Cosa succede quando acquisisci un marchio in difficoltà, oppure caduto in disgrazia

InViaggi e Teorema, Columbus e Marcelletti. Cos'hanno in comune questi quattro gloriosi tour operator? Caduti in disgrazia e praticamente cessata l'attività, i rispettivi marchi sono stati rilevati (spesso dai curatori fallimentari) da altri t.o., che mirano a rilanciarli. Questo solo negli ultimi tre anni. **Val la pena acquisire un marchio, magari spendendo un sacco di soldi?** Sono più i rischi o i vantaggi? Usciamo dal turismo e vediamo cosa è successo in altri settori. Il bilancio offre più ombre che luci e bisogna avere la pazienza di leggere fino in fondo.

Abbigliamento giovanile: Guru – La parabola del marchio di abbigliamento creato da **Matteo Cambi** a Parma, nel 1999, è balistica, ovvero dalle stelle alle stalle in una manciata di anni. Da zero ai cento milioni di euro del 2006, dalle prime magliette artigianali distribuite agli amici a milioni di T-shirt vendute in tutto il mondo: nei primi anni 2000 la margherita stilizzata a sei petali colorati, con contorni neri

marcati, diventa un love-mark, indossato da calciatori e soubrette televisive, deejay e protagonisti del gossip da spiaggia. Nel 2008 il tracollo: 100 milioni di debiti, Matteo Cambi prima arrestato e poi condannato per bancarotta fraudolenta. Dal 2008 a oggi il marchio Guru passa di mano tre volte: acquisito dal colosso indiano **Bombay Rayon Fashion Limited**, nel 2016 la sua partecipata italiana, **Brlf Italia**, chiede il concordato preventivo; nel 2019 subentra la svizzera **Ibs Sagl di Lugano**, che però affida la commercializzazione alla monegasca **Ghep**, che nel 2021 diventa l'unica titolare di Guru. Oggi sul sito di Guru l'iconica T-shirt con la margherita si compra con 30 euro, ma chi se la ricorda più?

Sportswear: Sergio Tacchini, Fila, Ellesse – Negli anni '70/'80 gli italiani erano i più bravi e innovativi creatori di abbigliamento sportivo nel mondo. Altro che **Nike** o **Adidas**. Limitandoci al tennis, Sergio Tacchini, marchio creato nel 1966 dall'omonimo tennista, vestiva Jimmy Connors e Ilie Năstase, Adriano Panatta e John McEnroe. Fila, fondata a Biella nel 1911, nel 1973 diventa Fila Sport e veste Guillermo Vilas e Björn Borg (che con l'iconica polo in cotone a costine vince cinque tornei di Wimbledon consecutivi). La perugina Ellesse, fondata nel 1959 da **Leonardo Servadio**, da cui prende le iniziali, nel 1975 comincia a produrre abbigliamento da tennis e veste Corrado Barazzutti, che nel 1976 vince l'unica Coppa Davis per l'Italia, in Cile. Sergio Tacchini, Fila ed Ellesse sono marchi tuttora presenti nello sportswear, ma – da molti anni e dopo innumerevoli vicende societarie – non appartengono più ai fondatori, né hanno sede in Italia. Dal 2019 Sergio Tacchini fa capo a due private equities americani, **Twin Lakes Capital e B. Riley Principal Investments**. Nel 2007 Fila viene acquistata dall'imprenditore sud-coreano **Gene Yoon** e a Biella rimane solo la Fondazione Fila Museum, che accoglie oltre 30.000 tra capi di abbigliamento, scarpe e accessori a marchio Fila. Dal 1994 Ellesse è un marchio della holding britannica **Pentland Group**,

che controlla tra gli altri **Speedo e Berghaus**. Nessuno dei grandi tennisti italiani di oggi indossa questi marchi, ormai diventati "heritage brands": Matteo Berrettini veste Boss, Jannik Sinner e Lorenzo Musetti sono sponsorizzati da Nike sin da quando erano ragazzini.

