Progetto FATA
From Awareness To Action

Rafforzare la conoscenza e la cooperazione pubblico-privata contro le nuove forme della contraffazione online

FATA
From Awareness
To Action

Rapporto finale

Aprile 2022

con il supporto di

amazon

Progetto FATA

From Awareness To Action

Rafforzare la conoscenza e la cooperazione pubblico-privata contro le nuove forme della contraffazione online

Autori (Crime&tech):

Mirko Nazzari
Michele Riccardi
Flaminia De Biase

Autori (Ministero dell'Interno):

Stefano Delfini
Loredana Stamato

Citazione suggerita: Ministero dell'Interno e Crime&tech-Università Cattolica del Sacro Cuore, 2022, *Progetto FATA: From Awareness To Action. Rafforzare la conoscenza e la cooperazione pubblico-privata contro le nuove forme della contraffazione online,* Milano: Università Cattolica del Sacro Cuore.

Progetto grafico:

Ilaria Mastro

ISBN: 978-88-99719-33-3

Crime&tech s.r.l.
Spin-off di Università Cattolica del Sacro Cuore (UCSC) - Transcrime
Largo Gemelli 1, 20123 Milano
Tel. +39 02 7234 3715/3716
info@crimetech.it
www.crimetech.it

Sommario

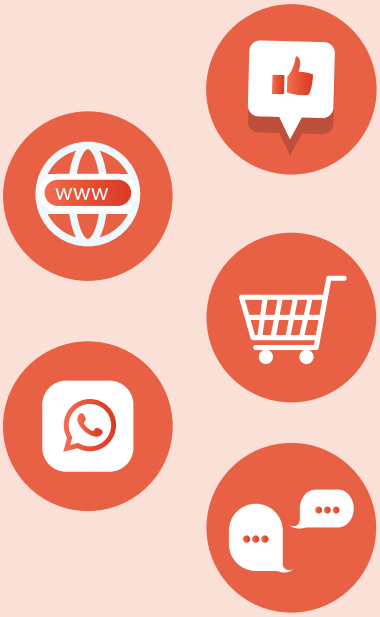
FATA

Introduzione

- Il **fenomeno della contraffazione è profondamente mutato** negli ultimi anni, influenzato dai cambiamenti nelle abitudini d'acquisto e nei canali utilizzati dai consumatori.
- La **diffusione dell'*e-commerce*** ha generato nuovi schemi e *modi operandi*, fatto emergere nuovi attori criminali e stretto i legami tra **contraffazione, frodi finanziarie e reati *cyber***.
- Autorità pubbliche e *marketplace* sono in prima linea nella lotta a queste minacce emergenti ma è necessario un **nuovo paradigma** in termini di sensibilizzazione, prevenzione, indagine e cooperazione.
- Questo studio, realizzato nell'ambito del **progetto FATA - From Awareness to Action**, ha lo scopo di fare luce sulle **nuove minacce della contraffazione sui mercati online**, sottolineare le sfide, presentare le **buone pratiche** nel settore pubblico e privato e proporre delle **direzioni future** di intervento e di collaborazione tra le parti.
- Lo studio si fonda su una rassegna approfondita di **casi studio**, documenti giudiziari, report istituzionali e sulle informazioni raccolte in **interviste**, a livello italiano e internazionale, con interlocutori privilegiati di forze dell'ordine, autorità pubbliche, *marketplace*, operatori postali e di logistica, aziende e titolari di diritti di proprietà intellettuale.
- FATA è un progetto realizzato da **Crime&tech**, spin-off del centro Transcrime di **Università Cattolica del Sacro Cuore**, insieme al **Ministero dell'Interno** (attraverso il **Servizio Analisi Criminale della Direzione Centrale della Polizia Criminale - Dipartimento della Pubblica Sicurezza**) e con il supporto di **Amazon**.

Contraffazione e mercati online: minacce e trend emergenti

Canali



- I contraffattori oggi utilizzano **diversi canali online** in maniera contestuale e interconnessa, sia per pubblicizzare che per vendere prodotti contraffatti, e per compiere allo stesso tempo altri reati. Questi canali sono:
  - *social network*;
  - siti fraudolenti (es. siti clone realizzati tramite *cybersquatting* e/o *typosquatting*);
  - *marketplace*;
  - applicazioni di messaggistica istantanea;
  - *web-forum* e chat (es. chat di videogiochi).

- I criminali riescono a spostarsi tra i vari canali facendosi seguire dai consumatori finali, ad esempio attraverso **pratiche di *cross-linking*** tra siti e canali diversi, e avvalendosi spesso di account 'usa e getta' e strumenti di *spam*.
- Dall'analisi dei casi studio, di recenti report EUIPO e di studi scientifici, emerge un **uso significativo (e crescente) dei *social network*** come veicolo per pubblicizzare e vendere 'falsi', anche per le maggiori vulnerabilità rispetto ai *marketplace* (vedi sotto).

