell'uso aziendale dei Social Media, vengono in rilievo tre profili:

- il primo, relativo al rapporto tra le aziende e i gestori dei Social Network Site (si pensi, ad esempio, alla pubblicazione di immagini relative ad una campagna pubblicitaria che vengano cancellate dal *provider* in quanto ritenuti contrari alla pubblica morale);
- il secondo, relativo al rapporto tra le aziende e gli utenti dei servizi Social (come nel caso della moderazione e/o cancellazione di un commento);
- il terzo, relativo all'uso fatto dai dipendenti e collaboratori dell'azienda (sia con riferimento all'attività posta in essere attraverso i loro profili personali, sia con riguardo all'uso dei profili aziendali).

## *B. TUTELA DEI LAVORATORI*

La serie di apparati tecnologici che in questo momento sono in dotazione di ciascun individuo che lavora nel terziario (ma non solo) in un Paese occidentale include numerosi *device* informatici (*netbook, smartphone, tablet*).

Si tratta di strumenti dall'uso promiscuo: mentre il *personal computer* negli anni '80 era, sostanzialmente, una macchina da ufficio, adesso questi strumenti consentono alle persone di potersi connettere e lavorare anche lontano dall'ufficio; numerose indagini dimostrano, poi, che tra le applicazioni più utilizzate dai lavoratori ci sono proprio quelle del Web sociale.

Questi stessi siti vengono utilizzati dalle aziende per il conseguimento di una più efficace organizzazione (ad es. per *recruiting*), oltre che per il perseguimento diretto di finalità di *business*.

In proposito, va rilevato che il controllo dell'azienda dell'attività svolta sui Social Media dal dipendente è un tema delicato, in relazione al quale deve essere sempre assicurata la conformità allo Statuto dei lavoratori (Legge n. 300/1970).

In particolare, l'art. 8 della legge n. 300/70 pone il divieto generale di compiere qualunque indagine sulle opinioni del lavoratore, vale a dire su tutte quelle informazioni che non riguardino direttamente le sue competenze e la sua professionalità (es.: opinioni politiche, religiose o sindacali). Tale norma rappresenta il baluardo a protezione di qualunque ingerenza datoriale rispetto alla sfera privata del lavoratore, sanzionando aspramente ogni condotta discriminatoria, ed è una disposizione che non può essere derogata neppure da una espressa dichiarazione di volontà del lavoratore.

Dal momento che tale disposizione non è stata dettata con specifico riferimento ai Social Media ci si chiede quale tipo di uso il datore di lavoro possa fare delle informazioni ivi pubblicate. In proposito, è orientamento diffuso considerare lecito, ad esempio, ricercare i profili dei candidati nei Social Network professionali, dovendo invece il datore astenersi, nel rispetto dell'art. 8, dal verificare informazioni personali attraverso i Social considerati di natura ludica dalla coscienza collettiva (anche questo aspetto, però, è discusso se ci si trova in presenza di informazioni del lavoratore di pubblico dominio).

Nell'ambito, invece, del rapporto di lavoro, il datore può disciplinare l'utilizzo dei Social Network che non siano ritenuti necessari per l'esecuzione della prestazione lavorativa. La regolamentazione può arrivare anche alla predisposizione di appositi filtri che impediscano l'accesso ai siti "vietati" tramite i PC aziendali, senza poter però mai imporre dei controlli a distanza delle attività di navigazione dei dipendenti, come espressamente vietato dall'art. 4 dallo Statuto dei lavoratori.

L'uso eccessivo o la violazione del divieto di accesso ai Social Network con strumenti di proprietà dell'azienda può, poi, validamente costituire la ragione fondante l'irrogazione di sanzioni disciplinari o, addirittura, di licenziamento per giusta causa.

Da qualche tempo a questa parte, però, in molte realtà si sta facendo largo la consapevolezza delle potenzialità degli strumenti di comunicazione come i Social Media, anche nell'ottica di visibilità, diffusione e promozione del marchio. Conseguentemente sta crescendo il numero di realtà produttive che regolamentano l'uso di questi canali tramite Codici di condotta (c.d. "Social Media Policy"), evitando così il loro generico divieto e rendendo chiari ai lavoratori i loro diritti.

### *C. RESPONSABILITÀ DELL'AZIENDA*

L'utilizzo dei canali Social può comportare una serie di responsabilità da parte delle aziende, principalmente con riferimento ai contenuti caricati sulla piattaforma (immagini, foto, video, brani musicali, ecc.).

Chi usa un Social Network site deve avere piena consapevolezza delle problematiche che questi strumenti implicano: innanzitutto bisogna verificare che tutti i contenuti pubblicati sui canali Social non ledano i diritti d'autore o di proprietà intellettuale di terzi soggetti (comportamento che potrebbe esporre l'azienda a contenzioso e a risarcimenti molto onerosi). In secondo luogo, sarà necessario fare attenzione a non porre in essere comportamenti che possano essere qualificati come concorrenza sleale, come l'adozione di nomi utente e/o tag che possano avere potenziale effetto confusorio rispetto ai prodotti e ai servizi di aziende concorrenti.

Con riferimento alla responsabilità dell'azienda, viene altresì in rilievo la disciplina sulla responsabilità amministrativa delle persone giuridiche dettata dal D. Lgs. n. 231/2001 per i reati commessi nell'interesse dell'azienda stessa.

Come noto, la responsabilità che può essere contestata alla persona giuridica è una responsabilità che trae origine dalla mancanza di idonei controlli gestionali che avrebbero potuto evitare il compimento dei reati. Appare quindi opportuno che, nell'ambito di tale attività organizzativa e di controllo, le aziende tengano in particolare evidenza le fattispecie di reato che possono essere poste in essere per il tramite dei Social Media, come reati societari (come quelli previsti agli artt. 2621 ss Codice civile) e crimini informatici (come quelli introdotti nel Codice penale dalla Legge n. 547/1993).

In tale ottica, assume particolare importanza l'adozione della Social Media Policy aziendale di cui si è fatto cenno e su cui si ritornerà in seguito.

### *D. RISERVATEZZA DEI DATI DEGLI UTENTI*

Il dato personale di un utente di un servizio Web è sempre più utilizzato per misurare il gradimento del servizio stesso, dei prodotti (specie se digitali), dei marchi, delle iniziative, dei contenuti, dei personaggi. Nel caso dei Social Media, questo profilo assume ancora maggiore rilevanza.

Infatti, attraverso l'analisi del dato comportamentale degli utenti di questi siti è possibile capire meglio quali sono i loro bisogni e orientare i servizi verso una maggiore soddisfazione: i profili di un Social Network qualsiasi forniscono informazioni organizzate in modo tale da permettere un'analisi statistica e demografica senza necessità di chiedere ulteriori informazioni.

Chi utilizza Social Network, inoltre, usa il vero nome (79%), foto (51%), nazionalità (47%) e risulta che appena il 58% degli utenti legga l'informativa privacy fornita dai Social Networks e solo il 70% di questi adotti comportamenti ad essa conseguenti.

I dati di un profilo di un qualsiasi Social sono organizzati attraverso elementi identificativi (nome, cognome, sesso, data di nascita, luogo di provenienza, titolo di studi, stato civile, relazioni di parentela, ore passate a giocare, ecc) che permettono la loro agevole estrazione in un database e, di conseguenza, la loro analisi e il loro successivo uso per finalità promozionali.

Con riferimento all'uso aziendale, appare opportuno sottolineare come la recente modifica del D. Lgs. n. 196/2003 operata dal Decreto legge 6 dicembre 2011 (convertito con modificazioni dalla Legge n. 214 del 22 dicembre 2011) abbia escluso dall'applicazione del Codice Privacy i dati riferiti a persone giuridiche, enti e associazioni.

Di conseguenza, il principale ambito relativo alla riservatezza è relativo ai dati degli utenti che utilizzano i profili Social dell'azienda. Con riferimento a questo aspetto, deve essere sempre garantita la conformità con quanto previsto dal codice in materia di protezione dei dati personali (D. Lgs. n. 196/2003).

La disciplina in materia di privacy riconosce al cittadino il potere contrattuale di gestire i propri dati decidendo a chi conferirli.

Rivestirà centrale importanza, quindi, la predisposizione di un'apposita informativa ai sensi dell'art. 13 D. Lgs. n. 196/2003 che - per comodità (e visto lo scarso spazio reso disponibile su alcune piattaforme Social*)* - potrebbe essere raccomandabile inserire, in posizione di facile accessibilità, all'interno del sito aziendale.

Tale informativa non rappresenta una duplicazione rispetto alla policy già predisposta dal titolare del Social Network site, ma deve coprire i profili relativi all'uso che l'azienda può fare dei dati dei propri utenti a seguito dell'interazione con i profili Social (specialmente in materia di invio di comunicazioni commerciali). Dovranno essere resi chiaramente evidenti i diritti dell'art. 7 D. Lgs. n. 196/2003. Tali diritti, cuore del potere di controllo che l'interessato ha sui propri dati anche una volta che questi sono stati conferiti, devono essere sempre riportati, in modo che anche qualora l'interessato li ignori, possa avere contezza della loro esistenza; si renderà opportuno indicare, poi, anche i recapiti (sia email che tradizionali) del responsabile del trattamento a cui gli utenti possono rivolgersi.

## I termini di servizio

Se è vero che, nella gran parte dei casi, l'iscrizione a un sito di Social Networking è gratuita, è anche vero che la registrazione di un profilo comporta la conclusione di un vero e proprio contratto a oggetto informatico (il cosiddetto contratto di Social Networking) e quindi - oltre alle innanzi citate questioni relative alla *compliance* con la normativa vigente - si pongono una serie di rilevanti profili di tipo contrattuale.

Innanzitutto, la decisione relativa all'iscrizione dell'azienda ai servizi Social deve essere presa (o quantomeno autorizzata) da un soggetto che, in base alla legge e agli atti societari ne abbia effettivo mandato; a prescindere da ciò, a seconda della realtà aziendale di riferimento, la scelta di aprire un profilo sui Social Media dovrà essere opportunamente condivisa con tutti gli uffici interessati (ad esempio, personale, marketing, legale, ecc.).

Tale autorizzazione è ancor più necessaria se si pensa che, di norma, l'utente dei siti di Social *networking* non ha la possibilità di influire sui contenuti del contratto (proponendo clausole o ottenendo la modifica di quelle già predisposte), potendo soltanto scegliere se

aderire o meno al servizio. Assume grande importanza la lettura dei termini di servizio (in inglese *Terms of Service* o *TOS*) che devono essere accettati dall'utente prima di poter accedere ai servizi di Social Media e, quindi, prima della creazione del profilo.

Tali condizioni, che è opportuno conservare al pari di qualunque altro contratto, si occupano di:

- riservatezza dei dati degli utenti (*privacy policy*);
- condotte consentite all'utente;
- diritti sui contenuti inseriti dagli utenti;
- limitazioni di responsabilità del fornitore.

Tra gli aspetti maggiormente rilevanti rientrano quelli legati alla riservatezza degli utenti e ai contenuti veicolati attraverso i canali sociali. Con riferimento al primo aspetto, deve essere sempre garantita la conformità con quanto previsto dal codice in materia di protezione dei dati personali (D. Lgs. n. 196/2003); invece, in relazione ai diritti d'autore e di proprietà intellettuale che l'azienda può vantare su alcuni dei contenuti pubblicati, si deve tenere conto che alcuni *provider* nei propri modelli contrattuali prevedono che l'utente trasferisca al fornitore il diritto di utilizzare, anche a fini commerciali, il materiale ospitato sui propri server.

Inoltre, bisognerà prestare attenzione al tipo di comportamenti vietati dal gestore del Social Network che potrebbero comportare la cancellazione del profilo o dell'account dell'azienda e alla circostanza che tutti i contenuti pubblicati sui canali Social non possano ledere i diritti d'autore o di proprietà intellettuale di terzi soggetti; tale comportamento potrebbe vanificare gli investimenti effettuati, oltre danneggiarne l'immagine ed esporla a contenzioso).

Inoltre, dal momento che i termini di servizio sono soggetti a frequente revisione e modifica da parte dei fornitori del servizio stesso, è opportuno monitorarne l'evoluzione in modo da valutare, volta per volta, se le modifiche possano essere accettate oppure l'azienda debba abbandonare il Social Network.

### Forme di tutela e raccomandazioni legali

L'uso dei Social Network è destinato ad incidere su alcuni processi dell'azienda, a prescindere dal fatto che questa abbia o meno intenzione di elaborare e seguire una strategia basata su di essi.

Il personale (dirigenti, dipendenti, stagisti e collaboratori in genere) di un'azienda usa, infatti, i Social Network, a prescindere dal fatto che siano state adottate: linee guida, policy o qualsiasi altra norma idonea a regolamentare tale ambito.

Atteso che i diversi modi per "offendere" attraverso i Social Network sono stati analizzati nei precedenti capitoli, è utile cercare di riprendere le diverse tipologie di offese, esse possono essere legate a:

- utilizzo indebito/distorto del brand aziendale;
- affermazioni e caricamento immagini contrarie ai principi dell'azienda (principi espressi, ad esempio, attraverso un codice etico come quello previsto dal dlgs 231 del 2001);
- dichiarazioni che turbano il comportamento degli stakeholder;
- comunicazioni che turbano il mercato azionario;

Dalla varietà di comportamenti da controllare e dagli impatti visti nel quadro normativo delineato (sto supponendo che di questo ne parli il primo capitolo *legal*) emerge in tutta chiarezza che non esiste una "ricetta" per eliminare ciascuno di essi, bensì esistono uno o più strumenti per affrontare il fenomeno nel modo più ampio possibile.

In questa situazione sembra coerente pensare di suggerire un approccio proattivo, al fine di evitare spiacevoli sorprese costituite, ad esempio, dalla episodi denigratori o altro, l'utente dovrà innanzitutto:

- interrogarsi sul ruolo attuale e potenziale dei Social Network per l'azienda/ente, in relazione a prodotto/settore merceologico/attività svolta (sia essa a scopo di lucro o meno) e ai canali di comunicazione che ritiene di promuovere, nel breve e nel medio termine.
- valutare quale impatto possano avere affermazioni fatte sui Social Network da parte del proprio personale;
- redigere la "documentazione" (codice etico, linee guida, policies, …) adatte al profilo emerso dagli step precedenti cercando di regolamentare comportamenti e dichiarazioni lesive per l'immagine dell'ente;
    - strutturare una policy rispondente agli elementi precedentemente accertati cercando di regolamentare comportamenti e dichiarazioni lesive per l'immagine dell'ente;
    - attribuire delle linee guida comportamentali, che si rivolgano: sia ai ruoli abilitati ad esprimere l'opinione dell'ente sia a coloro che non siano abilitati; queste linee guida dovranno andare dal generale (attenendosi ad un codice etico) al particolare (non parlare di nuovi prodotti in corso di realizzazione, non esprimere il proprio parere sulle sorti delle strategie poste in essere dall'azienda, …);
    - introdurre una "classificazione delle informazioni" per lo meno per quelle che meritano una specifica tutela, ad esempio apponendo una scritta accompagnata da un colore preciso che dia immediata evidenza (e faciliti la memorizzazione) dell'ambito di diffusione dell'informazione.

