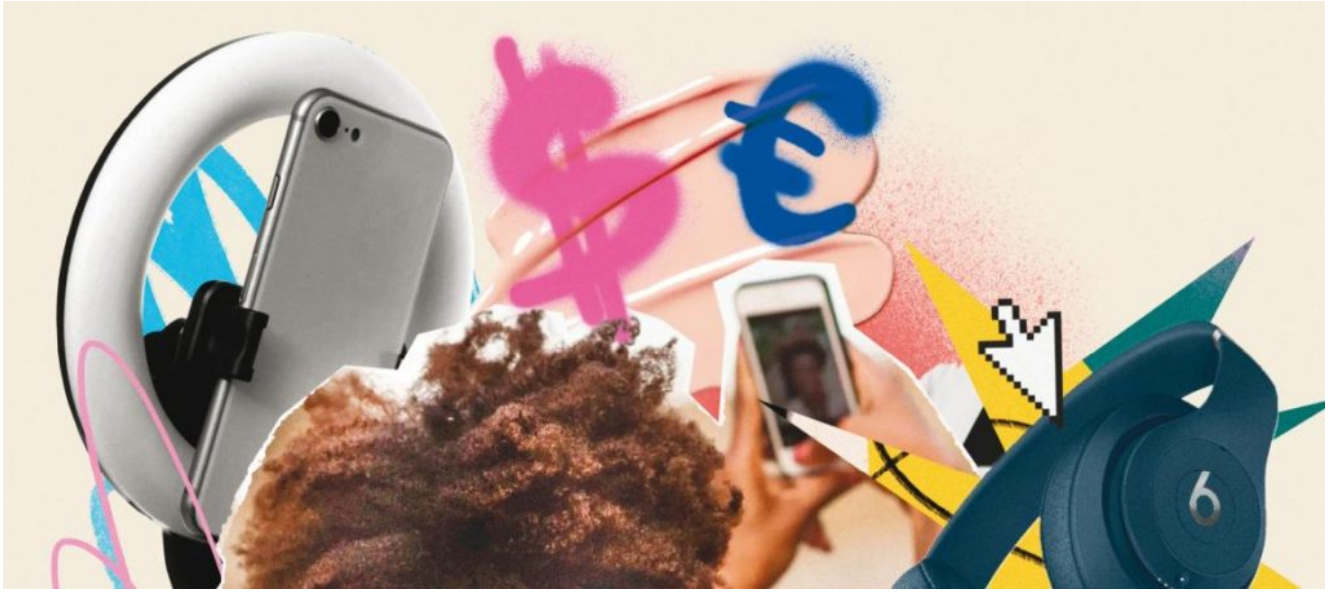
Carabinieri: un nuovo Digital Body cattura l’attenzione delle giovani generazioni e ridisegna la percezione online dell’Arma

“Ma che sta succedendo all’account Instagram del Carabinieri?”, si è chiesta l’Italia intera in questi mesi. Ce lo siamo chiesti anche noi, ed ecco le risposte

---

Vincere nell’influencer

marketing



PERCHÉ IL BUSINESS DEGLI INFLUENCER HA BISOGNO DI LIMITI

E come professionalizzare una pratica ancora in fase di maturazione

---

La goffa (ma efficace) disinformazione russa per far vincere Trump

Dietro le fake news sui gatti mangiati a Springfield e i legami immaginari tra Kamala Harris e il comunismo ci sono i servizi segreti russi che sfruttano ampie reti automatizzate di bot e duplicati falsi di articoli originali, reclutando anche influencer apparentemente inconsapevoli

---

Conti correnti “spiati” e crisis managament di Intesa San Paolo: alla ricerca

dell’autenticità perduta

Cosa è successo

Per i – pochissimi, immagino – che non avessero seguito la cronaca di questi giorni, la procura di Bari ha avviato un’indagine su *Banca Intesa Sanpaolo* a seguito del caso di Vincenzo Coviello, dipendente della filiale di Bitonto, in provincia di Bari, accusato di aver ficcanasato nelle reti aziendali violando i dati bancari di migliaia di persone, tra cui politici e personaggi molto noti, dalla Presidente del Consiglio Giorgia Meloni al Ministro della Difesa Crosetto, da Mario Draghi a Luca Zaia, ma anche Procuratori della Repubblica, ufficiali dei Carabinieri e della Guardia di Finanza, diversi cantanti e influencer, e chi più ne ha ne metta.