Attori

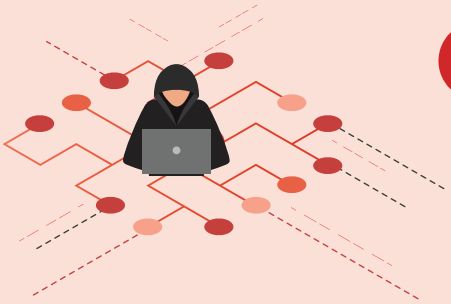
- Oltre ai soggetti coinvolti nel confezionamento e produzione di 'falsi', le nuove forme della contraffazione online vedono la partecipazione di diversi altri attori criminali, con ruoli ed *expertise* diversi.
- ***Influencer***: attori individuali, spesso di giovane età, che agiscono come **intermediari sui *social network* e nei forum dei mercati online** per attirare consumatori e collegarli con i fornitori di 'falsi', spesso localizzati in paesi asiatici e pronti a spedire direttamente i beni ai consumatori finali usando piccole spedizioni (*small parcel*) attraverso il sistema postale.

- ***Broker*** e sviluppatori, spesso dell'Est Europa e area russofona, che supportano contraffattori e gruppi criminali nello sviluppo e gestione di **servizi informatici** collegati alla vendita di falsi sul web, tra cui:
  - sviluppo e gestione di siti fraudolenti e siti 'clone';
  - sviluppo di 'carrelli' elettronici e sistemi di *cash-out* fraudolenti;
  - sviluppo e fornitura di *software* malevoli da veicolare tramite siti web e *marketplace* fraudolenti;
  - sviluppo di sisemi di produzione automatica di contenuti poi utilizzati in forum e chat per pubblicizzare beni contraffatti o siti fraudolenti (*spam-bot*).

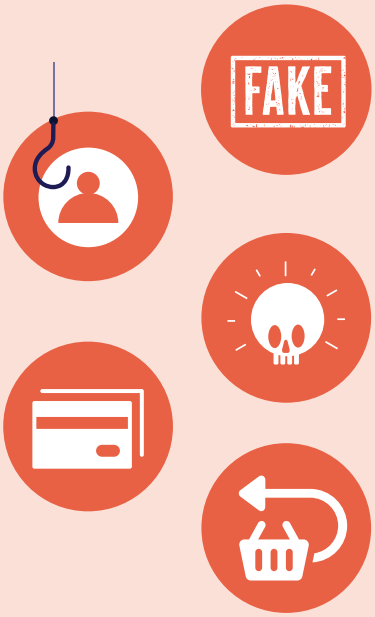
- *Broker* e **professionisti** che facilitano la costituzione e gestione di **società di comodo (*shell companies*)**, intestate a prestanome e spesso registrate all'estero (es. in paesi a bassa trasparenza societaria e in *Free Trade Zones*), utilizzate per varie ragioni, tra cui:
  - importare e giustificare, tramite fatture false, beni contraffatti poi venduti sul web;
  - intestare e gestire siti web fraudolenti;
  - aprire account di vendita come *seller* sui mercati online ufficiali;
  - riciclare denaro sporco e occultare trasferimenti illeciti (es. pagamento di stupefacenti) sotto forma di compravendite online.

- Gruppi di **criminalità organizzata**:
  - di matrice mafiosa (soprattutto legati alla Camorra), non-mafiosa, o di origine straniera (soprattutto cinese);
  - capaci di seguire e gestire l'intera filiera del falso online;
  - collegati con i siti di produzione all'estero;
  - in grado di gestire centri di assemblaggio e riconfezionamento sul territorio nazionale;
  - in grado di controllare la rete di vendita sul territorio (es. venditori abusivi) e quella online, appoggiandosi alle modalità sopra descritte;
  - potenzialmente collegati anche con gruppi terroristici ed estremisti.