Naturalmente quelli elencati sono solo alcuni dei molti rimedi/strategie che è utile porre in essere quando si tratta di limitare la diffusione di notizie ovvero impedire, per quanto possibile, che la vita privata del singolo incida negativamente sull'immagine dell'ente per cui lavora.

Di seguito si è provato a dare un'idea di questo processo, a mezzo di un diagramma di flusso.

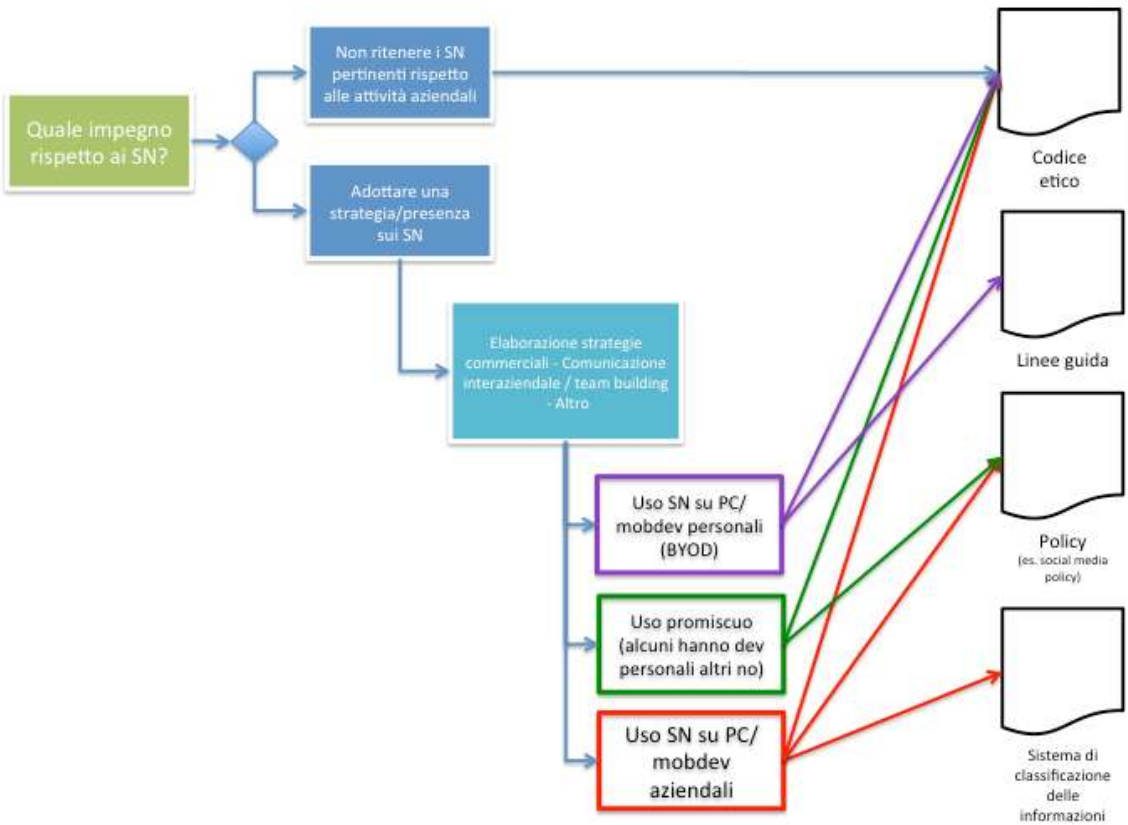


FIGURA 9 – PROCESSO DI ADOZIONE DI UNA STREGIA SOCIAL

Altro elemento da non sottovalutare riguarda gli aspetti legati alla gestione dell'identità di chi accede/rilascia dichiarazioni sui Social Network. Tanto più che, se per individuare un destinatario di una policy aziendale occorre avere la ragionevole conferma della sua identità, per infliggergli una sanzione disciplinare, occorre avere l'assoluta certezza della sua identità.

Se la conferma dell'identità può essere relativamente semplice (almeno sul piano teorico) in presenza di account aziendali, lo stesso non può dirsi per account "personali" per i quali la condotta può essere attribuita a familiari/conviventi (certamente non vincolati al rispetto delle procedure aziendali).

Inoltre il problema dell'identità si ripropone in molteplici situazioni, in particolare, nel caso di attacchi diretti dall'esterno verso l'interno, ad esempio nel caso di "flame".

### *Gestione dei flame*

Parlando di utenti dei Social Network ma anche dello specifico argomento dei "flame" (un messaggio deliberatamente ostile e provocatorio inviato da un utente alla comunità o a un altro individuo specifico) che possono provenire dalle fonti più diverse, bisogna evidenziare che opporsi ad un "flame" non è la stessa cosa che arginare o contestare un'affermazione fatta "in presenza fisica" da un concorrente o da un giornalista malizioso.

Occorre accertare l'identità di chi si esprime e valutare se l'affermazione fatta rientra in un qualche profilo di responsabilità, in quanto essa può integrare una fattispecie penalmente rilevante (ingiuria, diffamazione, …), integrare le fattispecie lesive della normativa sul trattamento dei dati personali, oppure un reato presupposto di cui al d.lgs. 231 del 2001.

A proposito del d.lgs. 231 del 2001, non sfugga che il flame può essere posto in essere per commettere, ad esempio, il reato di "aggiotaggio" attribuendo ad un blogger o comunque ad un terzo un'informazione che, in realtà è stata diffusa da uno dei soggetti ex artt. 6 e 7 del d.lgs 231 del 2001 allo scopo di ottenere oltre ad un interesse personale, anche un "interesse o vantaggio" per l'ente.

Questo ci porta a considerare che il modello "organizzativo-gestionale" debba introdurre, tra le procedure e le misure da adottare per ridurre il rischio di commissione di reati presupposto, il riferimento agli adempimenti indicati nel presente capitolo.

Tuttavia, una delle principali innovazioni quando si tratta a proposito di Social Network è rappresentata dalla constatazione che gli strumenti, anche quelli di tutela, si devono evolvere per stare al passo con le loro dinamiche.

Tra le regole principali per gestire la "Social Media Reputation" si annoverano due "tips" che sono utili anche nell'ambito di tutela di cui si tratta nel presente capitolo:

- monitorare le conversazioni che riguardano l'azienda per prevenire le situazioni di "malcontento";
- gestire le risposte a fronte di una situazione di malcontento.

Questo approccio consentirà di diminuire e, in molti casi, azzerare l'impatto dei c.d. "flame": rispondendo ai dubbi e alle contestazioni, rimuovendo le dichiarazioni diffamatorie oppure smorzandole, estromettendo i *troll* (in questa sede, per troll, si intende la definizione che di esso dà wikipedia: una persona che interagisce con gli altri utenti tramite messaggi provocatori, irritanti, fuori tema o semplicemente senza senso, con l'obiettivo di disturbare la comunicazione e fomentare gli animi) e i disturbatori, dai gruppi strutturati per promuovere il business.

Questo ci porta a considerare che la tutela dell'azienda deve essere giocata su molti campi dei quali quello "giudiziale" rappresenta, spesso, il minoritario e il meno efficace.

### *Regole di disclosure*

In presenza di organizzazioni complesse la “vincolatività” delle procedure deve essere rafforzata dalla classificazione dei contenuti trattati dagli operatori, in modo che ciascuno sia in grado di conoscere l’ambito di diffusione delle informazioni trattate.

La differenza tra controllare la diffusione delle informazioni quando già circolano oppure quando vengono generate è di immediata percezione.

La seconda modalità facilita il mantenimento del controllo e risulta più efficace nel momento in cui occorre adottare una determinata linea comunicativa ovvero compartimentare la diffusione di informazioni che riguardano l’azienda, inoltre una “classificazione delle informazioni” strutturata, è opponibile al personale che non l’abbia rispettata.

La forza di un’efficace modalità di classificazione è esponenzialmente incrementata in presenza di una chiara procedura e di precise istruzioni su come applicarla. Il quadro deve essere completato da una serie di accordi di riservatezza verso coloro che accedono alle informazioni aziendali, specie quando si tratta di consulenti e collaboratori esterni.

### *Aggiornamento periodico*

La velocità dei mutamenti e l’eterogeneità dei Social Network (in genere le strategie di Social Networking ne ricomprendono molteplici: Twitter, Facebook, Foursquare, LinkedIn, …), impone un’assidua osservazione delle policy, dei contratti e, a cascata, delle linee guida aziendali che su di essi possono essere strutturate. Occorre istituire una sorta di osservatorio, che si può immaginare “condiviso” tra più entità, che verifichi periodicamente l’evoluzione delle regole contrattuali dei diversi Social Network utilizzati (ma anche di quelli che possono rivelarsi utili in prospettiva) e ne valuti impatti e criticità redigendo un report con una cadenza piuttosto frequente (si può iniziare da una reportistica mensile per poi adattare la tempistica una volta raccolte statistiche di rilievo sulla frequenza media degli aggiornamenti).

Lo stesso monitoraggio può essere rivolto in molteplici direzioni, tra queste anche la verifica di “cosa si dice” dell’azienda ed in che termini se ne parla, e si rivela lo strumento più efficace per la gestione dei flame (di cui si è detto).

## Adempimenti in materia di protezione dei dati personali: la profilazione dei dati personali

Il fronte più delicato, in relazione alla protezione dei dati personali, è l’attività di profilazione degli utenti che accedono ai Social Network. Queste attività portano alle aziende ingenti profitti, perché consentono di individuare le preferenze e le attitudini degli utenti e di indirizzare specifiche offerte commerciali mirate ai loro gusti. Grazie alla efficacia dello strumento, che consente appunto di conoscere meglio la clientela e di migliorare l’offerta, il ROI è assai favorevole.

In questo contesto, per “profilazione” si intende il trattamento volto a definire il profilo o la personalità dell’interessato o ad analizzare abitudini e scelte di consumo ovvero a monitorare l’utilizzo dei servizi di comunicazione elettronica (con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti).

La profilazione è una attività intrusiva che presenta rischi considerevoli per la vita privata delle persone e per questo è soggetta a particolari limitazioni dalla normativa in materia di protezione dei dati personali.

E‘da considerare in linea di principio vietato un trattamento di profilazione che presenti rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che potrebbe determinare.

Non è lecito, ed è sanzionato dalla legge, che gli utenti non siano informati che ogni loro pubblicazione, ogni loro commento ed ogni pagina visualizzata sul Social Network costituiscono un *input* per i motori di profilazione, i quali costruiscono a loro insaputa un profilo virtuale molto dettagliato allo scopo di offrire contenuti commerciali ritagliati sui propri interessi: ciò è tanto più grave perché i dati che riguardano gli utenti sono di norma venduti ad aziende esterne, con un accrescimento dei rischi relativi alla tutela della

riservatezza (anche perché potrebbero essere utilizzati per ulteriori finalità non commerciali di natura discriminatoria). Inoltre la nostra normativa stabilisce con chiarezza che l'attività di profilazione deve avvenire in conformità ad una serie di adempimenti.

Infatti chi intende avvalersi dello strumento della profilazione deve in primo luogo eseguire **l**a notificazione del relativo trattamento al Garante per la protezione dei dati personali, quando esso è svolto, come nel caso dei Social Network, con strumenti elettronici. La notificazione compete al titolare del trattamento, cioè a colui che decide in ordine alle finalità, alle modalità del trattamento e agli strumenti utilizzati, compreso il profilo relativo alla sicurezza.

L'obbligo di notificazione al Garante è stato circoscritto, con l'art. 37 del Codice della privacy (D. Lgs. 30 giugno 2003, n. 196), alle sole operazioni di trattamento che possono determinare i più considerevoli rischi per i diritti degli interessati (la precedente normativa, invece, prevedeva per tutti i titolari l'obbligo di effettuare la notificazione, a meno che potessero avvalersi dei casi di esonero o di possibile utilizzazione di una notificazione semplificata). Fra questi casi per i quali l'obbligo di notificazione ancora sussiste è stata compresa l'attività di profilazione degli utenti.

Con la notificazione al Garante viene in sostanza acceso un faro su quei trattamenti di dati personali che per la natura dei dati trattati o in ragione delle relative modalità di trattamento sono considerati idonei a recare pregiudizio ai diritti e alle libertà degli interessati.

La notificazione è una dichiarazione con la quale un soggetto pubblico o privato (in qualità di titolare del trattamento) rende nota al Garante per la protezione dei dati personali l'esistenza di un'attività di raccolta e di utilizzazione dei dati personali, svolta quale autonomo titolare del trattamento. E questa attività da parte del Garante è resa accessibile al pubblico gratuitamente per via telematica mediante il registro dei trattamenti.

La notificazione è indirizzata telematicamente al Garante, prima che inizi il trattamento dei dati, tramite il sito www.garanteprivacy.it, utilizzando la procedura indicata nelle istruzioni. Dall'8 gennaio 2009 è stato posto in linea un nuovo modello di notificazione ulteriormente semplificato.

Se si omette la notificazione o la si presenta in ritardo o incompleta, il titolare è punito con una sanzione amministrativa consistente nel pagamento di una somma da ventimila a centoventimila euro.

La falsa dichiarazione contenuta nella notificazione è un reato, punito con la reclusione da sei mesi a tre anni, salvo che il fatto configuri un reato più grave.

Il secondo adempimento è l'informativa che deve essere resa all'interessato a cura del titolare del trattamento ai sensi dell'art. 13 del Codice della privacy. All'atto della raccolta dei dati personali che lo riguardano l'interessato deve essere posto in condizione di sapere, in modo completo e trasparente, che saranno analizzate le sue preferenze per tutte le finalità che pure dovranno essergli adeguatamente ed esaurientemente rivelate, oltre all'indicazione dei soggetti che eseguiranno (o potranno eseguire) questa analisi e circa i soggetti che utilizzeranno (o potranno utilizzare) queste informazioni per le relative finalità.