Denunciato lui, indagata però anche la banca: avrebbe violato la ben nota – per gli addetti ai lavori – Legge 231/01 sulla “responsabilità amministrativa delle persone giuridiche”, non informando le autorità in maniera tempestiva sugli accessi

compiuti dal proprio dipendente in violazione dei dati dei clienti della banca stessa. Un modello che in Banca Intesa esiste, é sorvegliato da un Organismo di Vigilanza composto da professionisti di primissimo piano e grande competenza, ma che probabilmente – alla prova dei fatti – avrebbe mostrato qualche limite, se non altro per come il management della Banca l'ha applicato, circostanza inspiegabile per un colosso di quelle dimensioni.

I numeri del dossier

Oltre 7.000 mila accessi abusivi sui conti di 3.572 clienti sparsi in 679 filiali in tutta Italia, effettuati tra il febbraio del 2022 e l'aprile del 2024, data nella quale il dipendente infedele sarebbe stato formalmente sospeso dall'incarico (ma torneremo su questo più avanti nell'articolo), per venir poi licenziato lo scorso 8 agosto, al termine di un procedimento disciplinare interno.

Movimenti dei conti correnti, bonifici in entrata e in uscita, importo dei depositi e degli investimenti, prelievi dei Bancomat e utilizzo delle carte di credito: nulla sarebbe sfuggito al ficcanaso reo-confesso, e per questo gli avvocati dei Clienti "spiati" affilano i coltelli e preparano cause per danni a carico della banca, che – oltre che dover "pagar pegno" dal punto di vista finanziario e patrimoniale – non ne uscirà benissimo neppure da quello reputazionale.

Motivazioni, mandanti ed eventuali responsabilità

Coviello si sarebbe difeso adducendo a semplice (sic!) "curiosità morbosa", ma gli inquirenti passano al setaccio il web e i dispositivi elettronici: c'è un mandante, e/o le informazioni sono state rivendute a qualcuno, oppure sono state trasferite a terzi? La Procura sospetta che Coviello abbia agito (cito verbatim il provvedimento dei PM)

“verosimilmente in concorso – e previo concerto – con persona/e da identificare”: quindi l’ipotesi è che esistano presunti mandanti degli accessi abusivi ai sistemi informatici della banca.

Il giallo si dipanerà sicuramente nelle prossime settimane, e i mass-media non mancheranno di aggiornarci, ma ciò che pare più inquietante è che Coviello avrebbe continuato a spiare i conti, come se nulla fosse accaduto, anche dopo le prime contestazioni: dagli atti della banca emergerebbe che dal novembre 2023 (data dell’avvio delle verifiche interne) ad aprile 2024 (data della sospensione dall’incarico) il dipendente infedele avrebbe eseguito ulteriori 347 accessi abusivi, interrogando i conti di 261 clienti da lui non gestiti.

E – clamoroso – la banca non avrebbe potuto, o saputo, impedirlo.

I precedenti

Questa banca parrebbe non essere nuova al mancato presidio dei rischi reputazionali: nel recente passato, Intesa Sanpaolo e Isybank, la banca digitale del gruppo, sarebbero finite sotto la lente delle Autority per aver comunicato in maniera “*ambigua*” a centinaia di migliaia di correntisti “*con modalità che non sembravano coerenti con l’importanza della questione trattata*” – il trasferimento dei loro conti correnti dalla prima, controllante, alla seconda, controllata.