Schemi



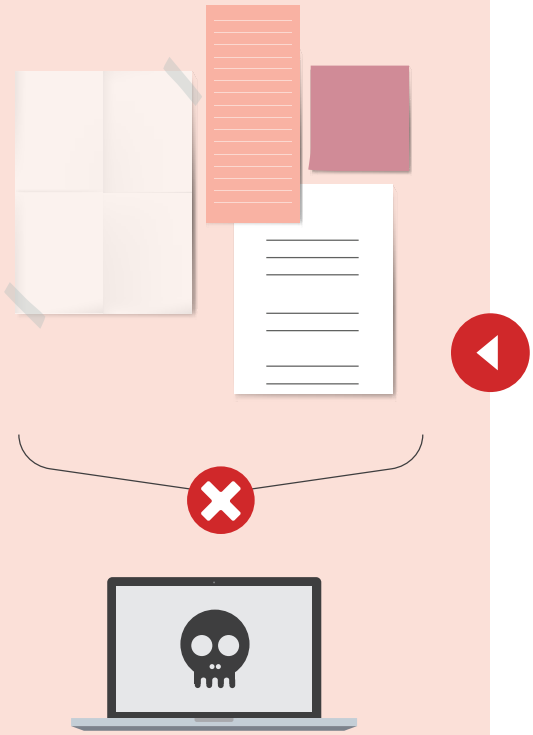
- Questi attori cercano di trarre il massimo vantaggio e profitto dall'interazione con i mercati online **sfruttando e infiltrando tutti i servizi offerti**: creazione account, acquisto, pagamento, reso, dialogo con gli altri utenti.
- Questo si manifesta in una crescente interconnessione di schemi criminali (***poli-criminalità***) e in un sempre più stretto legame della contraffazione con **frodi, reati economico-finanziari e reati *cyber***.
- Non un singolo reato ma un processo (***fraudster journey***) che si compone di diverse tappe e reati:
  - **vendita di 'falsi'**, attraverso i canali e le modalità sopra illustrate;
  - **furto di identità** di consumatori e *seller*, compresi i dati relativi ai metodi di pagamento, ad esempio tramite tecniche di *e-skimming*[1] sui siti 'clone' o *phishing*[2];
  - **diffusione di software malevoli** tramite *marketplace* fraudolenti o siti clone, e finalizzati sempre al furto di identità o scopi estorsivi (*ransomware*);
  - **frodi nei servizi di pagamento**, utilizzando gli identificativi rubati o le carte clonate in precedenza;
  - **resi fraudolenti**, successivi ad acquisti online, che comportano ad esempio la restituzione di versioni contraffatte al posto dei prodotti originali.



1. L'*e-skimming* è una tecnica di *hacking* che ruba le informazioni caricate dai clienti sui siti di shopping online.

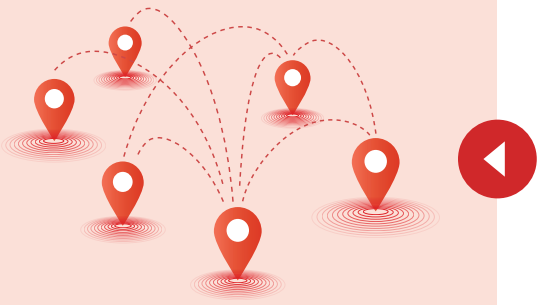
2. Il *phishing* è una tipologia di attacco di *social engineering* che mira a far credere gli utenti che l'e-mail ricevuta provenga da un'istituzione attendibile (es. banca). L'email, che fa riferimento a qualcosa di cui l'utente ha bisogno/vuole, chiede di cliccare su dei link per inserire le proprie credenziali o scaricare un allegato.

Attività di prevenzione e contrasto: le buone pratiche e le sfide



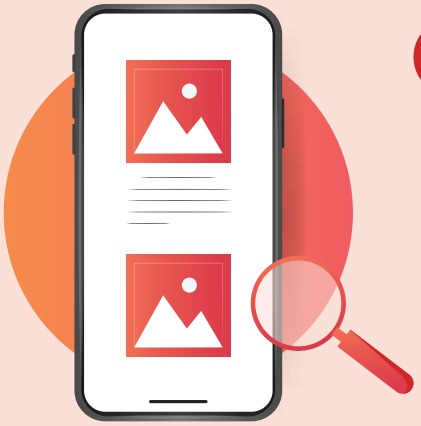
- Assicurare il volume e la prominenza dell'attività di *enforcement* contro la contraffazione dovrebbe rappresentare una priorità. La reintroduzione della contraffazione tra le priorità EMPACT per il ciclo 2022-2025 punta chiaramente in questa direzione, sottolineando l'importanza di rendere i contraffattori responsabili dei loro reati.
- Le buone pratiche per il contrasto alla contraffazione sui mercati online sono identificabili in due principali linee di intervento:
  - la **prevenzione** attraverso il controllo dei (a) prodotti, (b) delle inserzioni e (c) dei venditori sui mercati online;
  - la **collaborazione e lo scambio informativo** tra i diversi stakeholder, in particolare tra forze dell'ordine, *marketplace* e titolari di diritti.
- Nonostante le buone pratiche, esistono diverse sfide da affrontare, in primo luogo le **differenze tra operatori diversi** (piccoli vs. grandi, *marketplace* vs. *social media*) in termini di sensibilità al problema, disponibilità alla cooperazione con le autorità e adozione di strumenti di prevenzione adeguati.
- In particolare, dall'analisi degli studi disponibili, dalle interviste e dai casi studio è emersa una **maggiore vulnerabilità dei *social network*** rispetto ai *marketplace*, anche per l'attività meno sviluppata di *seller vetting* e l'assenza di controlli estesi sulle campagne di sponsorizzazione.