Gelati: Grom – L'Italia è considerata la patria del gelato e non poteva che nascere a Torino, nel 2003, l'avventura del manager ex PWC **Federico Grom** e dell'enologo **Guido Martinetti**. Occupa 25mq la prima gelateria Grom, a pochi minuti da piazza San Carlo: con un capitale di partenza ridottissimo, cui contribuiscono parenti e amici, si fonda su un'idea di marketing precisa, "Il gelato come una volta". In un unico stabilimento nella cintura torinese e solo con ingredienti di prima qualità, a chilometro zero e da presidi Slow Food, vengono prodotti i semilavorati dei vari gusti: questi, confezionati e surgelati, sono distribuiti alle gelaterie per essere miscelati, mantecati e serviti al pubblico. Il prezzo di vendita è più quello di una pasticceria torinese, che di una gelateria su strada. La crescita è esplosiva: decine di Grom aprono in Italia e all'estero (New York, Londra, Hong Kong) e dopo i 16 milioni di euro di fatturato, nel 2009, si toccano i 23 milioni nel 2011. L'avventura imprenditoriale indipendente di Grom e Martinetti termina bruscamente nel 2015, quando – reduci da alcune difficoltà finanziarie – cedono Grom alla multinazionale britannico-olandese **Unilever**, che in portafoglio dispone già di vari marchi di gelati industriali, tra cui **Algida e Magnum, Carte d'Or e l'americana Ben&Jerry's**. Da allora Grom sbarca nei supermercati con le classiche vaschette da frigo, chiude diversi punti vendita in Italia e dice addio all'artigianalità che l'aveva caratterizzata fino ad allora. Grom e Martinetti restano nel board per diversi anni, pur con sempre minore autonomia gestionale, ma sembrano non condividere più la strategia di Unilever: negli USA è la GDO a intermediare quasi il 97% delle vendite, lasciando alle gelaterie una quota residuale, e il gelato in vaschetta è consumato tutto l'anno. La gelateria con

coni e coppette, aperta solo 6 mesi l'anno, non funziona più.

Formazione: Pegaso Università Telematica – Nel 2006 **Danilo Iervolino**, napoletano, classe 1978, figlio d'arte (il padre Antonio fonda le Scuole Paritarie Iervolino per far recuperare la bocciatura ai cattivi studenti) ha un'idea meravigliosa, ispirata da due accadimenti, uno pubblico e uno privato. Nel 2003 era stato emanato il decreto "Moratti-Stanca" che istituiva le università telematiche; Iervolino si era appena laureato in economia a Napoli e durante un soggiorno negli USA aveva scoperto la formazione a distanza e le nuove piattaforme tecnologiche che – grazie al boom mondiale di internet, si era nel 2002 – si stavano sviluppando. Nel 2006 nasce l'Università Telematica Pegaso, con la forma giuridica di società per azioni, della quale Iervolino è presidente del CdA e maggiore azionista: Pegaso ottiene l'accreditamento del Ministero dell'Istruzione e attiva i primi due corsi di laurea, in giurisprudenza e scienze della formazione. In un sol colpo, Iervolino rompe il monopolio statale (o privato, ma solo per eccellenze come Università Cattolica o Bocconi, Luiss o IULM) e impone il modello della formazione a distanza, basata sul PC e sull'interazione col docente. Il successo è immediato: i corsi di laurea si moltiplicano, sedi di esami si diffondono a decine in tutta Italia, a iscriversi e laurearsi (il titolo è equiparato a quello ottenuto in una università tradizionale) sono prima in migliaia, poi in decine di migliaia. La svolta arriva un anno fa, a settembre 2021: il private equity britannico **CVC Capital Partners** rileva l'intera proprietà della holding, a cui fanno capo Pegaso Università Telematica e l'Università Mercatorum, valutando l'asset – la cifra è ufficiosa – un miliardo di euro. Danilo Iervolino rimane nel board, ma investe i guadagni in nuove attività, comprando prima la **Salernitana Calcio** (e qui incrocia Gerardo Soglia ex CIT e Buon Viaggio Network), poi il settimanale L'Espresso da Gedi/la Repubblica.

Due note a margine: di tutte le imprese citate, l'unica a non

aver ceduto proprietà/marchio causa difficoltà finanziarie o industriali è quella di Iervolino. Guru, Sergio Tacchini, Fila, Ellesse, Grom e Pegaso – tutte eccellenze italiane – oggi sono in mani straniere.

Conclusione, per i pazienti lettori arrivati fin qui: è costoso e complesso rilevare un marchio, soprattutto se questo è in difficoltà (o peggio). Per questo rimango perplesso sul rilancio di tour operator che hanno vissuto tempi migliori. Nel nostro settore, è un'eccezione: nessuno si è mai sognato di rilanciare marchi come **Jolly Hotels o Motel Agip, CIGA o Metha Hotels; e tantomeno** **Alpi Eagles o Volare Airlines, AirOne o Gandalf.** E neanche **Alitalia**, pensa te.