È quanto si leggeva in una nota diffusa dall’Antitrust riguardo quella vicenda, a seguito dell’avvio di un procedimento istruttorio generato dalle segnalazioni pervenute da oltre 2.000 correntisti, evidentemente contrariati dal modo di procedere dell’istituto, accusato non solo di aver “traslocato” i conti senza chiedere il consenso dei correntisti, ma anche di aver apportato, con l’occasione (e con scarsa trasparenza, secondo l’Autority) “*importanti*

modifiche delle condizioni contrattuali e delle modalità di fruizione del servizio", nonché generato un aumento dei costi di tenuta del conto a carico dei clienti.

Insomma, in quanto a relazioni con gli stakeholder, gli spazi di miglioramento parrebbero più che evidenti, e la reputazione della banca avrebbe già dovuto scricchiolare. O forse no: vediamo perché.

L'atteggiamento (benevolo) dei mass-media

Molto pungente l'analisi di "Morning", l'eccellente podcast quotidiano condotto da Francesco Costa: secondo i redattori de Il Post, *"…forse non è un caso che siano Il Fatto, Domani e Il Manifesto i tre giornali che dedicano più spazio e aggiornamenti alla storia del dipendente di Intesa Sanpaolo (…), i giornali con il minor numero di inserzioni pubblicitarie ogni giorno, e quindi tra quelli che ricevono meno denaro dagli inserzionisti pubblicitari".*

E Intesa San Paolo, si sa, è un inserzionista pubblicitario che muove cifre enormi. Per motivi forse opposti e speculari, in questo periodo di concitati aggiornamenti sulla vicenda, in diverse sue edizioni un importante quotidiano non ha fatto minimamente menzione, nemmeno con un piccolo box – prosegue Costa – e quel giornale *"è La Stampa, il quotidiano di Torino, dove* (incidentalmente, ndr) *ha sede Intesa Sanpaolo. Uno si aspetterebbe di trovare sul giornale di Torino gli aggiornamenti più completi, approfonditi e informati su una questione così vicina a quel giornale, a quella città, a quella redazione. E invece è proprio il giornale che non bisogna guardare, purtroppo, se si vogliono avere notizie sull'accaduto*", conclude Costa.

Maligni, questi de Il Post. Ciò detto, come ha reagito alla crisi Intesa San Paolo?

Il caso, sotto il profilo del Crisis management

La riflessione – lato comunicatori e relatori pubblici – è quindi la seguente: qual è stato esattamente il grado di responsabilità dell'istituto di credito, e quindi quale sarà l'impatto sul perimetro reputazionale di Intesa San Paolo?

Se lo chiedono in molti, considerando che non più tardi dell'anno scorso, la banca risultava ai vertici della Top 20 dell'ESG Perception Index, l'osservatorio sulla reputazione di sostenibilità (che peraltro pare non azzeccarci molto, se consideriamo che anche la Giorgio Armani Operation, recentemente commissariata dal Tribunale di Milano, era ben posizionata in quella classifica).

La banca – nei propri comunicati ufficiali – si dice costernata, e dichiara *"di aver fatto tutto il possibile per intervenire sollecitamente e limitare i danni nell'interesse dei correntisti e degli azionisti".*

Tuttavia qualcosa non torna, e per un motivo molto semplice: perché Intesa avrebbe lasciato Coviello in condizione di continuare a spiare per altri mesi, nonostante sapesse che i fatti descritti configurassero una violazione delle normative di norme aziendali (e non solo) riguardanti la privacy…?

E ancora: se l'istituto aveva contezza della gravità dello scenario, perché si è mosso così tardi? Forse – denuncia Il Post – si voleva tentare di risolvere la cosa internamente, al fine di limitare il danno reputazionale?

Genuinità e coerenza: 4 in condotta

Per farci un'idea dell'aderenza del comportamento di Intesa San Paolo alle migliori prassi in tema di crisis management e crisis communication, analizziamo brevemente contenuti e *tono di voce* delle comunicazioni della banca.