La prevenzione attraverso la verifica di prodotti, mercato e venditori



La prevenzione alla vendita dei 'falsi' sui canali web si concentra su tre linee di controllo:

- La **verifica e il tracciamento dei prodotti** da parte di *brand owner*, tramite soluzioni procedurali o tecnologiche, tra le quali si distinguono le seguenti buone pratiche:
  - l'uso di sistemi di tracciamento di natura materiale, elettronica (es. RFID), chimico-fisica e digitale;
  - l'impiego di soluzioni basate su *blockchain* e *Distributed Ledger Technology* (DLT);
  - l'impiego di altri sistemi di serializzazione;
  - lo sviluppo e uso di soluzioni condivise tra *brand owner* diversi.



- Il **monitoraggio di inserzioni e messaggi su *marketplace*, *social media* e forum**, finalizzato a individuare e rimuovere in maniera tempestiva le pubblicità di 'falsi'. Questo avviene tramite l'impiego, più o meno sviluppato, di:
  - soluzioni per il riconoscimento automatico dei contenuti, come l'*image recognition* di immagini di prodotti contraffatti;
  - l'analisi testuale finalizzata a individuare contenuti falsi e testi fraudolenti;
  - l'individuazione di recensioni anomale o ricorrenti che potrebbero nascondere frodi o vendita di 'falsi';
  - lo *screening* dei siti per individuare siti 'clone' e vetrine fraudolente di prodotti.

- L'**adeguata verifica dei venditori** (*Know Your Business Customer* o *Seller vetting*) finalizzata a censire i venditori (o gli aspiranti tali) ed evitare che siano accreditate presso *marketplace* e *social network* società, magari di comodo, utilizzate per vendere 'falsi'. Tuttavia:
  - la conoscenza sulle pratiche di *seller vetting* è limitata, anche per le difficoltà degli operatori di condividere pubblicamente informazioni a riguardo (a parte qualche eccezione, vedi Sezione 4.1);
  - dall'analisi appaiono differenze significative nelle prassi tra operatori diversi, con i *marketplace* generalmente più attrezzati rispetto, ad esempio, ai *social network* (in cui le pratiche di *on-boarding* sono di fatto assenti);
  - emergono sistemi evoluti di *on-boarding*, che combinano verifiche digitali con verifiche 'materiali' (es. circa la consistenza di indirizzi e caselle postali);
  - ma appare limitato l'uso di indicatori e modelli di rischio più evoluti, che invece risultano già ampiamente impiegati nell'antiriciclaggio e in ambiti limitrofi (es. anticorruzione, 231/2001[3]);
  - non è possibile conoscere il tasso medio di 'respingimento' degli aspiranti venditori, con qualche eccezione (es. per Amazon solo il 6% riesce a concludere il processo di accreditamento).

3. Il Decreto Legislativo n. 231 dell'8 giugno 2001 è una legge italiana che prevede una responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni per alcuni reati commessi commessi nel suo interesse o vantaggio da persone che rivestono funzioni di rappresentanza, amministrazione o direzione dell'ente.

Collaborazione e scambio informativo tra stakeholder

Sia in Italia che all'estero possono essere evidenziate delle buone pratiche in termini di collaborazione e scambio informativo:

- **tra *marketplace*, *brand owner*, operatori postali**: ad esempio in termini di azioni congiunte per perseguire legalmente i contraffattori, o di condivisione di dati su soggetti criminali identificati (al fine di arginare il fenomeno dei trasgressori recidivi);
- **tra autorità pubbliche e soggetti privati**: ad esempio per condividere dati ed informazioni che sono utili alle forze dell'ordine per individuare più velocemente i responsabili della contraffazione sui canali online; e per sensibilizzare consumatori e aziende sui rischi della contraffazione (come nella *Settimana della contraffazione*);
- **tra diverse autorità pubbliche**, come il Desk Interforze Anticontraffazione, coordinato dal Ministero dell'Interno - Servizio Analisi Criminale della Direzione Centrale della Polizia Criminale, o il Consiglio Nazionale per la Lotta alla Contraffazione e all'Italian Sounding (CNALCIS).