L'informativa va fornita all'utente di regola all'atto della sua registrazione nel sito, unitamente alle altre che obbligatoriamente devono essergli fornite (in che modo e per quale scopo verranno trattati i propri dati personali; se il conferimento dei propri dati personali è obbligatorio o facoltativo; le conseguenze di un eventuale rifiuto a rendere disponibili i propri dati personali; a chi saranno comunicati o se saranno diffusi i propri dati personali; chi è il titolare e (se è stato designato) il responsabile del trattamento).

L'utente deve essere, in particolare, informato circa il soggetto al quale potrà rivolgersi in qualsiasi momento per esercitare i diritti di cui all'art. 7 del Codice della privacy (accesso, integrazione, correzione, cancellazione dei dati, opposizione al trattamento, ecc.). L'omessa o inidonea informativa è punita con la sanzione amministrativa del pagamento di una somma da seimila euro a trentaseimila euro (art. 161 del Codice della privacy).

Una informazione più analitica e più dettagliata, in particolare sulle misure di sicurezza adottate e sulle modalità con le quali disattivare in ogni momento i *cookies*, dovrebbe

essere rilasciata nella Privacy Policy del sito, alla quale si può fare riferimento con uno specifico *link*.

L'ultimo adempimento è l'acquisizione di un consenso specifico da parte dell'utente alla sua profilazione.

Il consenso dell'interessato va documentato per iscritto (art. 23 del Codice della privacy) ed è valido se all'interessato è stata resa l'informativa (art. 13 del Codice della privacy) e se è stato espresso dall'interessato liberamente e specificamente in riferimento al trattamento di profilazione chiaramente individuato da parte di soggetti pure chiaramente individuati.

Il trattamento di dati personali effettuato in violazione dell'articolo 23 del Codice è punito con la sanzione amministrativa del pagamento di una somma da diecimila euro a centoventimila euro (art. 162, comma 2 bis, del Codice della privacy). Potrebbe essere altresì applicata una sanzione di natura penale (art. 167 del Codice della privacy).

Nel caso di utilizzo di Social Media da parte di un'azienda, il quadro delle relazioni interessate, però, si complica. Tra il Titolare del trattamento che si va ad instaurare e l'interessato, cioè l'utente, si frappone il fornitore della piattaforma Social utilizzata.

Di fatto, il Titolare del trattamento, cioè l'azienda che decide di comunicare tramite una piattaforma Social, crea un'occasione perché l'utente fornisca informazioni personali al detentore della piattaforma, in aggiunta a quelle già eventualmente fornite.

Questo consente al detentore del Social Media di arricchire la profilazione dell'utente in proprio possesso e di rivenderne le utilità non solo al Titolare di cui sopra ma a chiunque sia interessato a comprarle.

Rispetto a questo processo, l'azienda ha ben poche opportunità di intervento perché si tratta di relazioni commerciali prestabilite rispetto alle quali, indipendentemente dalle proprie dimensioni, non ha potere negoziale, o ne ha pochissimo. E, anche potendo, probabilmente non ha alcun interesse a intervenire se non è in discussione un diretto interesse di business.

Può invece essere importante assumere delle precauzioni che riducano il rischio di essere coinvolti in dispute o contestazioni derivanti dalle politiche commerciali, di privacy o di sicurezza del fornitore della piattaforma Social.

I passi sopra descritti che regolano la conformità alla normativa italiana in materia di protezione di dati personali devono essere sviluppati non solo in relazione alle finalità del Titolare ma anche tenendo conto delle politiche applicate dal fornitore della piattaforma di cui il Titolare sia ragionevolmente consapevole.

Ad esempio, l'informativa all'interessato deve indicare con chiarezza che il detentore della piattaforma prescelta sviluppa per proprio conto, indipendentemente dalla volontà del Titolare, attività di profilazione e che, quindi, aderendo all'iniziativa l'interessato si espone a questo tipo di indagine, al di là di quanto posto autonomamente in essere dal Titolare.

Analogamente ci si dovrà comportare in relazione alla proprietà dei dati, alla loro conservazione e al diritto di cancellazione.

L'obiettivo di fondo è di circoscrivere le responsabilità, informando pienamente non solo di ciò che autonomamente si pone in essere ma anche di ciò a cui indirettamente l'interessato si troverà a partecipare.

L'analisi attenta dei contratti proposti dai fornitori delle piattaforme Social ha dunque una duplice finalità: tutelare la sicurezza delle informazioni aziendali e ridurre il rischio di conformità e legale connesso all'uso di Social Media.

## I contenuti, tra copyright e creative commons

Sui Social Network, tra gli impatti di maggior rilievo trovano senz'altro spazio i contenuti: immagini, testi, tracce audio, loghi e quant'altro.

Questo aspetto deve essere osservato sotto due punti di vista:

1. il primo riguarda l'uso che terzi fanno dei contenuti che ci appartengono (il logo dell'azienda, le affermazioni provenienti da "organi ufficiali", …);
2. il secondo riguarda l'uso di contenuti (prodotti da terzi) sui siti e nei gruppi gestiti dall'azienda o da terzi per conto dell'azienda e i limiti, talvolta insormontabili, che vengono posti per la diffusione di materiale che incorpori contenuti protetti a livello planetario da sistemi DRM.

Se per il primo la gestione può essere assimilata alle misure di monitoraggio predisposte per i flame, per il secondo aspetto, la questione si fa più complessa.

Per ciò che riguarda l'uso di contenuti prodotti da terzi sarà preferibile prediligere materiale contrassegnato Creative Commons ovvero sottoposto ad altri sistemi di tipo copyleft, ancor meglio se prodotto ad hoc, onde ovviare ad iter autorizzativi spesso senza uscita.

Ad esempio, la messa a disposizione dei contenuti su Youtube è filtrata in automatico per bloccare l'uso di brani coperti da copyright, ne consegue che eventuale materiale prodotto per essere condiviso sui Social Network, può essere impoverito dal blocco suddetto che non sempre è agevole rimuovere/aggirare.

Questo perché esiste un criterio, ripreso da un'attività tipica della distribuzione di contenuti radiofonici e televisivi, che su youtube, viene definito "syndication".

La syndication è  la messa a disposizione di un contenuto audio-video.

Youtube, subordina questa disponibilità ad una serie di criteri tra cui: la distinzione delle piattaforme su cui renderlo disponibile e la presenza di contenuti che possano far insorgere questioni legali correlate alla tutela dei diritti d'autore.

Ne discende un ulteriore legame con un altro aspetto affrontato nei termini d'uso di youtube, ovvero le c.d. piattaforme monetizzate.

Vengono considerate "piattaforme monetizzate" le seguenti piattaforme:

- Applicazione YouTube nativa su Android
- Applicazione YouTube nativa su Xbox
- Applicazione YouTube nativa su GoogleTV
- Sito web YouTube Mobile (m.youtube.it)
- YouTube sulla TV (solo versioni più recenti)

Sempre nella documentazione predisposta da Youtube, oltre alle suddette piattaforme monetizzate, con il termine "tutte le piattaforme" si intendono quelle seguenti:

- Applicazione YouTube nativa su iPhone, iPad
- Applicazione YouTube su Apple TV
- Applicazione YouTube legacy su Wii ("XL")
- TVsM e feature phone legacy basati su API YouTube.

In pratica al verificarsi di determinate condizioni, legate al profilo di disponibilità dei contenuti attribuito dai titolari dei diritti d'autore, i file multimediali disponibili su youtube per PC, non sono visibili sulle altre piattaforme.

I contenuti predisposti in violazione dei termini d'uso di Youtube, vengono bloccati, rimossi o impoveriti (si pensi al blocco di una colonna sonora), per cui per predisporre una strategia di gestione sui Social Media, occorrerà progettare contenuti "compliant" sin dal principio con i requirements del Social Network (nell'esempio appena fatto, youtube) su cui sono destinati ad essere immessi direttamente ovvero ad essere immessi in seguito a condivisione (intendendosi con il termine "condivisione" l'attività di segnalazione di un contenuto interessante attraverso la sua messa a disposizione su piattaforme ulteriori rispetto a quelle su cui si è, originariamente, proceduto allo upload, in sostanza il retweet in Twitter o la condivisione sul proprio diario/bacheca in Facebook, Linkedin, ecc.

### Come è stato affrontato il tema dalla giurisprudenza

A margine dei discorsi fatti è utile porre in risalto alcuni elementi emersi in recenti sentenze pronunciate sia contro le società che gestiscono i Social Network, sia contro dichiarazioni diffamatorie "postate" sui diari, sulle bacheche ovvero attraverso gli strumenti messi a disposizione dai Social Network.

Il Tribunale di Livorno, con sentenza 31.12.2012 n° 38912, ha stabilito che

"*l'uso di espressioni di valenza denigratoria e lesiva della reputazione del profilo professionale dell'ex datore di lavoro pubblicate sulla bacheca del proprio profilo Facebook integra sicuramente gli estremi della diffamazione, alla luce del carattere pubblico del contesto in cui quelle espressioni sono manifestate, della sua conoscenza da parte di più persone e della possibile sua incontrollata diffusione tra i partecipanti alla rete del Social Network.*

*Più esattamente tale comportamento va qualificato come delitto di diffamazione aggravato dall'avere arrecato l'offesa con un mezzo di pubblicità (fattispecie considerata al terzo comma dell'art. 595 c.p. e equiparata, sotto il profilo sanzionatorio, alla diffamazione commessa con il mezzo stampa), poiché la particolare diffusività del mezzo usato per propagare il messaggio denigratorio rende l'agente meritevole di un più severo trattamento penale*". (fonte: Michele Iaselli, altalex.com)

Dunque non solo viene riconosciuta l'integrazione degli elementi della diffamazione ma viene attribuita l'aggravante di cui al terzo comma, dell'art. 595 c.p., che recita:

*"Se l'offesa è recata col mezzo della stampa o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico, la pena è della reclusione da sei mesi a tre anni o della multa non inferiore ad euro 516"*.

Un'altra sentenza, meno recente che merita tuttavia di essere segnalata per la risonanza che ha avuto è senz'altro quella del Tribunale di Milano del 12 aprile 2010, n. 1972. In quell'occasione vennero condannati tre dirigenti di Google Italia S.r.l.per violazione della privacy per trattamento illecito di dati ( ex art. 167 del decreto legislativo 30 giugno 2003, n. 196) a seguito del caricamento da parte di alcuni ragazzi di un video sulla piattaforma on line che ritraeva un adolescente diversamente abile insultato e vessato dai compagni di scuola. La sentenza se da un lato provocò la sollevazione di molte "firme" del web (blogger e non solo), dall'altro identificò nella mancata, corretta, informativa nei confronti degli "uploaders" il profilo di responsabilità del "content provider"

La sentenza sopra citata è stata comunque ribaltata, dalla pronuncia della Corte d'Appello di Milano del 21 dicembre 2012 che ha assolto i dirigenti di Google Italia ritenendo che non potesse sussistere in capo al "provider di contenuti" l'onere che il Tribunale di Milano, in primo grado, aveva ravvisato.

Molte altre sono le sentenze di notevole interesse, sopratutto in Nord America, interessante ad esempio una presa di posizione del District Attorney di Boston avverso Twitter per aver "segnalato ai propri users che erano in corso indagini nei loro confronti".

In molti casi queste sentenze pur perseguendo il malcelato scopo di arginare lo strapotere e la "posizione dominante" dei colossi che controllano i Social Network, forniscono indicazioni utili in merito alla possibilità di tutela, rispetto all'abuso da parte di terzi, delle informazioni rese disponibili sulla Rete in generale e sugli strumenti Social in particolare.

## Trascurare la sicurezza: esempi di casi critici

Ci sono nuovi rischi collegati ai Social Media? Sì, certo e l'abbiamo visto nel capitolo precedente. E come per ogni cosa nuova, bisogna imparare a gestirli. Ripercorrere esperienze critiche, alcune risolte positivamente, altre meno, può aiutare a contestualizzare il tema, sottraendolo alla inevitabile astrattezza di una trattazione formale.

Nei casi riportati nel seguito, tutti di pubblico dominio, anche se con diversi livelli di notorietà, abbiamo ritenuto di mantenere in chiaro il nome dell'azienda o del soggetto interessato.

Ci scusiamo di quella che può, in taluni casi, apparire come una pubblicità negativa però, il riferimento ad un marchio o ad un nome preciso e noto consente di apprezzare meglio alcuni aspetti interessanti:

- le difficoltà riguardano ogni tipo di soggetto: dalla grande azienda al personaggio politico
- la capacità di reagire, spesso, è inversamente proporzionale alle dimensioni
- le reazioni del pubblico ad una iniziativa di Social Media hanno sempre una componente di imprevedibilità

D'altra parte, le aziende citate, che sono tra le prime ad essersi scontrate con le difficoltà di questa nuova forma di relazione, emergono anche come le più innovative: hanno sperimentato e, probabilmente, hanno imparato, costruendo un vantaggio competitivo che, chi non ha voluto rischiare, oggi deve recuperare.

Abbiamo già identificato i principali cluster per i rischi generati dall'utilizzo dei Social Media in azienda: rischio di conformità, operativo, relazionale.

Come si accennava, i rischi relativi ai Social Media hanno una caratteristica particolare derivante dalla natura stessa dei Social Media: quella di socializzare velocemente qualsiasi informazione con tutti contatti attivi e propagandosi poi in modo non controllabile verso tutti i contatti dei contatti e così via.

L'impatto reputazionale di eventi dannosi associati a rischi inclusi nel cluster relazionale viene così amplificato velocemente fino a creare in pochi istanti un audience di carattere globale, in grado di incidere direttamente, per la sua ampiezza, su parametri di business molto rilevanti e misurabili come fatturato e valore dell'azione.

I Social Media espongono a "pubblico giudizio" tutto ciò che riguarda l'azienda in termini di prodotti, servizi e comportamento, accelerando la diffusione delle informazioni nel web, siano esse vere o false, positive o negative.

Qualche esempio dei più noti e clamorosi esempi di insuccesso o di situazioni non previste in tale ambito può aiutare a comprendere meglio i rischi e la necessità di prevedere, al giusto livello aziendale, dei modelli di reazione adeguati all'accadere di eventi non desiderati, in modo di assicurare una risposta sollecita e corretta.