“*Come noto* – scrive Intesa San Paolo nei propri comunicati stampa indirizzati ai mass-media – *un dipendente infedele della nostra banca, con un comportamento che ha gravemente violato le norme, i regolamenti e le procedure interne, ha consultato dati e informazioni riguardanti alcuni clienti* (in realtà migliaia, ndr) *in modo ingiustificato. Il sistema interno di controlli lo ha individuato, abbiamo inviato notifiche al Garante della Privacy, abbiamo licenziato il dipendente infedele e abbiamo sporto denuncia come parte lesa (…) Siamo molto dispiaciuti di quanto accaduto e chiediamo scusa. Quanto avvenuto non dovrà più accadere. Confermiamo che non c’è stato alcun problema di sicurezza informatica, rispetto alla quale Intesa Sanpaolo si colloca tra le migliori posizioni internazionali.*”

Gli analisti de Il Post sottolineano come “*…una volta che la struttura di controllo interno ha evidenziato le anomalie, si è subito avviata la procedura disciplinare e l’analisi dei fatti, che ha richiesto una complessa ricostruzione di quanto avvenuto*”.

Ottimo. Peccato che durante questa analisi complessa, il dipendente abbia serenamente continuato a fare esattamente quello che faceva prima.

E – aggiungiamo noi – l’istituto non ha effettuato alcuna comunicazione alla pubblica opinione: sorprendentemente, per quasi un anno la vicenda è restata sotto traccia, tradendo il rapporto di fiducia non solo con la propria audience, ma con tutto il mercato.

Inoltre, rimarca Costa, “*…se è vero che la banca non ha alcuna responsabilità, significa che non avrebbe potuto fare nulla per accorgersi prima di questi settemila accessi abusivi. Vuol dire che qualsiasi altro dipendente di Intesa Sanpaolo, per quanto ne sappiamo, potrebbe in questo momento fare la stessa cosa. D’altra parte, Coviello lo faceva da anni. Evidentemente non esiste un sistema che faccia scattare un allarme quando*

avvengono accessi così anomali”. Incredibile, considerato quanto sarebbe semplice – ce lo confermano vari esperti informatici – disporre di un sistema di controllo in grado di allertare immediatamente per accessi a conti correnti al di fuori del proprio perimetro territoriale di competenza. Più che corretta quindi l’analisi della redazione di Morning: incomprensibile che il colosso bancario non disponga di sistemi di allerta in grado di intercettare *sollecitamente* – e non dopo mesi – accessi abusivi ai conti di questa portata.

Appurato questo, dove sono le scuse incondizionate di Intesa San Paolo?

Il tentativo di contenimento del danno, che fa ancora più danno

La verità è che in Intesa avrebbero dovuto fare dei controlli, avrebbero dovuto essere attrezzati per tracciare più che sollecitamente degli accessi abusivi, non hanno fatto nulla di tutto ciò, e ora – nell’evidente tentativo di ridurre l’angolo di attacco e di attribuzione delle responsabilità – ci raccontano di essere anche loro “parte lesa” e di aver fatto tutto il possibile per intervenire.

Ebbene, se non c’è stato *“nessun problema di sicurezza informatica”*, come afferma Intesa…cosa è successo? Tutto in ordine, tutto bene? Pare di no, la contraddizione è evidente: quindi la strategia narrativa scelta da Intesa per fronteggiare questa preoccupante crisi di reputazione pare scricchiolare, e molto, in termini di genuinità e coerenza, che – ben lo sa qualunque addetto ai lavori – sono tra gli ingredienti base di un buon crisis management.

Di nuovo, l’ennesima volta per una grande azienda: un approccio dilettantesco, basato sulla “dilazione”, sulle ammissioni tardive e parziali, sul *“cerchiamo di raccontarvela bene e di infiocchettarla quanto meglio possibile”,* al fine (pensa forse il management della banca) di ridurre l’impatto

negativo sull’indice reputazionale dell’azienda.