Le sfide chiave

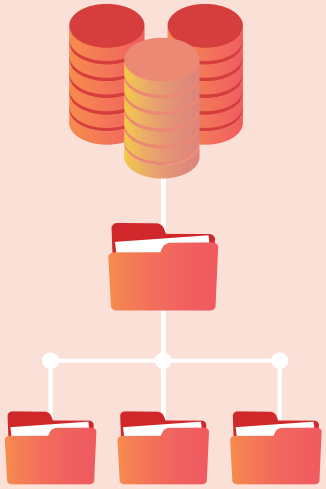
Nonostante le buone pratiche sopra menzionate, la lotta alla contraffazione sui mercati online è ostacolata da due criticità principali che limitano le attività di prevenzione, repressione e contrasto messe in atto dagli *stakeholder* coinvolti, sia del settore privato che di quello pubblico:

- **L'assenza di canali dedicati e le difficoltà nello scambio di informazioni** tra più attori e in diverse direzioni:
  - dalle autorità pubbliche al settore privato: ad esempio dei dati sui sequestri effettuati o sull'esito di procedimenti giudiziari intentati a carico di soggetti segnalati da *marketplace* e *brand owner*;
  - dal settore privato alle autorità pubbliche, asimmetrie rilevanti esistono tra i diversi stakeholder per quanto riguarda la cooperazione e la condivisione dei dati con le forze dell'ordine. Ad esempio, gli intervistati hanno segnalato pratiche di condivisione dati meno consolidate con i social media, se comparate con i *marketplace*;
  - dai *brand owner* agli altri attori, spesso ancora limitato alla condivisione delle tradizionali linee guida sui segni distintivi, nonostante la disponibilità di dati più evoluti (es. tracciati 2D e 3D che faciliterebbero l'individuazione dei falsi);

- nelle condivisioni volontarie tra attori privati e pubblici di informazioni sui soggetti criminali già identificati, di account sospetti o di carte e metodi di pagamento clonati o fraudolenti.

- **Le difficoltà nelle indagini *cross-channel* e *cross-border***. L'interconnessione degli schemi e dei canali usati dai contraffattori, e la loro natura transnazionale, richiede un approccio integrato che è però ostacolato da:
  - la segmentazione delle autorità di contrasto, che rende difficile un dialogo unico tra e con le diverse unità specializzate che si occupano di contraffazione, frodi, reati economici e *cybercrime*;
  - i problemi nella cooperazione internazionale, soprattutto con alcuni paesi extra-UE e in particolare quando è difficile determinare in maniera chiara il principio di territorialità.

Raccomandazioni e direzioni future di intervento



Dall'analisi delle nuove minacce, e delle vulnerabilità nei sistemi di contrasto, emergono **tre direzioni future** con delle proposte specifiche di intervento:

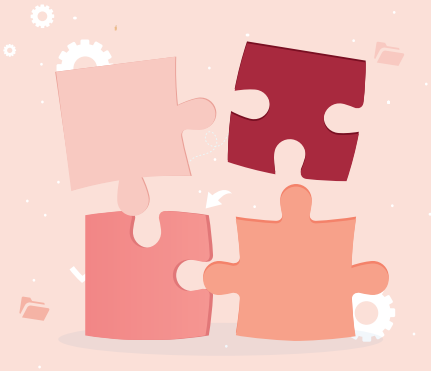
Rafforzare il monitoraggio del fenomeno

- **Istituire un osservatorio scientifico di monitoraggio** che possa creare, gestire e aggiornare una **banca dati**:
  - contenente schemi e casistiche (anonimizzate) di contraffazione sul web e di comportamenti fraudolenti sui mercati online;
  - accessibile ad autorità pubbliche e *stakeholder* privati;
  - ispirata a iniziative simili in ambito antiriciclaggio (es. raccolte di Modelli e schemi di comportamenti anomali pubblicate dall'UIF – Unità di Informazione Finanziaria).

Potenziare capacità tecnologiche ed analitiche

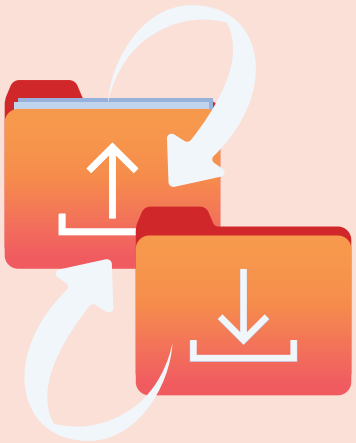
- **Sviluppare e diffondere nuovi strumenti di analisi e di *early-detection***, soprattutto tra quegli operatori meno attrezzati, anche facendo leva sulle risorse e le opportunità messe a disposizione dal PNRR (es. la possibilità di costituire *Partenariati estesi (PE)* con le università sui temi dell'Intelligenza Artificiale e del Made in Italy).