### *Reazioni inattese*

- Il 18 Gennaio la multinazionale di fast food McDonalds ha creato e condiviso su Twitter (@McDonalds) l'hashtag "#McDStories", chiedendo ai quasi 300.000 follower di utilizzarlo per condividere le belle storie di tutti i giorni legate alla marca.

  Il risultato? Inatteso. La rete ha sommerso di commenti e tweet negativi l'azienda (se fate una ricerca, guardate anche la gallery dei top video), criticandola sul cibo spazzatura, il trattamento dei dipendenti, il servizio offerto, l'igiene … tanti anche i tweet italiani!

  Il management è stato così costretto a sospendere l'iniziativa dopo pochissimo, commentando che l'azione non ha avuto l'effetto sperato.

- I brand Patrizia Pepe ha lanciato da tempo una campagna "misteriosa". In prima battuta, le modelle protagoniste

avevano il volto coperto dagli oggetti più disparati e il claim recitava “Who is Patrizia?”. Successivamente, il brand ha preso a chiederci “Where is Patrizia?”, mostrandoci bellissime modelle in luoghi particolari. A questa campagna gli utenti hanno reagito in modo inatteso, ponendo essi stessi una domanda, che può essere riassumere in “Quanto pesa la modella?”.

La foto incriminata è quella che vedete qui a lato, pubblicata sulla bacheca della pagina di Facebook del brand. Due fan commentano in maniera forse un po’ colorita dicendo che sono foto e modelle come queste ad alimentare modelli sbagliati e apostrofando la protagonista della campagna come anoressica. Qualcuno si è unito al coro, altri hanno difeso il brand. E la replica di Patrizia Pepe non si è fatta attendere, senza però riuscire a riprendere gli obiettivi originali della campagna.

### *Presenza passiva sui Social Media*

- Una nota catena americana di pizzerie (Domino's Pizza) nell’aprile 2009, ha subito un brusco calo di vendite, in ragione della pubblicazione su Youtube di un video da parte di 2 suoi dipendenti. In questo video i due impiegati mostravano le loro molteplici violazioni di regole igienico-sanitarie durante la preparazione di un pasto. L’effetto del video, di enorme diffusione su Youtube, è stato amplificato dal fatto che la reazione della compagnia è avvenuta solo alcuni giorni dopo la pubblicazione dello stesso, causando inoltre all’azienda un calo del 10% in market capitalization nel periodo immediatamente successivo all’accaduto.

**FIGURA 10 - IL CASO "PATRIZIA PEPE"**

### *Sottrazione di identità*

Il sindaco di Roma Alemanno aveva aperto un account su Twitter con il seguente nome: @AlemannoTW. Dei burloni aprirono un account imitazione col nome @AlemannoTW, dove la “l” (elle) minuscola era stata sostituita con la “I” (i) maiuscola, evidentemente indistinguibile. L’account fasullo pubblicò messaggi falsi e dissacranti ma divertenti. Il sindaco di Roma ha reagito duramente all’accaduto pubblicando su Facebook una nota ufficiale per informare i cittadini dello scambio d'identità: "Vi segnaliamo una gravissima sottrazione di identità verificatasi sul Social Network Twitter, ed avvenuta tramite una combinazione per niente casuale delle lettere del cognome del sindaco Gianni Alemanno". La rapidità della reazione ha fatto sì che la situazione venisse ripresa in poco tempo.

5 agosto 2012 – Nell’arco di tre giorni l’agenzia giornalistica Reuters è stata vittima di due attacchi informatici. Il 3 agosto gli hacker sono riusciti ad accedere alla piattaforma di blogging ed hanno postato false notizie attribuite all’agenzia giornalistica. Reuters ha messo offline la piattaforma di blogging e l’attacco si è spostato sull’account Twitter dell’organizzazione, che è stato rinominato e dal quale sono stati inviati dei falsi messaggi

- http://www.theregister.co.uk/2012/08/05/reuters_hacked/
- http://www.zdnet.com/reuters-twitter-account-hacked-7000002142/
- http://news.cnet.com/8301-1009_3-57486971-83/reuters-twitter-account-hijacked-fake-tweets-sent/

### *Gestione della presenza sui Social Media*

Nestlé ha avuto un grave problema relativo ai Social Media nel corso del 2010. La loro pagina Facebook e il video su YouTube sono stati sotto pressione da parte di Greenpeace per le politiche utilizzate per l’acquisto di olio di palma. Greenpeace accusa l’azienda di sostenere la deforestazione e di minacciare le scimmie Orangutan in via di estinzione. Greenpeace ha creato un video che ha paragonato mangiare una barretta di Kit Kat ad uccidere un orango. Questo video è stato messo su YouTube e ha ricevuto più di un quarto di milione di visite nelle prime due settimane.

Nestle ha ottenuto da Youtube che il video venisse rimosso, sostenendo che il video violava il loro marchio di fabbrica, cosa probabilmente vera.

La rimozione ha provocato la reazione dei sostenitori di Greenpeace che hanno iniziato a fare commenti negativi sulla pagina di Facebook aziendale.

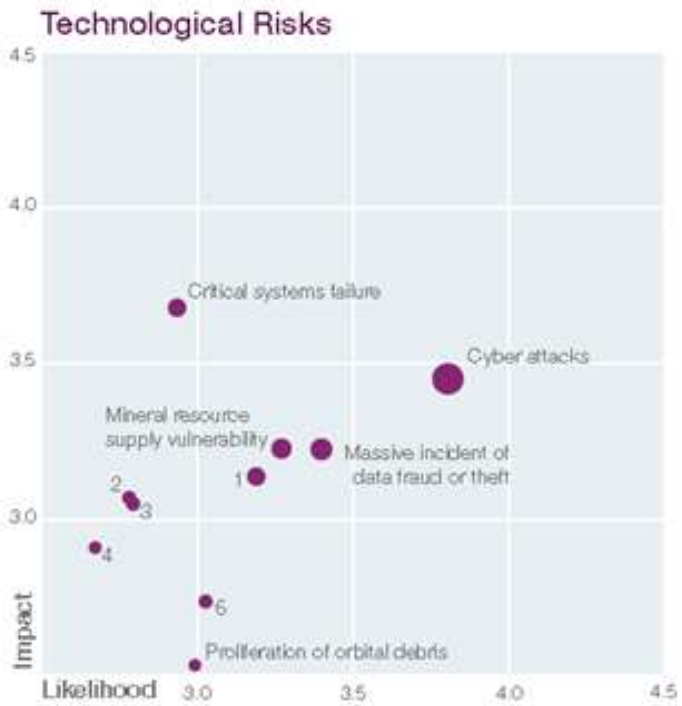
Nestlé poi si è organizzata per proteggere la propria pagina eliminando i commenti critici, causando la reazione dei sostenitori di Greenpeace con altri interventi negativi: tutto questo è continuato per diverse settimane.

### *Incidenti di sicurezza*

- 6 giugno 2012 – Secondo un rapporto pubblicato in Norvegia sono state pubblicate su di un sito Internet russo circa 6,5 milioni di hash SHA-1 delle password LinkedIn associate ad una richiesta di aiuto per poterle decifrare. Diversi ricercatori di sicurezza hanno verificato che si tratta di password utilizzate in modo univoco per l'accesso a LinkedIn.
- https://isc.sans.edu/diary.html?storyid=13390
- http://www.zdnet.com/blog/btl/6-46-million-linkedin-passwords-leaked-online/79290
- 24 luglio 2012 – Gli utenti della piattaforma di gaming online Gamigo sono stati invitati a cambiare con urgenza le loro credenziali di accesso dopo che è stato rinvenuto su Internet un file contenente 11 milioni di hash delle password appartenenti agli utenti del sito, che includeva anche 8,2 milioni di indirizzi email diversi. Il file è stato postato su di un forum già impiegato in precedenza per pubblicare le password sottratte da LinkedIn, eHarmony ed altri siti web. Gamigo ha confermato l'autenticità delle informazioni rivelate ed ha confermato la rilevazione di una breccia di sicurezza nel marzo 2012, quando sono state copiate le informazioni contenute in un vecchio database http://www.h-online.com/security/news/item/11-million-passwords-leaked-from-online-gaming-platform-1651198.html

## Trascurare la sicurezza: aspetti economici danni e criminalità

Dati riguardanti gli aspetti economici della criminalità informatica, al momento della redazione del presente documento, vengono forniti quasi esclusivamente da aziende attive nel settore della sicurezza informatica. La presenza di dati pubblicati da enti governativi e non governativi, laddove esistenti, risultano di scarsa rilevanza e non sufficienti a descrivere questo ampio fenomeno.




Source: World Economic Forum

In una recente pubblicazione del Word Economic Forum [2] dal titolo "Global Risks 2012" vengono analizzati i principali rischi globali ai quali sono sottoposti settori pubblici o privati dell'economia, nel loro complesso. Questi rischi sono mappati secondo cinque macro aree: rischi economici, ambientali, geopolitici, sociali e tecnologici.

Nella categoria afferente i rischi tecnologici si evidenzia come i "cyber attacks" e i "massive incident of data faud or theft" ricoprono un ruolo fondamentale in termini di impatto e probabilità di un loro verificarsi.


nza CC BY-SA 3.0 IT Oracle Community For Security

In interessanti studi condotti da primarie aziende operanti nel comparto della sicurezza informatica quali Symatec e Trend Micro, emerge una tendenza che vede i nuovi bersagli degli attacchi informatici, le piccole e medie imprese.

**FIGURA 11 - RISCHI TECNOLOGICI: TABELLA PROBABILITÀ/IMPATTO**

Sempre nel settore privato, la survey commissionata da *Check Point Software Technologies* dal titolo *"The impact of cybercrime on businesses"* ***[3]*** e condotto da Ponemon Institute, sulla base di 2.618 interviste a executive e responsabili della sicurezza IT negli Stati Uniti, Regno Unito, Germania, Hong Kong e Brasile rileva che gli attacchi rivolti alle aziende non solo crescono numericamente, in media 66 episodi a settimana, ma anche in sofisticazione, comportando danni economici assai rilevanti.

Di seguito si riporta una tabella riepilogativa della stima dei danni per ciascun attacco che comprende costi d'investigazione, di marketing e brand reputation per ristabilire la fiducia

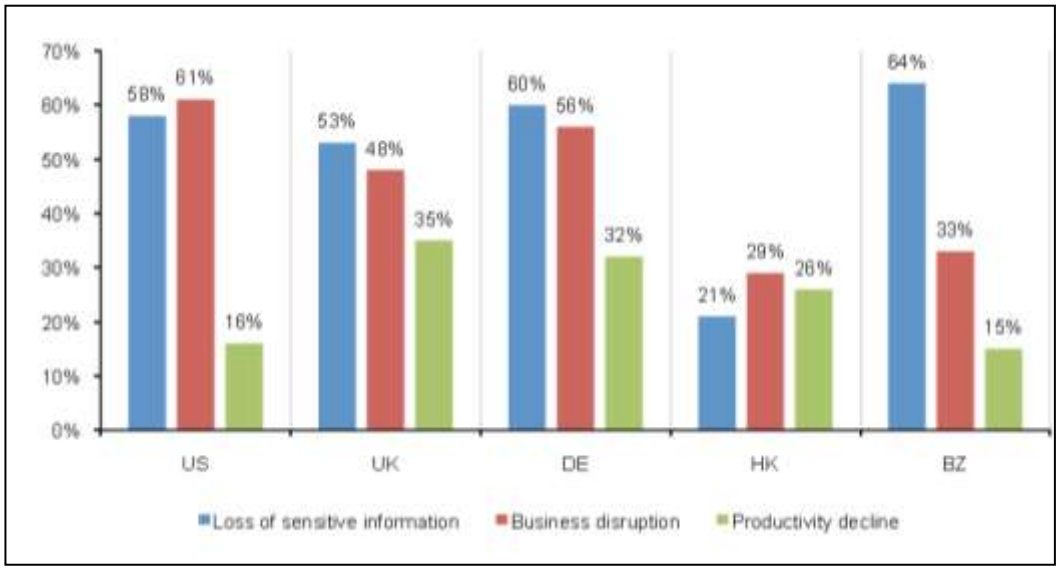
**TABELLA 9 - DANNI PROVOCATI DA CIASCUN ATTACCO**

| Dollar range | US | UK | DE | HK | BZ |
|---|---|---|---|---|---|
| < 10,000 | 2% | 5% | 2% | 15% | 10% |
| 10,000 to 50,000 | 9% | 18% | 9% | 21% | 19% |
| 50,001 to 100,000 | 10% | 27% | 12% | 28% | 26% |
| 100,001 to 200,000 | 13% | 31% | 33% | 15% | 15% |
| 200,001 to 300,000 | 30% | 9% | 27% | 8% | 9% |
| 300,001 to 400,000 | 22% | 5% | 5% | 9% | 5% |
| 400,001 to 500,000 | 7% | 3% | 8% | 3% | 8% |
| 500,001 to 1,000,000 | 4% | 1% | 3% | 1% | 5% |
| > 1,000,000 | 3% | 1% | 2% | 0% | 3% |
| Total | 100% | 100% | 100% | 100% | 100% |
| Extrapolated value | $276,671 | $229,560 | $298,359 | $159,244 | $106,904 |

nell'azienda colpita dagli attacchi e gli investimenti in tecnologia.

Interessante è notare come nella survey la perdita d'informazioni sensibili e d'interruzione del servizio sono le due principali conseguenze degli attacchi mirati.

**TABELLA 10 - CONSEGUENZE DEGLI ATTACCHI**




Ultima, ma non meno importante, è la percezione che gli executive e i responsabili IT di tutte le aree di business considerate, hanno nei confronti delle attività svolte dai propri dipendenti che comportano i rischi maggiori, collocando al primo posto l'utilizzo di device mobili, seguito dall'accesso ai Social Network e dal ricorso a dispositivi rimuovibili, come le chiavette Usb.

La tabella che segue riporta l'esito di una rilevazione di questa percezione.