Peccato che questi atteggiamenti, queste strategie, appaiano non solo fortemente desuete, ma in gran parte disallineate da quell’impianto teorico, sostenuto da migliaia di case-history pratiche, che, se convintamente e tempestivamente applicato, avrebbe davvero contributo a ridurre la forza d’urto della vicenda, tutelando il valore della banca. Così non è stato, perché c’è sempre qualche comunicatore “che la sa lunga”, i signori del “ve lo spieghiamo noi, come si fa, che siamo una grande agenzia di comunicazione…”

Cosa succederà ora?

Certo, in Intesa San Paolo non sono stati con le mani in mano, e un segnale l’hanno dato: oltre a denunciare e licenziare Coviello, e mettersi a completa disposizione delle autorità (e sarebbe assai singolare il contrario), il CEO di Intesa ha proposto lo scorso mese al CdA della banca la nomina – a mio avviso assai tardiva – del Generale del Corpo d’Armata dei Carabinieri Antonio De Vita nel ruolo di Chief Security Officer di gruppo, nuova area a riporto diretto del Consigliere Delegato, con responsabilità su temi di Cyber Security e Sicurezza.

Tuttavia, si sa, la scelta, per un’azienda coinvolta in una crisi reputazionale, di un registro narrativo nel quale inserirsi al fine di tentare di dimostrare coerenza, autenticità e trasparenza gestionale, mantenendo almeno in parte il governo dei flussi di comunicazione, è cosa delicata, e non può essere improvvisata, né affidata alle funzioni che routinariamente si occupano della comunicazione corporate.

Gli ultimi decenni sono infatti costellati di “cadaveri” vittime di questo peccato mortale: aziende floride la cui business continuity è stata pregiudicata, in tutto o in parte, non solo dalla deflagrazione di crisi reputazionali peraltro del tutto prevedibili, ma anche (e, a volte, soprattutto) da

come esse sono state – o no – gestite. Esempio tra tutti valga la crisi dell'impero di Chiara Ferragni, generata da seri e fondati motivi endogeni, ma amplificata dalla totale inadeguatezza della gestione da parte della protagonista di quella vicenda – che certo, a sua discolpa, non è una specialista in queste materie – come anche dei suoi consulenti, quelli del *"Chiara è la regina dei Social e sa cosa fare"* (molto probabilmente della stessa scuola di quelli di Intesa San Paolo).

Inoltre, tutti i colossi come Intesa San Paolo destinano ingenti risorse all'implementazione delle proprie strategie ESG (Environment, Social and Governance) e alla loro rendicontazione, e allora la domanda è una sola: situazioni come questa non rientrano forse nel perimetro ESG? A quando un approccio più genuino e concreto a queste tematiche, abbandonando definitivamente – sarebbe pur ora! – un approccio basato sulla mera *compliance*, del tipo *"dobbiamo sistemare anche questa task, flagghiamo questa incombenza, e procediamo oltre…",* tipica dell'abbraccio mortale tra grandi aziende e grandi società di consulenza?

Come ben sappiamo, la reputazione è l'asset immateriale più importante per un'azienda, tale da condizionarne il valore di mercato fino alla metà della sua capitalizzazione, e una crisi mal gestita non fa altro che distruggerne in modo significativo il valore, con buona pace soprattutto dei piccoli azionisti, vere vittime incolpevoli di questa storia di "cattivo management": quante volte l'abbiamo ripetuto? Fino alla noia. Eppure, evidentemente, questo concetto così elementare è ancora lontano – i fatti lo confermano – dall'essere compreso e fatto proprio da top management e Consigli di Amministrazione della maggior parte delle società quotate in Italia.