- **Formare i soggetti pubblici e privati sui temi del *data analytics*** con corsi dedicati per illustrare gli strumenti disponibili, le loro potenzialità, e discutendone i vincoli a livello tecnologico e legale, in primis quelli legati alla privacy.



Espandere cooperazione e scambio informativo

- **Creare una nuova alleanza tra gli *stakeholder***, nella forma di gruppo di lavoro stabile e multidisciplinare che sia in linea con le nuove forme della contraffazione online, e quindi possa:
  - raggruppare autorità pubbliche (forze dell'ordine, autorità giudiziaria, agenzie di supervisione e protezione della filiera legale) e soggetti privati (mercati online, *social media*, titolari di diritti, operatori postali e di logistica, servizi di pagamento);
  - includere le autorità attive nel contrasto ai reati *cyber* (es. Polizia postale, ACN - Agenzia per la cybersicurezza nazionale) e le autorità di *intelligence* finanziaria (es. Banca d'Italia – UIF);
  - includere centri di ricerca scientifica ed università.



- **Esplorare dei nuovi meccanismi di scambio e condivisione delle informazioni** tra gli *stakeholder*, anche riservate, al fine di moltiplicare la prevenzione e l'*early-detection* condivisa, potenziare le economie di scala e ridurre i costi ricorrenti. Questi nuovi sistemi potrebbero:
  - basarsi su tecnologie evolute di scambio sicuro e anonimizzato (es. *federated learning*);
  - prendere spunto da progetti simili lanciati in altri paesi (es. la collaborazione tra Amazon ed altri *marketplace* negli Stati Uniti per realizzare sistemi di scambio di informazioni su contraffattori verificati);
  - ispirarsi a sistemi di condivisione lanciati in altri ambiti (es. tra i soggetti obbligati antiriciclaggio nei Paesi Bassi e a Singapore);
  - rispettare gli obblighi delle parti coinvolte, e la normativa vigente in termini di protezione dei dati personali, tutela dei diritti dei consumatori e della libertà di iniziativa imprenditoriale.

- Sostenere **le modifiche legislative o le indicazioni della Commissione** per chiarire aspetti legati alla privacy o altri temi, in modo da incentivare i diversi stakeholder a scambiare dati.

Prefazione

A cura del Ministero dell'Interno – Dipartimento della Pubblica Sicurezza – Direzione Centrale della Polizia Criminale – Servizio Analisi Criminale

Il fenomeno della contraffazione, al quale sono strettamente correlati quelli della pirateria multimediale e dell'abusivismo commerciale, risulta essere una delle più rilevanti, consolidate e trasversali forme di criminalità economica, ormai quasi del tutto appannaggio della criminalità organizzata transnazionale.

Si tratta di un'attività illegale che:

- si manifesta in modo articolato, strutturandosi in almeno quattro fasi (produzione, trasporto, distribuzione all'ingrosso e vendita al dettaglio), secondo i canoni della "catena di fornitura" o filiera, tipica dei sistemi economici avanzati;
- si caratterizza per la capacità di adeguarsi, con rapidità, all'evoluzione del commercio internazionale, allo sviluppo delle nuove tecnologie ed ai mutamenti degli orientamenti e delle esigenze dei consumatori nonché per la reattività con cui è in grado di adottare proprie contromisure alle strategie di contrasto predisposte dalle Forze di polizia.

Le analisi quantitative più aggiornate e affidabili sulle dimensioni del commercio mondiale di prodotti contraffatti e usurpativi (EUIPO e OECD 2021a), stimano che, nel 2019, il volume del commercio internazionale di tali prodotti sia stato di ben 464 miliardi di dollari U.S.A., pari al 2,5% del commercio mondiale e che, nello stesso anno, le importazioni di prodotti falsi nell'Unione Europea siano state pari al 5.8% delle importazioni complessive, per un ammontare di 119 miliardi di euro[4].

In tale contesto, recenti studi rivelano che l'Italia è, dopo gli Stati Uniti d'America, il paese al mondo maggiormente penalizzato dalla contraffazione e dalla pirateria (OECD 2018).

Da un punto di vista merceologico, il fenomeno - in origine circoscritto quasi esclusivamente ai beni di lusso - si è esteso gradualmente alle più diverse categorie di prodotto, al punto che ogni tipo di articolo al quale la proprietà intellettuale aggiunge un valore economico e quindi crea differenziali di prezzo, è attualmente oggetto d'interesse per la contraffazione o la pirateria, inclusi quelli particolarmente sensibili sotto il profilo della salute (medicinali, alimenti, tabacchi, ecc.) e della sicurezza (ad es. giocattoli, trapani elettrici).