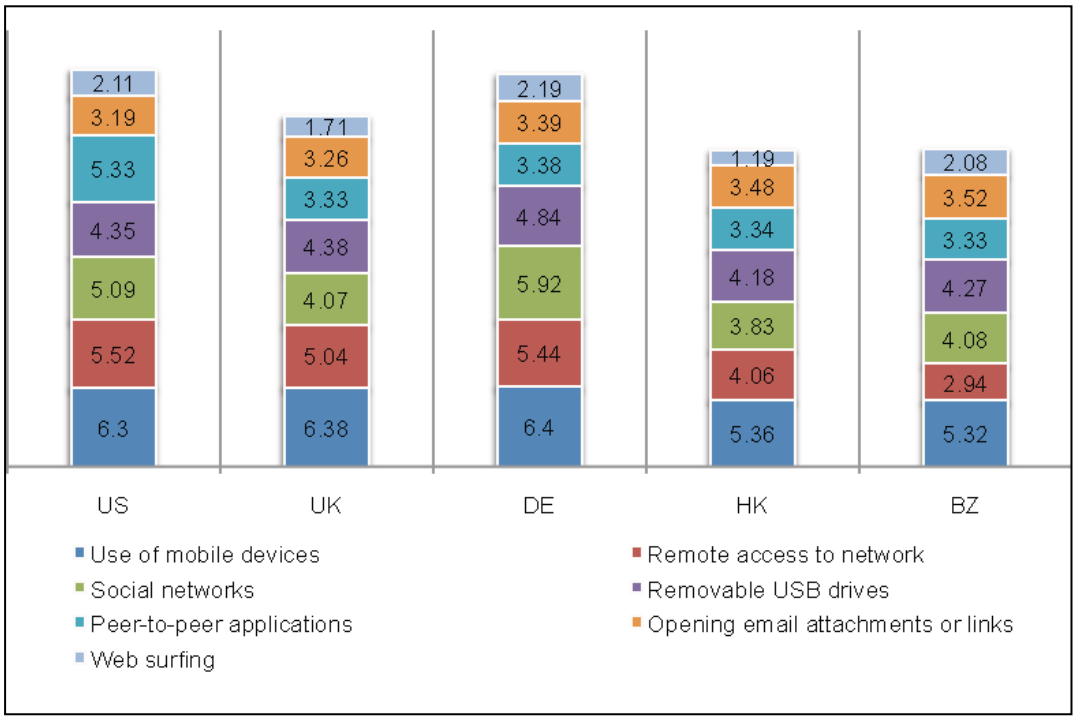



**FIGURA 12 - PRINCIPALI FONTI DI RISCHIO (7-ALTO 1-BASSO)**

# PARTE TERZA: I CASI AZIENDALI

## Il caso Bisazza

Bisazza è uno dei brand di lusso più autorevoli nell'ambito del design e leader mondiale nella produzione del mosaico di vetro per la decorazione di interni ed esterni. Fondata nel 1956 ad Alte in provincia di Vicenza, oggi è un'impresa all'avanguardia caratterizzata da dinamismo imprenditoriale, utilizzo di moderne tecnologie e attenzione alle evoluzioni del mercato.

In questi ultimi anni la strategia di Piero Bisazza, Amministratore Delegato dell'Azienda, si è focalizzata sul rafforzamento del marchio, la qualità del prodotto e il potenziamento del retail, attraverso l'apertura di dieci spazi monomarca, Anversa, Barcellona, Berlino, Chicago, Londra, Los Angeles, Miami, Milano, Parigi e New York, in aggiunta ai 5000 punti vendita in tutto il mondo.

Dal 2005 l'Azienda fa parte di Altagamma, fra i nomi di eccellenza delle imprese Italiane.

A Giugno 2012 è stata inaugurata la Fondazione Bisazza, un nuovo spazio culturale dedicato al design e all'architettura contemporanea, che oltre ad accogliere le opere e le installazioni firmate da alcuni progettisti di fama internazionale, ospita una serie di mostre temporanee provenienti dalle più importanti istituzioni del mondo.

Sulla scia della strategia aziendale, nel corso del 2012 è stato attivato un Piano per l'approccio strutturato al Social Network, con l'obiettivo di:

- Potenziare il web marketing aziendale nei canali Social
- Aumentare la percezione del marchio e il suo corretto posizionamento online
- Stimolare l'interazione con i pubblici elettivi del brand
- Gestire la brand reputation.

Oggi Bisazza permette ai suoi utenti di diventare dei designer per qualche minuto. Nella pagina Facebook aziendale è infatti possibile giocare, creare e divertirsi con "Design Your Bisazza", un'applicazione in cui si può costruire il proprio decoro in mosaico utilizzando le tessere Bisazza e diverse funzioni di disegno, per poi condividerlo nella propria bacheca e sfidare i propri amici in una gara di creatività.

Nel proprio sito internet, Bisazza invece ha lanciato un'applicazione dove la costruzione del mosaico viene fatta in modo più professionale con tantissime possibilità di combinazione delle tessere e l'opportunità anche di caricare una foto e renderla un mosaico.

Per pubblicizzare queste applicazioni, con un'attività di digital PR, sono stati contattati diversi influencer nel mondo del design, per far testare le applicazioni e condividere il risultato ottenuto.

Company Facebook page: facebook.com/Bisazzaofficial

Company Twitter account: twitter.com/bisazzacom

Company website: www.bisazza.com/

La strategia di canale fil-rouge del progetto è rappresentata nella figura seguente.

### *D Post prodotto*

Immagini e testi emozionali per aumentare il livello di gradimento (mi piace, retweet) e commenti. Le immagini hanno come soggetto delle immagini di prodotti ambienti o in still life.

### *#BisazzaWorld E*

Racconto dei progetti contract di Bisazza attraverso un viaggio itinerante nei diversi paesi del mondo. Tono emozionale e friendly per incuriosire e far conoscere creando engagement (mi piace, retweet..)

### *NEWS EVENTI M*

Link referrals al sito con anticipazione delle news più importanti alla community

### #DesignTips M

Rubrica con consigli di design, arredamento e anche piccoli accorgimenti per la cura del proprio mosaico in casa. L'obiettivo di questa rubrica è stimolare interazione con l'utente (commenti) oltre al solo "mi piace"; creare engagement e condivisione di idee…

**#News eventi, esempio: Cersaie Live M**

L'evento del Cersaie è stato raccontato in tempo reale su Twitter creando una diretta di aggiornamenti, interviste e anteprime sulle nuove collezioni Bisazza

**D #Preview collection**

I fan e followers di Facebook e Twitter hanno avuto il privilegio di conoscere in anteprima le novità della Collezione Mosaico 2013.

**#DesignYourBisazza E**

Abbiamo iniziato la campagna #DesignYourBisazza creando interazione coinvolgendo un pubblico più ampio possibile attraverso il passaparola.

**Risultati raggiunti da Marzo a Ottobre 2012**

Account Facebook: su Facebook Bisazza ha aumentato in maniera rilevante la sua attività, raggiungendo i 6125 fans e con un'interazione media per post pubblicato che si aggira su 70 "mi piace". Si punta molto sulla condivisione di fotografie che ritraggono le creazioni e le ultime collezioni realizzate. Per ogni post vi è una buona risposta dei fans, i quali autonomamente pubblicano risposte molto positive sui post pubblicati. L'applicazione "design your Bisazza" lanciata di recente ha subito ottenuto commenti positivi e buona interazione.

Account Twitter: su Twitter Bisazza ha raggiunto i 490 followers a fronte di 324 following, mantenendo un tipo di comunicazione molto diretta col follower (condivisione shortlink e rimandi su link esterni), tanto che si registra un buon numero di tweet positivi diretti a Bisazza e altri portali dedicati al mosaico/design, con allegati link esterni che rimandano principalmente a foto o interventi su blog.

La Funzione *Press Relations* ha sviluppato il progetto con il supporto esterno di un'agenzia di Specialisti di settore e coordinandosi – secondo necessità – con vari dipartimenti aziendali: Area IT, tecnica, grafica e commerciale.

Il Progetto ha anche fornito l'occasione per standardizzare le esperienze Social di origine spontanea, create dalle filiali; la pagina

creata da Bisazza USA e quella Bisazza Australia, sono state fatte convergere nella nuova pagina Bisazza.com.

La Policy interna del Gruppo non prevede l'accesso ai Social Network dall'interno, con l'eccezione dell'area *Press Relations.* Tutti gli altri accessi sono sottoposti ad un sistema di Web Filtering che presiede alla navigazione Sicura, bloccando l'accesso ai siti definiti non accessibili.

Recentemente è stato rilasciato su Facebook un Game proprietario *(*Design Your Bisazza, sopra citato*),* accessibile dall'interno, il cui accesso è vincolato ad una precisa fascia oraria.

## Il caso Bticino

La scommessa di BTicino sui Social Network riguarda un largo spettro di Social Network tradizionali, dove ha una presenza articolata, che si affianca ad esperienze di Social Network "proprietarie" iniziate nei primi anni 2000, che non sono però oggetto di questa trattazione e per le quali vi rimandiamo al sito (http://www.myopen-legrandgroup.com/).

Ha una pagina su Facebook, dove presenta prodotti presenti e passati oltre a un configuratore che permette agli utenti di definire le soluzioni domotiche più adatte e condividerle con i propri "amici".

Su YouTube mette video pubblicitari per i prodotti più complessi e tutorial per installarli.

Su Flickr ci sono immagini dei prodotti, come su Pinterest, dove però BTcino ha cercato di creare accostamenti visivi che richiamano le peculiarità del brand e dei suoi prodotti.

Blink [www.blinkproject.it] è il corporate blog di BTicino sul mondo del progetto contemporaneo.

Un hub di connessioni, un punto di incontro, condivisione e interazione.

Un osservatorio digitale dove si parla soprattutto di architettura e design, ma con uno sguardo interessato ai territori limitrofi della cultura del progettare.

Con una **pagina Facebook totalmente dedicata** (www.facebook.com/BTicinoSocial) e un nuovo modo di comunicare orientato ai Social, BTicino crea un canale di comunicazione continuativo dedicato al suo mondo con quattro obiettivi fondamentali: contattare, informare, ispirare e coinvolgere.

Informare e contattare, attraverso il wall e la welcome page, i consumatori abituali per coinvolgerli in experience totalmente nuove, e realizzare un luogo virtuale dove creare il primo contatto con nuovi potenziali interlocutori. Uno spazio dove il visitatore possa ascoltare, ma soprattutto possa essere ascoltato dal brand.

Ispirare, attraverso le experience create ad hoc, un nuovo modo di concepire gli spazi della propria casa: il configuratore ripensato per Facebook permette di scoprire tutte le soluzioni estetiche e domotiche proposte da BTicino, su misura per gli ambienti di ogni cliente e su suoi gusti.

Proprio per la caratteristica tipica di BTicino di orientarsi verso tutto ciò che è innovazione, il nuovo progetto Social non utilizza solo Facebook, ma coinvolge anche **Pinterest** , www.pinterest.com/BTicino, il nuovo Social Network basato sulla condivisione di immagini, il cui uso si sta diffondendo molto velocemente. Qui gli utenti vengono connessi attraverso interessi simili: la vetrina di Pinterest si presta particolarmente ad esibire il design dei prodotti di BTicino.

BTicino è parte del Gruppo Legrand, specialista globale nelle infrastrutture elettriche e digitali dell'edilizia, e come tale è solo uno degli attori, all'interno del Gruppo, del mondo dei Social Network. Il sito della Capogruppo ha dedicato una pagina alla mappatura di tutti i Social Network alimentati dalle filiali nel mondo.

L'impostazione della pagina evidenzia una regia centrale, confermata dalle politiche sia di comunicazione che di utilizzo dei diversi siti nel mondo.

La "*Netiquette"* pubblicata sulle diverse pagine Facebook, al di là della lingua, è la stessa in tutto il mondo, così come l'impostazione grafica e la struttura dei contenuti. Nel disclaimer si sottolinea che la pagina è moderata e che quanto pubblicato è verificato da amministratori che si riservano la facoltà di eliminare contenuti non conformi allo spirito della pagina o delle condizioni di utilizzo.

bticino

Netiquette

**ARTICOLO 1: MODERAZIONE**

Questa pagina Facebook è uno spazio aperto a tutti gli utenti. Per garantire la qualità e la correttezza della comunicazione, la pagina è moderata. Tutti i messaggi vengono letti per garantire corrispondenza allo scopo della pagina Facebook, il rispetto delle condizioni di utilizzo e la presente netiquette.

**BTicino comunica che i seguenti messaggi verranno automaticamente eliminati:**

- Messaggi pubblicitari, promozionali o commerciali e tutti i tipi di annunci economici
- Spam e pubblicazione ripetitiva di messaggi identici o simili
- Messaggi contenenti dettagli o recapiti personali: numeri di telefono, indirizzi postali o elettronici e link a siti web terzi
- Qualunque argomento punibile ai sensi di legge: incitazioni all'odio razziale e alla violenza, pedofilia, negazionismo, apologie ai crimini di guerra, antisemitismo ecc.
- Qualunque argomento discriminatorio: razzismo, omofobia, sessismo ecc.
- Insulti, oscenità, pornografia o incitamento al consumo di droga
- Gli attacchi diretti tra gli utenti o i partecipanti ad una discussione
- I messaggi fuori tema o considerati come "troll" (messaggio o persona il cui carattere è in grado di generare polemiche o è eccessivamente provocatorio, senza cercare di essere costruttivo. Il troll è una forma di spam)

**ARTICOLO 2: DIRITTI E DOVERI DEGLI UTENTI**

**Per garantire la qualità dei contributi, vi invitiamo a:**

- Non scrivere messaggi sotto forma di SMS
- Non abusare di lettere maiuscole e della punteggiatura
- Utilizzare la lingua italiana
- Citare le vostre fonti

Uno o diversi amministratori della pagina Facebook si riservano il diritto, senza alcun preavviso per l'utente, di cancellare tutto o parte dei messaggi che contravvengano al presente statuto e alle condizioni di utilizzo o che siano contrari alla legge, e di escludere dalla pagina Facebook, temporaneamente o definitivamente, gli utenti che li violino palesemente, ripetutamente e sistematicamente.

Le decisioni degli amministratori non possono essere contestate. Lasciando o inviando messaggi alla pagina Facebook, l'utente si impegna a rispettare l'autorità degli amministratori e allo stesso tempo le presenti disposizioni.

Quello che non si evince navigando tra le varie pagine è la politica interna del Gruppo nei confronti dell'utilizzo da parte dei dipendenti dei Social Network, che, pur non impedendo l'accesso, non lo contempla, se non per motivi rigorosamente collegati all'attività lavorativa. Per rafforzare questa impostazione è stata diffusa dalla Capogruppo, la procedura che informa il personale dell'attività di controllo, effettuata nel rispetto dei principi di pertinenza e non eccedenza, mediante un sistema di webfiltering e di tracciamento delle navigazioni, per monitorare eventuali "*abusi riguardanti la consultazione di siti senza alcuna attinenza con l'attività lavorativa (Social Network, download per uso privato, etc …)".*

La Direzione Risorse Umane è l'unico ente deputato all'analisi delle statistiche mensili di accesso e garante del rispetto del criterio di gradualità dell'indagine.