In definitiva, come possa un colosso come Intesa San Paolo arrivare in buona parte impreparato a un appuntamento decisamente critico come quello che sta vivendo, senza aver

fatto – ne sono certissimo – neppure un assessment sui temi reputazionalmente più sensibili, al fine di individuare, prevedere e mitigare i rischi, resta per me un mistero davvero insondabile.

Le aziende di pesticidi e OGM hanno creato un social per identificare chi li critica

Un’inchiesta ha messo in luce un complesso sistema di monitoraggio e attacco nei confronti dei critici del settore agrochimico e delle biotecnologie, gestito da aziende con legami profondi con i business dei pesticidi e degli OGM. Queste aziende avrebbero creato una sorta di “social network

privato”, una piattaforma esclusiva su cui raccogliere e condividere informazioni su figure pubbliche, accademici e attivisti che si oppongono o criticano il loro operato. Tra i bersagli figurano anche esponenti delle Nazioni Unite. Il servizio sarebbe gestito da *v-Fluence*, una società specializzata in raccolta di informazioni e gestione della comunicazione di crisi. L’azienda, fondata da Jay Byrne, **ex dirigente di Monsanto**, figura di spicco nel settore agrochimico, fornisce strumenti per monitorare e rispondere alle critiche rivolte all’industria. Le indagini rivelano inoltre che parte del finanziamento di queste operazioni potrebbe provenire dal **governo degli Stati Uniti**.

I documenti che svelano il fatto sono stati diffusi da ***Lighthouse Reports***, un’importante organizzazione di giornalismo collaborativo con sede in Belgio, che ha condotto e pubblicato un’inchiesta nella quale riferisce che i più grandi produttori di pesticidi e portatori d’interesse del settore chimico hanno **profilato centinaia tra i più noti e importanti critici** di un settore che a livello globale vale 78 miliardi di dollari. Sul portale *Bonus Eventus*, erano contenuti i loro profili, completi di indirizzi di residenza e numeri di telefono. Nella lista dei “cattivi” sono presenti circa **3.000 organizzazioni e 500 tra accademici, scienziati, esperti** di diritti umani delle Nazioni Unite, ambientalisti, giornalisti, politici e funzionari pubblici. Solo 1.000 privilegiati possono accedere. Nell’elenco dei membri della rete dell’industria agrochimica vi sono i dirigenti di alcune delle più grandi aziende di pesticidi al mondo, insieme a funzionari governativi di diversi paesi.

L’inchiesta è nata da una soffiata su un tentativo di sabotaggio nei confronti di una conferenza scientifica tenutasi a Nairobi, in Kenya, che presentava soluzioni sostenibili per i pesticidi. Le richieste in base al *Freedom of Information Act* (FOIA) hanno rivelato un’ampia corrispondenza tra funzionari pubblici statunitensi, una ONG

keniota, un dirigente del settore pesticidi e la società v-Fluence su come sovvertire l'evento. Un mix di analisi delle tracce di denaro e ricerche sui registri della spesa pubblica ha portato alla luce **contratti stipulati tra v-Fluence e la United States Agency for International Development** (USAID). Tra il 2013 e il 2019 circa, l'Agenzia statunitense ha incanalato oltre 400.000 dollari alla società privata per servizi tra cui il "monitoraggio rafforzato" dei critici degli "approcci agricoli moderni" e per costruire *Bonus Eventus*, il social network con profilazione dei critici.

Bonus Eventus, lanciato nel 2014, è nato da un'idea di Jay Byrne, ex dirigente delle comunicazioni dell'azienda agrochimica **Monsanto** – acquistata dalla tedesca Bayer nel 2016 – e della sua società di gestione della reputazione, v-Fluence. L'inchiesta fa notare come dai documenti del tribunale si sappia che entrambi sono attualmente citati in giudizio negli Stati Uniti, insieme al produttore di pesticidi Syngenta, per aver presumibilmente soppresso informazioni per oltre 20 anni sui rischi per la salute associati a un erbicida, il Paraquat.