

## Pubblicità fraudolenta e social media: un'analisi dei recenti studi

di Elena Carpani, EY Studio Legale e Tributario

Recentemente, l'organizzazione TRACIT (Transnational Alliance to Combat Illicit Trade), in collaborazione con l'American Apparel & Footwear Association (AAFA), ha pubblicato un interessante report in materia di pubblicità on line di prodotti contraffatti (che, d'ora in poi, chiameremo, ai fini del presente contributo, "pubblicità fraudolenta") intitolato "*Fraudulent Advertising Online - Emerging Risks And Consumer Fraud*".

La pubblicità fraudolenta è un fenomeno noto da tempo, ma recentemente in espansione soprattutto sui social networks (principalmente Facebook e Instagram, ma anche YouTube e LinkedIn).

Da maggio 2017 ad oggi, oltre 70 grandi società di prodotti di consumo e abbigliamento sono state interessate da campagne di pubblicità fraudolente di propri prodotti su social network. I brands colpiti sono del calibro di Apple, Tommy Hilfiger, LEGO, Lacoste, Timberland, ossia appartenenti a società che hanno maturato molta esperienza nel contrastare la contraffazione dei loro marchi e che investono enormi risorse nella tutela della proprietà intellettuale.

Ciononostante, la pubblicità fraudolenta sembra non avere argini ed è in continua e inarrestabile diffusione. Guardando i numeri, il Global Brand Counterfeiting Report 2018-2020 ha stimato che il mancato guadagno delle aziende causato dalla contraffazione online ammontasse a ben \$ 323 miliardi nel 2017<sup>1</sup>. L'aumento degli acquisti online, incentivato anche dalle misure emergenziali di contrasto al COVID-19, ha sicuramente innalzato tale dato.

Come le normali pubblicità, anche quelle di cui stiamo parlando utilizzano tecnologie di targeting del consumatore sulla base di interessi specifici, posizione, dati demografici o cronologia di navigazione, rendendo le campagne molto profittevoli in pochissimo tempo.

Anche dal punto di vista tecnico e di design del post pubblicitario, tali pubblicità hanno caratteristiche estremamente subdole.

La tipica campagna di Fraudulent Advertising online utilizza, infatti, immagini di prodotti originali presentati con modalità totalmente confondibili e con prezzi non distanti da quelli degli omologhi prodotti originali.

Dal punto di vista tecnico, si evidenzia che vengono mostrati agli utenti, all'interno dei post, degli URL di destinazione falsi, oppure molto simili a quelli reali, anche utilizzando banali tecniche di occultamento URL (come, per esempio, bit.ly) che, in ogni caso, impediscono il "detect" da parte di sistemi di scansione automatica delle contraffazioni online.

---

<sup>1</sup> Global Brand Counterfeiting Report 2018-2020: <https://apnews.com/ef15478fa38649b5ba29b434c8e87c94>

Ciò significa che i contraffattori conoscono molto bene i software di investigazione online e sanno come aggirare i relativi controlli.

Alcuni social network tentano da anni di contrastare il fenomeno tramite portali per la segnalazione di IP infringements. Queste misure però non affrontano il problema alla radice. Anche in seguito alla segnalazione, e successiva rimozione, della pubblicità fraudolenta, la stessa spesso ricompare online nelle successive 24 ore, con contenuti leggermente diversi. Allo stesso modo, si stanno diffondendo annunci fraudolenti "sprint" veicolati tramite Instagram Stories che restano online solamente per 24 ore ma che hanno vastissima diffusione e popolarità tra gli utenti.

I tentativi di contrastare le pubblicità fraudolente on line risultano, quindi, spesso inefficaci.

I danni derivanti dalla pubblicità fraudolenta online sono facilmente intuibili.