In caso di accertamento di un utilizzo anomalo, saranno verificati preventivamente i dati aggregati, riferiti all'intera struttura lavorativa o su aree. Il controllo anonimo potrà concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati ed autorizzazioni ricevute. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

A fronte di ulteriori anomalie riscontrate si potrà procedere all'analisi di un controllo su base individuale, limitando però, in questa fase, il campo di analisi al solo tempo trascorso in rete.

In caso di presenza di elementi oggettivi e/o comportamenti del dipendente che configurino un potenziale e incombente rischio per la Società le modalità dei controlli potranno essere appositamente rivalutate, su autorizzazione della Direzione Risorse Umane.

## Il caso Lugana

Lugana è la prima DOC riconosciuta in Lombardia e una delle primissime in Italia, a testimoniare l'alto valore storico e culturale di tale realtà. Sin dalla sua fondazione nel 1990, il Consorzio Tutela del Lugana DOC si prefigge come obiettivi di preservare e garantire l'unicità del Lugana, e al tempo stesso di promuoverne, diffonderne e valorizzarne la conoscenza, sia in territorio nazionale che oltre confine. L'area di produzione è contenuta: abbraccia le zone di Desenzano, Lonato del Garda, Peschiera del Garda, Pozzolengo e Sirmione.

Il percorso di crescita istituzionale e di prodotto ha reso il Lugana un vino e un marchio ormai maturo, che incontra il favore di fette di mercato sempre più ampie. Tale posizionamento è anche il frutto di un intenso sforzo di comunicazione, che vede il Consorzio impegnato su molteplici fronti e canali di comunicazione, come la carta stampata, gli eventi fieristici, e gli eventi sul territorio.

Appuntamenti italiani e internazionali, come Vinitaly di Verona, il Salone del Gusto di Torino e Prowein, si rivelano occasioni irrinunciabili per far apprezzare il Lugana nelle varie declinazioni ad un vasto pubblico sia di professionisti di settore che di semplici amatori. Accanto a tali vetrine di caratura internazionale si collocano inoltre i numerosi eventi di degustazione organizzati nel corso dell'anno, che richiamano un importante numero di visitatori e di ospiti, oltre ai consociati che propongono in degustazione le diverse tipologie di prodotto e le proprie etichette.

Sono proprio gli eventi ad aver trovato un importante terreno di sviluppo nelle piattaforme Social, approcciate in forma sperimentale dal Consorzio, che già da tre anni ha iniziato a testare gli effetti della promozione tramite il Web 2.0, realizzando benefici tangibili legati a:

- l'aumento del tasso di partecipanti agli eventi (circa 25% in più rispetto alla partecipazione ottenuta a fronte della promozione attraverso i canali tradizionali);
- la possibilità di avere partecipanti composti da un pubblico informato del vino ma non professionista.

“Per anni la comunicazione del Consorzio è stata rivolta soltanto agli operatori del settore - commenta il Direttore del Consorzio Carlo Veronese - oggi però le finalità promozionali che il Consorzio è chiamato a perseguire sono cambiate, devono adattarsi ad un pubblico assai più vasto, coinvolgere sempre di più i consumatori, anche quelli non appassionati, e questo richiede di semplificare i messaggi, di far sì che siano immediati ed accattivanti, il meno possibile autoreferenziali”.

C’è inoltre un altro importante aspetto da considerare, che ha a che fare con il nuovo paradigma della comunicazione mediatica: “un meccanismo regolato fino a non molto tempo fa da una dinamica discendente, dall’alto verso il basso - spiega Veronese - una volta era la stampa di settore a rappresentare il destinatario finale dei nostri sforzi, in quanto soggetti in grado di esercitare un’influenza diretta sulle opinioni e le scelte dei ristoratori, che a loro volta incidevano direttamente sulla determinazione delle scelte e sullo sviluppo delle preferenze del consumatore finale; oggi assistiamo invece a una logica che si sviluppa dal basso, in cui è il consumatore stesso che, informato e consapevole, sa già cosa chiedere al ristoratore e spesso cosa aspettarsi di trovare”. Questa rapida evoluzione è stata chiaramente favorita anche dallo sviluppo dei Social Network, in particolare da Facebook, una piattaforma di grandissimo impatto sui consumatori e sul mercato in generale.

Il Consorzio ha compreso il valore di Facebook e la coerenza rispetto ai propri obiettivi promozionali, in particolar modo ha inteso testarlo per la comunicazione e promozione dei propri eventi, e i risultati sono stati molto incoraggianti, al punto da decidere di aprire una propria pagina, nel luglio 2012, e di gestirla e monitorarla internamente, dopo un primo periodo di affiancamento da parte di una società di comunicazione del territorio, che ha aiutato il Consorzio a familiarizzare con lo strumento e ad approfondirne le potenzialità.

Attualmente la pagina Facebook del Consorzio conta 200 fan composti da operatori e da pubblico eterogeneo sia italiano che estero. Viene curata da una risorsa interna sotto la supervisione diretta del Direttore del Consorzio, i due amministratori della pagina. “Va tenuto conto inoltre della sempre maggiore attenzione da parte del mercato estero, confermata a Vinitaly 2012, e le indubbie potenzialità del prodotto, che hanno esortato ancora di più il Consorzio nell’incessante opera di divulgazione anche e soprattutto nei paesi oltreconfine - spiega il Direttore del Consorzio Carlo Veronese - È chiaro che Facebook possa rappresentare anche in tal senso un’importante leva di influenza nella crescita di una cultura internazionale del prodotto e dei brand che lo rappresentano”.

## Il caso Italcementi

### Chi è ITALCEMENTI

Italcementi Group, con una capacità produttiva di oltre 74 milioni di tonnellate di cemento annue, è il quinto produttore di cemento a livello mondiale.

Italcementi, fra le prime dieci società industriali italiane, è quotata alla Borsa Italiana.

Le società di Italcementi Group integrano l'esperienza, il know-how e le culture di 21 paesi in 4 continenti del mondo, attraverso un dispositivo industriale di 55 cementerie, 10 centri di macinazione, 8 terminali, 494 centrali di calcestruzzo e 91 cave di inerti.

Nel 2011 il Gruppo ha registrato un fatturato consolidato di oltre 4,7 miliardi di Euro.

Italcementi, costituita nel 1864, ha avviato nella seconda metà degli anni Ottanta una strategia di internazionalizzazione culminata nel 1992 con l’acquisizione di Ciments Francais.

Dopo una fase di riorganizzazione ed integrazione delle realtà acquisite, a partire dalla seconda metà degli anni Novanta il Gruppo ha rilanciato il processo di diversificazione geografica attraverso una serie di acquisizioni in Paesi emergenti come Bulgaria,

Marocco, Kazakistan, Thailandia, India oltre a operazioni di rafforzamento condotte in Nord America.

Nell'ambito del programma di espansione della presenza nel bacino del Mediterraneo, nel corso del 2005 il Gruppo ha ulteriormente sviluppato la propria presenza in Egitto, diventandone leader di mercato.

Nel 2006, a fianco di nuovi progetti di sviluppo in Kazakistan, è stato acquisito il totale controllo delle attività in India, mentre nel 2007 il Gruppo ha ulteriormente consolidato la sua presenza in Asia e Medio Oriente con operazioni in Cina, Kuwait, Arabia Saudita. All'inizio del 2011 Italcementi ha ceduto la filiale turca Set Group a Limak Holding.

Italcementi, quale membro del WBCSD - World Business Council for Sustainable Development - è tra i sottoscrittori dell'Agenda for Action della Cement Sustainability Initiative, il primo impegno formale che vincola alcune tra le maggiori imprese cementiere al mondo. Ad ulteriore conferma del proprio impegno su questi temi, a Italcementi è stata assegnata la copresidenza della Cement Sustainability Initiative per il periodo 2006-2007.

Inoltre Italcementi è stata inclusa nel "Sustainability Yearbook 2012", la più completa pubblicazione sulla sostenibilità aziendale presentata annualmente da SAM (Sustainable Asset Management). Il Gruppo ha anche aderito all'UN Global Compact, un'iniziativa strategica promossa dall'ONU con l'obiettivo di allineare le azioni delle aziende secondo principi universalmente accettati in termini di diritti umani, ambiente ed etica.

Attraverso le attività dei suoi Centri di Ricerca e Innovazione in Italia e in Francia, i più avanzati in Europa, il Gruppo si propone di anticipare gli orientamenti e le necessità del mercato dando priorità alle questioni ambientali e all'ottimizzazione delle risorse impiegate.

### Italcementi e i Social Network

I trend emergenti in ambito tecnologico, modalità di comunicazione e modelli di servizio che stanno influenzando i principali cambiamenti negli ultimi anni nel mondo IT, unitamente alle esigenze di razionalizzazione dei costi, hanno spinto anche Italcementi ad alcune riflessioni sul tema e ad indirizzare alcuni ambiti di analisi e di pilota, per quanto riguarda l'adozione di soluzioni di mobility, modelli di servizio cloud\saas ed anche Social Network.

Ad oggi quest'ultimo tema è stato affrontato marginalmente e rispetto ai due filoni principali:

- il tema della posizione aziendale ( HR ) rispetto all'utilizzo dello strumento Social in ottica di norme comportamentali e policy di utilizzo per il dipendente;
- il tema delle opportunità di business ( B2B o B2C).

Sul primo aspetto, è stato analizzato il dato che ad oggi, Facebook risulta essere il sito più acceduto anche dall'interno della rete aziendale. Tuttavia questo risultato, che non sorprende vista la popolarità di FB, risulta essere anche di difficile interpretazione rispetto all'utilizzo effettivo del mezzo da parte del dipendente, in quanto la pervasività del servizio FB come servizio integrato ad (o integratore di) altri servizi è tale da rendere probabile la tracciatura di accessi a FB che non si riflettono in un utilizzo prettamente di tipo privato (si pensi anche alle funzionalità di autenticazione via FB, pagine commerciali FB, like-button, ecc...)

Questa considerazione, unitamente alla presa d'atto dell'affermazione dei Social Network come strumenti di comunicazione di massa ed allo sforzo di Italcementi di fare leva sulle nuove modalità comunicative per un rinnovamento anche culturale verso l'innovazione e la comunicazione interna, ha fatto desistere l'azienda dall'idea iniziale di un blocco alla navigazione verso i Social Network.

Rimane tuttavia ancora da sviluppare una formale policy interna che ne regolamenti l'utilizzo ed educhi l'utente sui possibili rischi.

Per quanto riguarda il secondo aspetto, attualmente non è stato sviluppato un piano d'azione per l'utilizzo dello strumento Social Network in ambito Business.

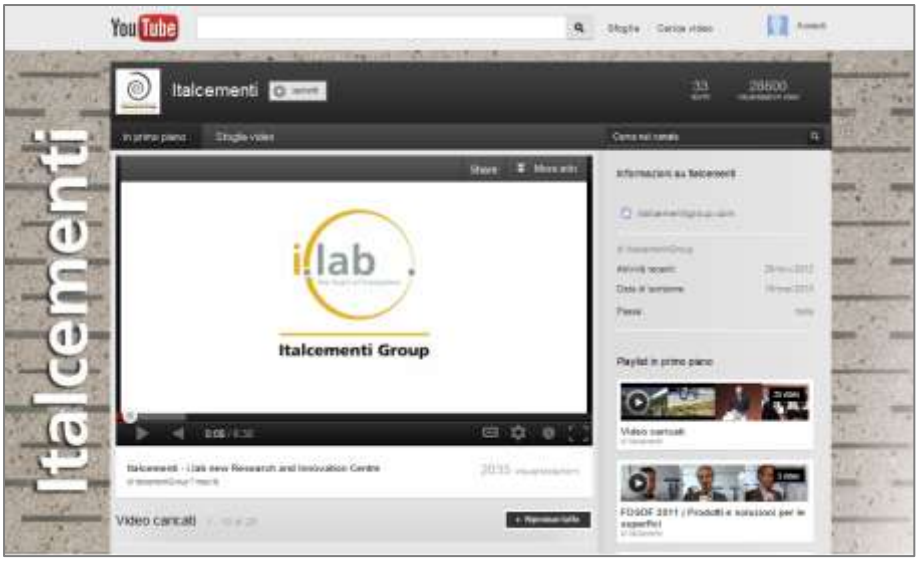
Tuttavia alcune iniziative e idee di sviluppo sono state portate avanti, in collaborazione tra la direzione IT e gli attori interni maggiormente interessati al tema (Marketing/Comunicazione ) che si possono riassumere nei seguenti punti:

- Sfruttare il Social Network per sviluppare una presenza attiva nelle community di quelli che sono per il business Italcementi i principali stakeholder (architetti, ingegneri,…). L'obiettivo è l'acquisizione di "lead" di qualità, da cui far maturare o scaturire opportunità di business. Il tema si applica in modo più sostanziale ai "prodotti speciali", ovvero prodotti utilizzati nell'ambito di costruzioni speciali, finalità artistiche, cementi speciali.. (ad oggi caratterizzati da volumi bassi ma potenzialmente con margini elevati).
- Rivisitare e potenziare i canali di comunicazione già esistenti per acquisire o influenzare il posizionamento generale di Italcementi. E' un tema di carattere marketing e comunicazione, nell'ambito del quale rientra la gestione attuale di un profilo Italcementi sia su YouTube che su Twitter.

La presenza attiva su YouTube si giustifica anche con motivazioni di tipo "reputazionale": il rischio di non presidiare canali così potenti di comunicazione per evitare che lo spazio "pubblico" di questi mezzi venga sfruttato unicamente per veicolare messaggi di tipo negativo o che in qualche modo possano ledere l'immagine dell'azienda o comunque la cui fonte non sia quella ufficiale Aziendale.

Potremmo dire che l'attenzione al presidio dei domini internet "ufficiali" aziendali oggi si sposta (complicandosi) al problema di garantire l'identità della fonte di informazione.