Negli ultimi anni si è assistito ad un notevole aumento della falsificazione dei cd. dispositivi "ITC", categoria nella quale rientrano telefoni cellulari, computer, tablet, lettori DVD, cuffie, auricolari, microfoni, ecc.: nel loro insieme, costituiscono il comparto che assicura, oggi, i maggiori ricavi illeciti. Dal punto di vista quantitativo, invece, gli articoli in pelle, giochi e giocattoli, capi di abbigliamento, calzature, orologi e occhiali risultano essere ancora le merci più diffuse nei circuiti illegali.

I principali fattori che, combinandosi tra loro, hanno determinato l'espansione dell'"industria del falso" verificatasi negli ultimi decenni, possono essere così sintetizzati:

- la situazione di crisi che investe molte piccole imprese;

4. Secondo precedenti rapporti OCSE-EUIPO, realizzati con la stessa metodologia, il commercio di prodotti contraffatti e usurpativi aveva costituito il 2.5% del commercio mondiale nel 2013 e il 3.3% nel 2016, per un valore, rispettivamente, di 461 miliardi di USD e 509 miliardi di USD. Pertanto, sia in valori assoluti che in termini percentuali, il valore del commercio di falsi è rimasto, negli ultimi anni, a livelli costantemente elevati, approssimandosi al valore del prodotto interno lordo di paesi quali l'Austria o il Belgio.

- la crescita della disoccupazione, che induce i lavoratori a rendersi disponibili a fornire prestazioni lavorative in modo clandestino, occasionale e a basso costo;
- la razionalizzazione dei processi produttivi, da parte delle grandi e medie imprese, mediante la delocalizzazione e l'esternalizzazione di alcune fasi intermedie, con la conseguente esposizione al rischio di appropriazione indebita di "*know-how*" industriale;
- la crescente disponibilità sul mercato di strumenti e attrezzature tecniche capaci di rendere agevole la duplicazione dei prodotti tutelati;
- la tendenza consolidata, da parte dei consumatori, a ricercare e acquistare articoli anche falsi, a condizione che siano "griffati", in quanto ritenuti rappresentativi di un certo stile di vita;
- l'incremento dei grandi flussi migratori clandestini, atteso che i cittadini stranieri, presenti illegalmente nel territorio dello Stato, possono, in modo facile e immediato, trarre i mezzi di sostentamento vendendo abusivamente merce falsa o facendosi reclutare per il confezionamento della stessa;
- l'indulgenza o tolleranza nei confronti della contraffazione e della pirateria da parte dell'opinione pubblica, da ricondurre ad una scarsa conoscenza degli effetti dannosi di questi fenomeni;
- l'interesse della criminalità organizzata, che ha compreso le rilevanti opportunità di arricchimento illecito offerte da questo "business", ad alta redditività e a basso rischio, per il quale i sodalizi coinvolti possono approfittare di quelle forme di "controllo illegale del territorio" di cui si avvalgono anche per altre attività delittuose, nonché dell'esperienza da essi storicamente acquisita in altri settori illeciti, come il contrabbando di t.l.e. ed il traffico internazionale di sostanze stupefacenti, che richiedono, per le loro articolate dinamiche, organizzazioni criminali strutturate, capaci di infiltrarsi nelle grandi infrastrutture del trasporto e di gestire una composita e sofisticata rete di persone e di risorse indispensabili al funzionamento della filiera illecita[5]. È stato, pertanto, agevole l'inserimento degli stessi sodalizi anche nel business del "falso", nel momento in cui è apparso evidente che il rapporto costi/benefici era sensibilmente sbilanciato a favore di quest'ultimi.

Ministero dell'Interno – Dipartimento della Pubblica Sicurezza – Direzione Centrale della Polizia Criminale – Servizio Analisi Criminale

La Direzione Centrale della Polizia Criminale, attraverso il Servizio Analisi Criminale, struttura a composizione interforze ove operano appartenenti alla Polizia di Stato, all'Arma dei Carabinieri, alla Guardia di Finanza e alla Polizia Penitenziaria, cura, in collaborazione con le Prefetture, il sistema di monitoraggio denominato "Co.Ab." (Contraffazione e Abusivismo), che consente la raccolta dei dati relativi alle operazioni eseguite ed ai risultati conseguiti in questo settore, dalle Forze di polizia e dalle Polizie Municipali.