Tali pubblicità, dando una falsa impressione di autenticità di marchi famosi, ingannano il consumatore che è indotto ad acquistare prodotti contraffatti e nella maggior parte dei casi privi dei requisiti di sicurezza previsti dalle normative di settore. Si pensi ai cosmetici e ai prodotti per la cura personale che, come accertato in occasione di numerose inchieste<sup>2</sup>, possono contenere livelli di piombo, mercurio, cianuro e altri agenti cancerogeni ampiamente

oltre i limiti consentiti dalla legge, causando gravi allergie e danni per la salute.

Per i brands, la minaccia rappresentata dalle pubblicità fraudolente consiste (oltre che nella perdita di profitti) nel danno d'immagine nei confronti del consumatore e nella diminuzione del valore del brand. La circolazione online di numerose contraffazioni sviscera inoltre il valore commerciale del brand e la sua forza in un successivo enforcement giudiziale.

Tali pubblicità online e i relativi siti sui quali il consumatore "atterra", mostrano, inoltre, di avere poca attenzione agli aspetti di tutela della privacy degli utenti, mettendo a repentaglio la sicurezza dei loro dati finanziari ed esponendo gli utenti ai più comuni reati informatici come, ad esempio, l'utilizzo illecito di carte di credito o conti bancari.

Ma quali sono le cause della crescente diffusione di tale fenomeno? Le ragioni sembrano da rinvenire nei seguenti fattori:

1. Bassissimi costi di realizzazione di una campagna fraudolenta: un'inchiesta condotta in nel Regno Unito<sup>3</sup> dimostra come sia possibile realizzare una truffa online su un noto social network al costo irrisorio di £ 15 (circa € 17). Si cita un esempio. Spendendo la suddetta somma, è stato possibile ottenere ben 3.834 visualizzazioni, 73 click e 19 condivisioni in 24 ore. Ulteriore incentivo è la

---

<sup>2</sup> Greenwood, C. (2015, May 17). Warning on fake make-up tainted by CYANIDE and other dangerous chemicals: Counterfeit versions of leading brands are being cooked up by criminals in squalid underground labs. Daily Mail. Disponibile al seguente link: <http://www.dailymail.co.uk/news/article-3085665/Warning-fake-make-tainted-cyanide->

[dangerous-chemicals-Counterfeit-versions-leading-brands-cooked-criminals-squalid-underground-labs.html](http://www.dailymail.co.uk/news/article-3085665/Warning-fake-make-tainted-cyanide-dangerous-chemicals-Counterfeit-versions-leading-brands-cooked-criminals-squalid-underground-labs.html)

<sup>3</sup> Disponibile al seguente link:

<https://www.which.co.uk/news/2019/06/how-our-fake-scam-ad-breezed-through-facebooks-approvals-process/>

sostanziale “immunità” dei realizzatori dei post che sono di fatto irrintracciabili dalle autorità.

2. Assenza di controlli da parte dei social networks e sui siti di destinazione: l'unico modo per costruire campagne illegittime online su social network è quello di creare un account. Il social network non effettua alcun controllo su tali account, ossia se esistano da tempo o siano stati creati ad hoc e se la pubblicità sia coerente rispetto al contenuto della pagina.

3. Assenza di cooperazione da parte dei “domain names registrars”: una pubblicità online reindirizza sempre ad un sito di destinazione esterno al social network tramite un URL. I social network non effettuano alcun controllo sul contenuto di tali siti esterni (e forse sarebbe anche troppo chiedere un simile adempimento). Per tale ragione, è necessario che i providers di nomi a dominio e spazi web (ad es. GoDaddy, Aruba, EuroDNS) migliorino i propri controlli, anche collaborando con i social networks.

TRACIT e AAFA ritengono che per limitare il fenomeno, sia sicuramente necessario, un aumento dei controlli “alla fonte” da parte dei social networks. Le tecnologie di Intelligenza Artificiale (AI) possono aiutare i social networks a rintracciare attività e post truffaldini con maggiore efficacia. AAFA ha anche proposto di implementare un'**autorizzazione** per le pubblicità online da rilasciare previa verifica da parte di un organismo indipendente di una *disclosure* bancaria e finanziaria della società esponente e di informazioni certificate sulla reale esistenza (anche fisica) della società.