Il Jova Beach Party, il fratino, gli econazisti e il greenwashing

Danilo Selvaggi (Lipu) risponde a Jovanotti e al Wwf

Come bloccano internet

Sappiamo perché i governi bloccano internet, totalmente o parzialmente (per spegnere il dissenso; impedire la sua organizzazione; ridurre l’accesso o la circolazione di

informazioni sgradite, ecc); sappiamo che negli ultimi anni lo hanno fatto sempre più spesso (182 casi nel 2021 in 34 Paesi contro i 159 del 2020). Ma non sappiamo molto di come avvengano effettivamente tali blocchi. Eppure anche il come è importante, per un motivo molto semplice: "l'assenza di comprensione tecnica ha un impatto nella nostra capacità di combatterli".

Una tassonomia dei blocchi internet

Così scrive un rapporto appena uscito dell'Ong Access Now che analizza le differenze tecniche dei vari tipi di blocchi della Rete tracciando una "tassonomia degli internet shutdown".
Ma prima di tutto una definizione. Per internet shutdown si intende, scrive Access Now, "la sospensione intenzionale di internet o di comunicazioni elettroniche, al fine di rendere le stesse inaccessibili o di fatto inutilizzabili, per una popolazione specifica o in una località, spesso per esercitare controllo sul flusso di informazioni".

Non solo. Siccome cresce la pressione internazionale contro questa forma di "punizione collettiva" (e aggiungo io, siccome un blocco totale ha costi economici non indifferenti) i governi stanno ricorrendo sempre di più a forme mirate, geograficamente o a livello di servizio/app specifiche. Ad esempio, c'è una mobilitazione di piazza antigovernativa? Si sospende il traffico dati mobile della zona, e via dicendo.

Ora il report identifica 8 tipi di shutdown, che vi riassumo qui di seguito (in un difficile equilibrismo tra tecnicismi, divulgazione e sintesi, dato che il report è dettagliato e rivolto a un pubblico tecnico):

1) Blocco fondamentale dell'infrastruttura

Quando l'interruzione nasce da un danneggiamento all'infrastruttura fisica. Esempio: quando nel 2015-2016 gli hacker di Sandworm (considerati legati all'intelligence russa)

hanno provocato un blackout elettrico in Ucraina, hanno anche causato un'interruzione nelle reti di comunicazione. O quando nel 2018 è andato a fuoco un centro tecnico di Orange in Costa d'Avorio dei cavi sottomarini sono stati distrutti col risultato di rendere il servizio inaccessibile per settimane. Per Orange si trattò di sabotaggio.
Vantaggi per chi lo fa: efficace; offre plausible deniablity (negazione plausibile: è stato un incidente, non volevamo mica censurare nessuno!); ma può essere alla portata anche di attori non statali.
Come affrontarlo: comunicazioni satellitari, radio, altre infrastrutture.

2) Routing

La manipolazione del network routing. L'informazione sul routing è alterata in punti chiave dell'infrastruttura di rete, come ai gateways internazionali, per non far passare il traffico ad altre infrastrutture, determinando uno shutdown. Non funziona bene su sezioni localizzate del network, e di solito è implementata per nazioni intere o grandi aree geografiche.
Vantaggi: un modo semplice di chiudere la connettività internet internazionale per un Paese. Ma ha lo svantaggio che i cambiamenti nel routing devono propagarsi e ci vuole del tempo.
Come affrontarlo: comunicazioni satellitari, radio, altre infrastrutture.

3) Manipolazione del sistema dei nomi di dominio (DNS)

Si usa la manipolazione dei DNS (il sistema che regola la traduzione dei domini in indirizzi IP) e in particolare dei domain name servers di un Paese per dirigere il traffico verso domini specifici (ad esempio WhatsApp) via dai server dell'azienda e mandarlo invece a server sotto il controllo del governo o che nemmeno esistono, causando un blocco del

servizio. Perché sia efficace serve il controllo (da parte del governo) o la collaborazione degli internet service providers (ISP). Inoltre alcuni meccanismi usati per implementare questo tipo di blocco sono facili da aggirare da parte degli utenti. In realtà questo tipo di manipolazione è molto complessa e con varie sfumature, per cui rimando al rapporto, che va molto in dettaglio.
Esempi: L'Iran anni addietro aveva bloccato Facebook Messenger in questo modo. Il Pakistan l'ha usata per bloccare alcuni social media durante le proteste del 2017. E la manipolazione dei DNS è stata usata per bloccare 25 siti in Catalogna in occasione del referendum del 2017 sull'indipendenza.
Vantaggi: facile da implementare contro social o piattaforme "hostate su un piccolo set di domini DNS".
Come affrontarla: a seconda della tipologia si possono usare server DNS non sotto il controllo delle autorità; e/o una VPN. Per proteggersi da attacchi di questo tipo può aiutare anche l'uso di una funzione DNS avanzata, nota come DNSSEC, "che aggiunge un livello di fiducia al DNS fornendo un servizio di autenticazione".