- E' stato attivato di recente un servizio IT basato su un service stile "dropbox". Il servizio risponde alle esigenze di scambi dati e di collaboration di base con utenti esterni. Abbiamo battezzato questo servizio come Social Business, in quanto, per quanto limitato rispetto a un concetto più ampio di Social Networking, è di fatto un primo esempio concreto di utilizzo di un concetto di "Cloud Social Business".
- Per quanto riguarda gli aspetti di security, i rischi principali identificati sono:
  - rischio relativo alla diffusione di informazioni non ufficiali
  - rischio di "sostituzione di identità"
  - rischi IT, questi ultimi principalmente legati al connubio Social Business-Mobility, quindi relativi all'introduzione di nuovi asset informatici (smartphone\Tablet ) e dei concetti BYOD.
- Su questi aspetti i punti di attenzione sono:
  - strumenti di gestione dei dispositivi mobili, che permettono anche il controllo e l'impostazione di policy di sicurezza
  - valutare il contesto da sviluppare per estendere maggiormente un concetto BYOD (aggiornamento della policy aziendale, education degli utenti, soluzioni tecniche )




Pagina YouTube ufficiale di Italcementi. Il profilo viene gestito dalla Direzione Comunicazione Immagine e riporta i video.

## Il caso Roadrunnerfoot

Nel 2007, su spin-off di Politecnico Innovazione, nasce la Roadrunnerfoot che progetta, produce e vende componenti di protesi ortopediche e ausili.

La mission dell'azienda è rendere la tecnologia accessibile all'utenza; infatti la Roadrunnerfoot si propone di ottenere un rapporto qualità/prezzo dei prodotti superiore ai concorrenti presenti sul mercato, realizzando prodotti ad elevato standard qualitativo, altamente prestazionali, fabbricati con materiali innovativi, ma contenendo i costi. I prodotti e la loro fabbricazione sono assolutamente MADE in ITALY, facendo della Roadrunnerfoot Engineering S.r.l. l'unica azienda Italiana che progetta e produce del settore ortopedico.

*"Rispetto ad una normale strategia di marketing, di fronte all'universo web è fondamentale stabilire delle "ancore" e delle linee direttrici in quanto la possibilità di perdersi è banalmente molto più facile".*

## L'azienda

Il brand della Roadrunnerfoot è fortemente legato alla personalità del **fondatore**, Daniele Bonacini, network aziendale e network individuale devono dunque andare di pari passo, il risultato è che si confondono spesso, rimanendo sempre legati ad una scelta iniziale dello strumento dettata dalla tipologia dell'interlocutore e lasciando poi ad esso la possibilità di interagire dove, come e quando desidera.

Es.:

- www.facebook.com/danielebonaciniroadrunner
- www.facebook.com/Roadrunnerfoot
- http://www.linkedin.com/in/danielebonacini
- www.linkedin.com/company/roadrunnerfoot-engineering-srl.

La Struttura dell'azienda è composta da: Direzione, progettazione, qualità, Corporate Social Responsibility, Commerciale, Logistica. L'area commerciale è strutturata per area geografica: Italia (minima), Europa, Latino-america, Russia ed Est Europa, Medio oriente. La struttura dell'azienda porta dunque l'interlocutore ad identificarla in modo differente: ad esempio, per il cliente mediorientale, sarà fondamentale il binomio Commerciale Medio oriente – CEO. Più la comunicazione sarà impostata su questo binomio più il cliente si sentirà seguito. Al fine di personalizzare la comunicazione è necessario che tutto lo staff possa gestire autonomamente i Social Media. Il settore Corporate Social Responsibility, occupandosi di donazioni, sponsorizzazioni, forniture umanitarie a costo di produzione, necessita di rimanere sempre ben distinto dal ramo commerciale, onde evitare di nuocere all'azienda invece di darle visibilità.

Gli Influencers sono giornalisti e atleti, utenti molto attivi nei Social Media, medici. Deve esserci una costante comunicazione con questi soggetti, tramite i loro blog e i Social Network, individuati sia a livello nazionale che internazionale (Cimmino, A nuoto nei mari

del globo, dall'Africa a Boston all'Italia, Travel for Aid- wordpress ,il ciclista Tricarico, Alex Zanardi, il blog, Bomprezzi Vita e Corriere della Sera, blog Simferweb della medicina in riabilitazione, blog di ortopedici, etc.). Il fondatore dell'azienda non ha né può gestire un blog personale per motivi di tempo, di fronte al proliferare di blogs e canali di comunicazione, mantenere una presenza su quelli esistenti è più semplice ed efficace.

## Il prodotto

Specificità del prodotto PROTESI, ORTESI, TUTORI, CARROZZINE, AUSILI SPORTIVI e mercato "di nicchia" (AMPUTATI)

## Il mercato

1. Roadrunnerfoot non vende direttamente all'utenza, deve dunque rivolgersi sia ai tecnici che agli utenti. Lo sviluppo dei social media è la perfetta soluzione trovando network sia propri di una categoria (es. pubblicazione scientifiche o d'altra parte community di utenti) sia di entrambe.
2. Il mercato italiano è di secondaria importanza, i mercati obiettivo sono molto diversi anche nel web

   - ITALIA, WEST EUROPE
   - US, LATIN AMERICA
   - RUSSIA, EST EUROPE
   - MIDDLE EAST
   - CHINA E SOUTHEST ASIA.

热点图中，红色表示用户点击密集、橙色次之、绿色表示点击较少

Esempi: I clienti dell'America Latina utilizzano i medesimi nostri Social, gli americani utilizzano più Twitter di altri Social, puntando ad una comunicazione più diretta, i russi hanno il loro Facebook , i clienti medio orientali privilegiano sempre un contatto diretto, telefonico, in Cina come in Russia i Social Media sono totalmente differenti.

E' fondamentale l'utilizzo della lingua del paese, il referente dell'azienda deve dunque saper gestire autonomamente il network del suo paese.

### Linee guida

Roadrunnerfoot ha impostato la sua presenza nei Social Network creando dei «contenitori», degli spazi, ove utenti e altri soggetti possano parlare dell'azienda e dei prodotti.

Dalla creazione dei profili a fine 2010 assistiamo oggi ad un naturale incremento del traffico che porta ad un monitoraggio costante e ad attività pianificate. I contatti non vengono più cercati ma gli utenti cercano Roadrunnerfoot.

Avendo percentuali elevate di export in paesi che non rispondono ai medesimi «appelli Social» l'azienda è passata da uno staff «ghost writer» al management autonomo dei diversi canali da parte dello staff.

La principale attività di Roadrunnerfoot è stata intervenire nelle Communities pertinenti, finalizzata alla creazione di conversazioni tra utenti /consumatori - altre aziende/fornitori

Elenco delle tipologie di communities cui RRf partecipa

- Community es. business 7pq, innovazione e imprese Italia degli innovatori, start up, auriga (vetrina made in Italy ICE), business link UK, etc.
- Community mirate es. ausili siva – eustin europa, medicali, tecniche oandp
- Community locali es. regione Lombardia , portali made in Italy es. italmarket
- Community sport platform beyond sport, running, podisti, etc
- Community CSR, community cooperazione (yahoo groups)
- Community utenti the best: US amputees, etc. in Italia le donne amputate spesso scrivono per problemi di estetica sui forum femminili.

Criticità: le Communities di amputati in Italia, per barriere culturali, non hanno sviluppo: ogni community pertinente è dunque un «contenitore» ove confluiscono queste voci.

Per i Social Media valgono alcuni paradigmi:

| ***I must*** | ***Trend/Variabili*** |
|---|---|
| 1. Creatività (contenuti)<br>2. Spontaneità<br>3. Aggiornamento/Feedback (engagement)<br>4. Monitoraggio (target) | 1. New ideas (US)<br>2. Stats about customers (Neilse, etc, …)<br>3. Coinvolgimento staff |

Aggiornamento significa non solo inserire news, interviste ed eventi (idealmente crearli anche quando non sussistono) ma anche valorizzare le news e gli eventi creando delle campagne ad hoc o continuando a postare notizie.

DANIELE BONACINI – PROFILO PERSONALE – join facebook oct. 2010

422 friends, aumentano ormai giornalmente, tra gli amici: ortopedici, colleghi, giornalisti, utenti, cliniche, di diverse aree geografiche. La crescita è stata determinata dal traffico generato indirettamente, per scelta. I post diretti da 1 a settimana tendono ormai a 5-6 al giorno.

Facebook Roadrunnerfoot – pagina «vetrina», le foto postate infatti determinano il traffico - joined Facebook oct. 2010 – il profilo rimarrà tale fino all'inizio di campagne ad hoc, per scelta.

Le statistiche fornite da Facebook vengono al momento utilizzate per controllare chi parla dell'azienda e in che termini, seppur tuttavia lo strumento sia veramente poco sviluppato. Per una verifica della web reputation in realtà l'unico strumento attuale è creare un'identità ad hoc che partecipi ai network altrui (l'azienda ne ha due).

Il profilo YouTube è sempre esistito dalla nascita dell'azienda ma solo oggi che l'azienda è sui diversi social media, questo canale sta portando nuovi contatti e visite.

I principali obiettivi e risultati conseguiti con LinkedIn riguardano l'attività dei gruppi, il settore sport e i developing countries.

Il profilo Flickr è una «vetrina» di presentazione più interattiva e informale di LinkedIn, l'azienda lo utilizza per le gallery sportive soprattutto. Anche i progetti di cooperazione internazionale possono essere valorizzati tramite questo canale.

Su Twitter la partecipazione è minima ma mirata (es. Twitter arabi nella giornata per le persone con disabilità). I principali obiettivi sono il mercato statunitense e le personalità che per l'azienda risultano influenti.

### Considerazioni sul caso

In Roadrunnerfoot non ci sono Social Media Policy formali ma i ruoli sono molto chiari, la condivisione è di prassi, non c'è spazio per i solisti, la Direzione è presente.

I Sistemi Informativi gestionali sono minimali e accessibili solo alla Direzione e alla Logistica; quest'ultima non è attiva sui Social Network. Amministrazione e paghe sono in service. In pratica c'è una barriera organizzativa oltre che tecnologica, tra l'Informazione Aziendale e la nuvola.

I Commerciali vivono su Internet, il fatturato è al 95% all'estero (Europa dell'EST, Africa, Asia, America) e l'attività commerciale è svolta dalla sede di Milano. La loro età media non arriva a 30 anni, nessuno è italiano e ognuno ha una lingua madre diversa. Essendo il cliente finale un disabile ed il prodotto un Dispositivo Medico soggetto alle disposizioni e ai controlli del Ministero della Sanità e alle Normative Normalizzate specifiche, è nel DNA di tutti l'attenzione all'informazione sensibile. Nessun riferimento / foto / filmato, viene postato o pubblicato senza un consenso formale del "titolare". Nessun prodotto viene anticipato al mercato prima del rilascio, da parte del Ministero, del certificato di libera vendita. A rafforzamento dell'attenzione della Direzione, l'area commerciale è sotto la responsabilità funzionale e gerarchica dell'Amministratore Unico.

La nuvola è il luogo virtuale dove si lavora, è molto serio e da trattare con professionalità e molta attenzione. E' lì che si trovano nuovi clienti, che si accresce la visibilità del marchio, che si trovano opportunità di finanziamento per il Sociale, avvisi per bandi e fiere, e dove si ascoltano le esigenze del cliente.

## Il caso Cesari

Umberto Cesari è stata la prima azienda privata in Emilia Romagna a credere nelle grandi potenzialità del vitigno Sangiovese e ha fatto da sempre del Sangiovese di qualità la propria filosofia produttiva. Questo fattore ha portato l'azienda a esportare i propri vini nel mercato americano fin dai primi anni '80.

La storia dell'Azienda, dal lontano 1965 ai giorni d'oggi, è quella di una famiglia intera, impegnata attivamente e quotidianamente nella sua crescita, nel suo sviluppo e nel suo successo.

L'azienda è situata sulle colline che dominano l'antica Via Emilia, al confine tra Emilia e Romagna, ad una altitudine che varia dai 300 ai 450 metri sul livello del mare, in località Castel San Pietro Terme.

Gli originari 20 ettari del primo podere, da cui ha preso avvio l'attività nel 1965, si sono ampliati negli anni raggiungendo attualmente i circa 140 ettari dove sono coinvolti un totale di 30 dipendenti.

Oggi l'azienda Umberto Cesari comprende cinque poderi: Casetta, Parolino, Ca' Grande, Laurento e Tauleto, in cui si producono annualmente circa 2.800.000 bottiglie, distribuite in più di 50 paesi. L'80% della produzione viene esportata all'estero: tra Stati Uniti, Messico, Caraibi per il 50%; Europa per il 30%; restante 20% nei restanti paesi.

### Umberto Cesari e i Social Network

Umberto Cesari ha fatto il suo ingresso nel mondo dei Social nel 2009, quando molte aziende ancora non conoscevano le potenzialità di questo strumento di comunicazione. L'azienda ha iniziato la sua avventura sui Social Network con l'obiettivo farsi conoscere e promuovere i propri prodotti e la propria attività attraverso nuovi canali, ma soprattutto con l'intento di creare un dialogo con i clienti/utenti, di coinvolgerli e far si che essi stessi diventassero ambasciatori del brand. In particolare l'approdo ai Social Network è avvenuto parallelamente all'ingresso in azienda di persone giovani che hanno fatto comprendere alla direzione la necessità di restare al passo con i tempi e di presidiare questi nuovi canali strategici per la comunicazione, in particolare per parlare ad un pubblico abbastanza giovane, sul quale l'azienda aveva deciso di focalizzarsi. Uno degli scopi che ha contribuito alla decisione di entrare nei Social Network è stato la necessità di ringiovanire l'immagine dell'azienda e il suo stile di comunicazione.

### *Il Social Network come influisce nella vostra immagine aziendale e sulla conservazione del Made in Italy? Quali sono le vostre aspettative?*

La redazione e la gestione di tutti i contenuti condivisi nei Social viene fatta internamente a cura dell'Ufficio Marketing, per garantire che quanto viene comunicato risulti fedele e coerente rispetto ai valori aziendali.

I primi Social Network che l'azienda ha esplorato sono stati Twitter, Facebook e You Tube, a seguire l'azienda ha creato profili pubblici anche su Instagram e Pinterest.

Il canale che raccoglie il maggior numero di persone e che ha dato più soddisfazioni, in termini di numero di fans, è sicuramente Facebook. Ad oggi i fan sono circa 6600: questo numero è notevolmente aumentato negli ultimi quattro mesi grazie a una campagna di ADV. La pagina Facebook viene aggiornata quotidianamente e i contenuti che vengono postati sono relativi a: informazioni storiche che riguardano i vitigni, informazioni sui prodotti (lancio di nuovi prodotti o vittoria di un premio), presenza dell'azienda a eventi, vignette umoristiche sul mondo del vino, ricette presenti sul sito (generalmente al venerdì), consigli su come riciclare i tappi di sughero e informazioni che riguardano le fasi dell'attività produttiva dell'azienda (ad esempio la vendemmia).