4) Filtraggio (Filtering)

Usa particolari apparecchiature (filtering appliances), adottate anche a livello corporate, per bloccare l'accesso a specifiche piattaforme, come Facebook, Twitter ecc. È un meccanismo usato spesso da Cina, Iran, Arabia Saudita. In genere tali apparecchiature sono già messe in piedi per filtrare siti criminali e poi sono estese ad altri.
Sono implementate a livello di backbone, dorsali internet (se il governo controlla le infrastrutture telco in un Paese), o a livello di ogni singolo ISP del Paese (e in tal caso il filtraggio non sarà omogeneo).
Esempi: il Brasile ha bloccato Whatsapp in questo modo nel 2015.
Vantaggi: nasce come tecnologia con vari scopi commerciali; ha effetto immediato; può essere molto granulare, anche sulla

base della localizzazione degli utenti. Quando l'utente prova a collegarsi a un sito bloccato, può vedere un avviso che dice che è bloccato ma anche un messaggio di errore.
Come affrontarlo: si possono usare VPN per aggirarlo (se non sono a loro volta bloccate)

5) Ispezione profonda dei pacchetti (Deep packet inspection o DPI)

Si tratta ancora di device di filtraggio in grado anche di valutare i contenuti del traffico e anche qua possono essere implementati a livello di backbone o da ogni singolo ISP. Sono strumenti che possono essere usati in un'ottica di sorveglianza ma anche di censura. Il Paese che forse più l'ha usata in questa maniera è la Cina.
Esempi: come segnalato dall'osservatorio anti-censura OONI (che ha collaborato al report di Access Now), Cuba ha usato questa tecnologia per bloccare Skype. L'Iran l'ha usata nel 2018 per bloccare Instagram.
Vantaggi: è una tecnologia potente con vari utilizzi, da quelli commerciali alla censura e sorveglianza. Anche questa può essere molto granulare.
Come affrontarla: con alcuni meccanismi per nascondere la comunicazione in un protocollo (obfuscation proxies).

6) Attacco attraverso un'infrastruttura non autorizzata (rogue)

Avviene quando l'attaccante introduce un meccanismo (in genere temporaneo) nell'infrastruttura o in un segmento di rete, così da clonare l'infrastruttura legittima a cui si connetterà l'utente. Che in quel modo, senza accorgersene, affida le comunicazioni all'operatore del nodo illegittimo. In genere si utilizza su reti cellulari e WI-Fi.
Esempi: nel 2016 durante una protesta in North Dakota i partecipanti hanno riferito di chiamate disconnesse e altri problemi al segnale mobile.
Vantaggi: permette di identificare i partecipanti a una

protesta o a una attività in un certo luogo.
Come gestirlo: Bisogna smettere di usare il sistema di comunicazione intercettato dai nodi non autorizzati.

7) Attacco di negazione del servizio – Denial of Service (DoS)

I suoi autori usano attacchi di negazione distribuita del servizio o DDoS (Distributed Denial of Service) e altri attacchi DoS (Denial of Service) per prendere di mira le comunicazioni di una piattaforma specifica, o anche le comunicazioni internet di un intero Paese, come accadde nel 2016 quando il gruppo dietro la botnet Mirai attaccò le telco e infrastrutture della Liberia (collegata a internet solo da un cavo sottomarino). L'offerta criminale di questi servizi, che possono essere acquistati da altri, è ampia e ben organizzata.
Esempi: i DDoS che si sono visti in Ucraina.
Vantaggi: plausible deniability (non sono stato io ma questo gruppo di scappati di casa); ma d'altro canto si tratta di uno strumento che possono usare anche attori non-statali; gli utenti non possono fare nulla per aggirare o risolvere il problema, se non lo risolve il fornitore del servizio sotto attacco.
Come mitigarli: la mitigazione va fatta prima usando dei servizi di protezioni dai DoS.

8) Throttling (limitazione)

È l'atto di limitare volutamente, senza bloccare del tutto, il flusso di dati attraverso una rete di comunicazione. Così sembra che il servizio o la piattaforma in questione siano disponibili, ma di fatto sono inutilizzabili. Ci sono vari meccanismi tecnici per farlo, e la comunicazione può essere limitata sulla base del protocollo, origine, destinazione ecc. È difficile distinguere se la causa sia voluta o dovuta ad altro.
Esempi: l'Iran col traffico HTTPS prima delle elezioni.

Vantaggi: plausible deniability; permette alcuni usi essenziali: spinge utenti via dai canali cifrati.
Come affrontarlo: se il throttling riguarda solo siti e servizi basati su uno specifico protocollo, si possono usare sistemi come VPN ecc. Altrimenti se tutto il traffico è limitato, è più difficile aggirarlo.

Il report, dopo aver classificato le diverse tipologie di shutdown, prosegue ad analizzare l'impatto di questi blocchi: quante persone hanno riguardato? Hanno impedito attività economiche? Servizi di emergenza? L'accesso a informazione indipendente? Comunicazioni interpersonali? Era facile migrare a una piattaforma equivalente? E quanto le persone si affidavano alla tecnologia/piattaforma bloccata? E infine, come si possono individuare e attribuire le diverse cause all'origine di questi blocchi?
Nella riconfigurazione di internet che sta avvenendo in questi ultimi tempi (o che alcuni vorrebbero far avvenire) anche le questioni tecniche assumono una forte connotazione di attualità politica. Non che ne siano mai state prive

---

La "Boiler Summer Cup": quando il bullismo diventa virale, e l'importante ruolo degli Influencer

TikTok è stato recentemente teatro di una controversia che ha suscitato indignazione e preoccupazione tra molti utenti e creators. La “Boiler Summer Cup”, una challenge vergognosa e offensiva, ha iniziato a spopolare sulla piattaforma. L’obiettivo di questa sfida era semplice quanto crudele: i partecipanti dovevano cercare di rimorchiare la ragazza più grassa in discoteca per poi ridicolizzare l’esperienza sui social media. Questa tendenza ha rapidamente attirato l’attenzione, suscitando la condanna da parte di numerosi creator e figure pubbliche, preoccupate per il messaggio degradante e disumanizzante che trasmetteva.

La “Boiler Summer Cup” non è solo un esempio di bullismo e body shaming, ma rappresenta anche una triste dimostrazione di come i social media possano amplificare comportamenti tossici e degradanti. Rendendo le donne oggetti di scherno e umiliazione pubblica, questa sfida non solo perpetua stereotipi dannosi, ma contribuisce a creare un ambiente online ostile e pericoloso per coloro che ne sono vittime. È un promemoria inquietante di come il potere delle piattaforme digitali possa essere usato in modo distruttivo, specialmente quando viene alimentato dalla ricerca di visibilità e

approvazione da parte di un pubblico altrettanto irresponsabile.

In questo contesto, il ruolo degli influencer e dei creator digitali diventa fondamentale. Con la loro enorme portata e capacità di influenzare le opinioni e i comportamenti, hanno una responsabilità morale significativa nel combattere fenomeni come la “Boiler Summer Cup”. Contestare pubblicamente queste sfide, sensibilizzare il pubblico sui loro effetti negativi e promuovere un uso consapevole e rispettoso delle piattaforme social è un dovere che non può essere ignorato. Quando un influencer prende una posizione netta contro il bullismo e la discriminazione, non solo invia un messaggio chiaro ai propri follower, ma contribuisce anche a creare una cultura online più sana e rispettosa.

Le reazioni alla “Boiler Summer Cup” da parte di alcuni creator sono state incoraggianti. Molti hanno utilizzato i loro canali per denunciare la sfida, esprimendo solidarietà alle vittime e invitando i loro follower a riflettere sulle conseguenze delle loro azioni online. Questa forma di attivismo digitale è cruciale per contrastare la diffusione di contenuti dannosi e per educare le nuove generazioni sull’importanza del rispetto e della dignità umana. Inoltre, la condanna pubblica di queste sfide può contribuire a disincentivare altri utenti dal partecipare a fenomeni simili in futuro, sapendo di poter incorrere nella disapprovazione della comunità.

Tuttavia, il lavoro di sensibilizzazione non dovrebbe fermarsi qui. È necessario che le piattaforme social come TikTok implementino politiche più rigorose per prevenire la diffusione di contenuti offensivi e per proteggere gli utenti vulnerabili. La collaborazione tra influencer, utenti e piattaforme è essenziale per creare uno spazio digitale sicuro e inclusivo per tutti.

“Boiler Summer Cup” è un triste esempio di come i social media

possano essere usati per perpetuare comportamenti dannosi e discriminatori. Ma è anche un’opportunità per riflettere sull’importanza del ruolo degli influencer nella promozione di valori positivi e nel contrasto alle dinamiche di bullismo e umiliazione online. Solo attraverso una condanna chiara e un’azione collettiva possiamo sperare di costruire una comunità digitale più rispettosa e consapevole.

Agrovoltaico: che cos’è e quali sono i suoi vantaggi

Una fonte di sostenibilità nel mondo agricolo