I post vengono sempre corredati da una foto e si cerca di scrivere una frase che inviti l'utente a interagire: l'obiettivo non è solo quello di informare chi segue la pagina, ma soprattutto di dialogare con i fan (per questo motivo si è scelto di rispondere sempre ai commenti) e di far si che i contenuti postati arrivino al maggior numero di persone possibile (ovvero che vengano condivisi). Chiaramente la percentuale dei commenti e delle condivisioni è molto bassa, ma quando i fans postano dei contenuti si tratta sempre di commenti positivi.

Tra le interazioni spontanee dei fans vanno ricordate anche le numerose richieste di informazioni su dove poter trovare i prodotti. I post che hanno più successo sono quelli relativi ai prodotti o a contenuti umoristici. Facebook si è rivelata inoltre la terza sorgente di traffico al sito (dopo gli accessi diretti e quelli da google, che la fanno da padroni), nel mese di settembre, per esempio, ha generato il 2.5% degli accessi.

Twitter è il secondo Social per numero di follower (225). Anche in questo caso, l'azienda cerca di twittare almeno tutti i giorni mettendo contenuti diversi rispetto a quelli presenti su Facebook. Anche in questo caso ci sono stati molti riscontri positivi. Sia per Facebook

che per Twitter è capitato spesso che le persone condividessero i momenti importanti della propria vita in cui i vini Umberto Cesari sono stati protagonisti.

Instagram e Pinterest sono gli ultimi Social Network a cui l'azienda si è avvicinata e stanno iniziando a dare risultati positivi. Su Instagram Umberto Cesari pubblica, almeno un paio di volte a settimana, foto scattate in azienda oppure ad eventi ai quali partecipa. Su Pinterest invece vengono inseriti contenuti che sono presenti sul sito web oppure che vengono ripresi dal web; per il momento sono state create 10 board dove vengono condivise immagini relative ai prodotti, ai vigneti, alle ricette tipiche emiliano – romagnole, al riciclo e immagini divertenti sul vino.

La nazionalità dei fan è molto variegata: le comunità più presenti sono quella italiana (circa il 28% del totale), quella messicana (28%) e quella serba (16%). Importanti sono anche le rappresentanze di Singapore, Hong Kong, Canada, Regno Unito, Belgio, Germania e Stati Uniti. La maggior parte della produzione dell'azienda viene venduta all'estero e, considerando che solitamente gli utenti sono fan di brand che conoscono, o di cui acquistano i prodotti, è coerente che la maggior parte non siano italiani. I Social Network da questo punto di vista rappresentano una risorsa preziosa per il marketing, poiché consentono di entrare in contatto diretto con un cliente finale, quello straniero, che altrimenti sarebbe difficilmente raggiungibile.

La pagina Facebook e gli account su tutti gli altri Social Network costituiscono per Umberto Cesari un modo per promuovere l'eccellenza della regione, la sua cultura enogastronomica e il Made in Italy. L'approccio strategico che ha guidato l'attività di promozione off-line dei vini Umberto Cesari all'estero è lo stesso seguito nella promozione del brand on-line: in vino è un prodotto intrinsecamente legato al luogo in cui nasce e alla sua cultura, non si può promuovere l'uno senza valorizzare anche il resto. E così sui nostri profili parliamo di cucina, di artigianato e di territorio, contribuendo a far conoscere all'estero ciò che di buono e di bello c'è nel nostro Paese.

### *Quali sono le modalità adottate in azienda per gestire e controllare tale attività in modo sicuro?*

I profili dell'azienda sui Social Network vengono gestiti da un gruppo ristretto di personale dell'ufficio marketing che ha il compito di selezionare, presidiare e controllare le informazioni aziendali che transitano sui Social Network ed in particolare sui gruppi ufficiali aziendali.

Questo permette di garantire un presidio della reputazione aziendale sui Social, sia in termini di diffusione di informazioni aziendali ritenute di dominio pubblico, sia in termini di risposta ad eventuali lamentele o azioni che possono danneggiare l'immagine aziendale. Il personale incaricato svolge inoltre un controllo periodico di ricerca, sui Social e sul Web, di conversazioni o commenti che riguardino Umberto Cesari.

Questo controllo viene realizzato monitorando, nei motori di ricerca oppure nelle opzioni di ricerca dei principali Social (come Twitter o Pinterest), i risultati per ricerche di parole chiave come "Umberto Cesari" o "sangiovese Cesari": in questo modo è possibile risalire ai commenti sull'azienda che non vengono pubblicati nei profili aziendali. Ad oggi l'azienda non ha riscontrato tramite i Social casi di diffamazione dei prodotti o diffusione indebita dei dati aziendali.

# APPENDICI

## Indice delle figure

Figura 1 - utilizzo dei social media....8
Figura 2 – Andamento dell'e-commerce B2C....9
Figura 3 – Utenti dei Social Media per Paese....9
Figura 4 – Penetrazione dei Social Media per Paese....10
Figura 5 – Fan Facebook dei marchi italiani....10
Figura 6 - i Social Media oggi e in prospettiva (Mckinsey 2012)....11
Figura 7 - Social Media e valore aggiunto alle imprese....17
Figura 8 - Benefici ottenuti dall'uso di Social Media....18
Figura 9 – Processo di adozione di una stregia social....50
Figura 10 - Il caso "Patrizia Pepe"....57
Figura 11 - Rischi tecnologici: tabella probabilità/impatto....59
Figura 12 - Principali fonti di rischio (7-alto 1-basso)....60

## Note e fonti

1. Symantec, *Symantec's Social Media Protection Flash Poll* - http://www.symantec.com/about/news/release/article.jsp?prid=20110721_01

2. World Economic Forum, *Global Risks 2012 - Seventh Edition*

3. Ponemon Institute, *"The impact of cybercrime on businesses"* - http://www.ponemon.org/local/upload/file/Impact_of_Cybercrime_on_Business_FINAL.pdf

4. NM Incite, *The Social Media Report 2012* - http://nmincite.com/download-the-social-media-report-2012/

5. McKinsey Global Institute Research, *The social economy: Unlocking value and productivity through social technologies, 2012* - http://www.mckinsey.com/insights/mgi/research/technology_and_innovation/the_social_economy

6. Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione nei siti web esclusivamente dedicati alla salute - 25 gennaio 2012 (Pubblicato sulla Gazzetta Ufficiale n. 42 del 20 febbraio 2012) http://www.garanteprivacy.it/garante/doc.jsp?ID=1870212

7. Formez, Linee guida Pubblica amministrazione e Social Media, 2012

8. Nielsen, http://nielsen.com/content/dam/nielsen/en_us/documents/pdf/Fact%20Sheets/NetView_US.pdf

9. FONTE - Libro: Product Innovation e Market Creation; Autori: Vicari, Cillo, Raccagni; Casa editrice: Egea Tools.

10. Provvedimento Tribunale Torino 7 luglio 2011 che identifica nel nome di un gruppo Facebook un "segno distintivo atipico" e, come tale, lo tutela (il provvedimento

è disponibile all'url http://www.personaedanno.it/attachments/allegati_articoli/AA_022237_resource1_orig.pdf)

11. Instagram, il noto Social Network attraverso cui gli utenti condividono le proprie foto, nel mese di dicembre 2012 ha annunciato l'intenzione di adottare nuovi termini di servizio che consentivano al gestore di vendere le immagini caricate dagli utenti senza riconoscere a questi ultimi alcun pagamento nè la possibilità di opporsi a tale cessione. Dopo tale annuncio, diversi professionisti e aziende hanno deciso di chiudere il proprio profilo al fine di evitare che si verificasse tale evenienza.

12. Social Media Marketing all-in-one for dummies – J. Zimmerman – Wiley, 2010

## Autori e contributori

Questo lavoro è frutto della collaborazione delle seguenti aziende, studi legali e associazioni.

Abeti
Studio Legale
ADS
Gruppo Finmatica
a process enabling IT company
BSC
CONSULTING
CBA
STUDIO
LEGALE e TRIBUTARIO
CSQA
CSQA
DIGITAL
MAGICS
eLEX
ERNST & YOUNG
Quality In Everything We Do
iDIALOGHI
ICT Security & Consulting
KPMG
cutting through complexity
Michael Slim International
Investigation Security & Intelligence
ORACLE
protiviti
Risk & Business Consulting.
Internal Audit.
Reply
spike
The Innovation Group
ZEROPIU
Difference as value
BLOG

## Team leader ed editor

**Fumagalli Sergio**, ZEROPIU - VP, marketing, relazioni esterne e partnership. Responsabile attività di consulenza sulla Privacy, coautore di “Privacy guida agli adempimenti”, Ipsoa 2005

**Gatti Francesca**, AUSED - CISA, CGEIT, Consiglio Direttivo AUSED, Coordinatrice dell’Osservatorio Sicurezza e Compliance di AUSED.

**Obialero Roberto**, ADS - Gruppo Finmatica - Business Development IT Security & Infrastructures, GCFA, GCFW

**Piazzese Rosario**, THE INNOVATION GROUP - Partner. Docente su tematiche di management e governance dei sistemi informativi presso accademie e università internazionali, è autore di pubblicazioni su Cloud, GRC e processi di allineamento strategico.

**Vallega Alessandro**, Oracle - Security Business Development Manager, Consiglio Direttivo Clusit, Coordinatore della Oracle Community for Security

**Zapparoli Manzoni Andrea**, iDialoghi - Presidente, Security Brokers - General Manager, Consiglio Direttivo Clusit, Consiglio Direttivo Assintel, Coordinatore GdL ICT Security Assintel, Membro Osservatorio per la Sicurezza Nazionale (OSN)

## Autori e contributori

**Abeti Riccardo**, Studio Legale Abeti - Membro del Comitato Esecutivo e Presidente della Commissione “New Technology, Personal Data and Communication Law” dell’Unione Avvocati Europei. Specializzato nel diritto delle nuove tecnologie.

**Albanese Andrea**, Social Network & Web Marketing Process Advisor, Sales & Post Sales Process Optimization; Web Business Intelligence & Real Time Customer behavior. Docente Master SNID Politecnico Milano. Collaboratore SDA Bocconi

**Alovisio Mauro**, Università di Torino; Avvocato; Fellow del Centro di ricerca su Internet e società Nexa del Politecnico di Torino; Presidente dell’associazione Centro studi di Informatica Giuridica di Ivrea-Torino

**Baduini Gabriele**, Spike Reply - Manager e Direttore Tecnico BU Roma

**Belisario Ernesto**, e-Lex, network di studi legali specializzati in diritto delle nuove tecnologie - avvocato, specializzato con lode in Diritto Amministrativo e Scienza dell’Amministrazione

**Bernardi Bruno**, CSQA Certificazioni - Responsabile Divisione Tecnologie e Sicurezza ICT

**Borgonovo Alberto**, KPMG Advisory S.p.A - Manager, Information Risk Management. CISA, CRISC, L.A.ISO27001, Prince2 Foundation, ITIL Foundation, OPST, socio ISACA e AIEA

**Castello Andrea**, CSQA Certificazioni - Responsabile schemi di Certificazione, Divisione Tecnologie e Sicurezza ICT

**Ferrara Marco**, KPMG Advisory S.p.A – Senior Consultant, Information Risk Management

**Ferretti Enrico**, Protiviti - Director, è responsabile dell’offerta di Information Security per Protiviti Italia. Certificazioni: CISA, CGEIT, CRISC, LA ISO27001, PCI-DSS QSA. Membro AIPSA, Membro AIEA

**Fioravanti Alberto**, DigitalMagics - Digital Magics S.p.A. Fondatore e Venture Partner

**Galimberti Matteo**, BSC Consulting - Solution Account Manager

**Gargano Antonello**, Protiviti - Manager, gestisce i servizi di consulenza in ambito Technology Risk Consulting per Protiviti Italia. Certificazioni: CISA, PCI-DSS QSA. Membro AIEA

**Giordano Davide**, Spike Reply - Senior Security Consultant

**Girolimetto Martina**, CSQA Certificazioni - Marketing & Comunicazione

**Lee Jun Woo**, KPMG Advisory S.p.A - Professional, Information Risk Management. CobiT 4.1 Foundation

**Leiweke Dominick**, THE INNOVATION GROUP - Jr IT Consultant e studente del Master of Science in Economics and Management of Innovation and Technology in Bocconi, Milano.

**Magri Michele**, Michael Slim International – CEO Michael Slim International – Digital investigation, Security, Intelligence. Certificazioni: CFE, ECCE. Membro del Board CFE Italy Chapter.

**Mariotti Andrea**, Ernst & Young - Director IT Risk & Assurance Services, CISA, CISM, CRISC, Lead auditor ISO27001, Lead Auditor ISO20000, socio AIEA e AIPSA

**Mecozzi Rodolfo**, Ernst & Young - Senior Manager IT Risk & Assurance Services, ITIL v3 Foundation Certificate

**Morato Matteo**, Ernst & Young - Senior Consultant IT Risk & Assurance Services

**Ongaro Riccardo**, AUSED - ICT Security and Architect

**Parisi Roberto**, Eretici - è nato a Vignola (Modena). Più volte ex ma mai pentito, vive e lavora a Milano nell'agenzia di pubblicità *Parisi Ferrandi: Eretici* (www.eretici.it*)* e in *Roberto Parisi: SE*, gruppo di lavoro dedicato all'analisi, interpretazione e influenza degli scenari politici e dei mercati.

**Pellicano' Gerolamo**, Studio Legale e Tributario CBA - avvocato cassazionista, è of Counsel di CBA Studio Legale e Tributario. Come deputato ha presentato nel 1991 una delle prime proposte legislative per la tutela dei dati personali.

**Prampolini Natale**, AIEA - ICT Strategy Architect, Senior Security Consultant, LA ISO27001, ISO20000, CISA, CISM, ITIL v.3, CMMI 1.2 DEV, Socio e Proboviro AIEA

**Quaroni Laura**, KPMG S.p.A. - Manager, Information Risk Management. CISA, CISM, CRISC, L.A.ISO27001, L.A. BS25999, Prince2 Foundation, ITIL Foundation, socio ISACA e AIEA

**Scozzari Sofia**, iDialoghi - Chief Operating Officer; Security Brokers - Social Business Security B.U. Director

**Seminaroti Paola**, Protiviti - Consultant, è coinvolta nei servizi di consulenza in ambito Technology Risk Consulting per Protiviti Italia

# SICUREZZA
## E SOCIAL NETWORK