Il citato Servizio ha fornito il proprio contributo anche nell'ambito del documento di valutazione della minaccia S.O.C.T.A. (*Serious and Organised Crime Threat Assessment*), in sinergia con il MISE, finalizzato a fornire lo scenario aggiornato su diverse aree criminali, quali "food fraud", "contraffazione del tessile", "pharma crime", "piracy online" e "product counterfeiting and intellectual property crime".

Il citato contributo, utilizzato dagli analisti di Europol per la redazione del documento finale, è stato sottoposto al C.O.S.I. (Comitato permanente per la Cooperazione Operativa in materia di Sicurezza Interna) ed approvato per il prossimo ciclo programmatico dell'Unione Europea per il periodo 2022-2025. Pertanto, la fase operativa E.M.P.A.C.T. (*European Multidisciplinary Platform Against Criminal Threats*) avrà tra le priorità anche quella del contrasto alla contraffazione e della tutela della proprietà intellettuale.

5. Nel contrabbando di tabacchi lavorati esteri, oltre alla gestione della rete dei "contatti" necessari per l'approvvigionamento ed il pagamento delle partite illecite e ad un rilevante apparato logistico idoneo alla ricezione, alla custodia ed al trasporto delle sigarette, occorre disporre anche di figure professionali in grado di provvedere alla predisposizione della documentazione fittizia indispensabile per eludere eventuali controlli e per procedere all'inoltro verso le successive tappe della spedizione.

A cura di Crime&tech – spin-off di Transcrime – Università Cattolica del Sacro Cuore

La crescita dell'*e-commerce* e dei consumi sui mercati online ha portato il fenomeno della contraffazione ad un'altra dimensione. Difficile da quantificare, ma sicuramente caratterizzata da nuovi attori, schemi criminali, *modi operandi* e reati. Ormai la vendita di 'falsi' sul web si accompagna ad un corollario più ampio di reati economici e finanziari, come ad esempio le frodi con i servizi di pagamento, il furto di identità e altre forme di criminalità *cyber*. Non più un solo reato quindi, ma un vero e proprio *fraudster journey*, un viaggio fraudolento, così come definito da uno dei soggetti intervistati per questo studio.

L'emergere di queste nuove forme non solo muta il profilo degli attori criminali coinvolti, ma anche quello delle vittime, che si allarga, includendo anche una serie di consumatori e utenti del web, spesso inconsapevoli o vulnerabili e poco equipaggiati. Di conseguenza, viene a moltiplicarsi anche il danno generato sui consumatori, le imprese, il sistema pubblico.

Le difficoltà ad indagare la contraffazione sui mercati online, e la carenza di studi sull'argomento, non possono che generare in noi un interesse di ricerca e di approfondimento. Come Crime&tech, spin-off del centro Transcrime-Università Cattolica del Sacro Cuore, abbiamo avuto la fortuna di poterlo coltivare insieme al Ministero dell'Interno e con il supporto di Amazon.

Con loro abbiamo prodotto questo studio che è solo uno dei risultati del progetto *FATA – From Awareness To Action*. FATA nasce proprio dall'intenzione di combinare l'esperienza e le conoscenze delle autorità pubbliche, da un lato, e dei mercati online, dall'altro; ovvero di chi è, oggi, in prima linea nel contrasto alle nuove forme della contraffazione online. E di condividere questa conoscenza con tutti quei soggetti (operatori dell'*e-commerce* e della logistica, titolari di diritti intellettuali, enti pubblici, consumatori) che hanno, in modo diverso, a che fare in questo ambito.

Riteniamo che FATA possa essere la prima pietra di un **osservatorio costante di monitoraggio** sui nuovi schemi della contraffazione online che tutti – ricercatori, autorità pubbliche, soggetti privati – avranno il compito di alimentare ed aggiornare. FATA è il primo risultato di una nuova alleanza tra il settore pubblico e il settore privato, e, speriamo, il primo seme di nuovo paradigma di prevenzione e di contrasto alla contraffazione online, finalmente integrato e capace di stare al passo con l'evoluzione di questo fenomeno criminale.

Crime&tech - Università Cattolica del Sacro Cuore

Crime&tech srl è lo spin-off di Transcrime, il centro di ricerca sulla criminalità transnazionale dell'Università Cattolica del Sacro Cuore. Crime&tech traduce le ricerche di Transcrime in servizi di *data analytics* e strumenti tecnologici per la valutazione, l'identificazione e la prevenzione dei rischi criminali. Inoltre supporta soggetti pubblici e privati in diversi ambiti, tra cui l'antiriciclaggio, l'anticorruzione e la prevenzione delle frodi nel settore retail.

A cura di Amazon

In Amazon, abbiamo una politica di tolleranza zero nei confronti di contraffazione e pirateria: siamo consapevoli dell'importanza di proteggere i consumatori, i marchi e il nostro store dai prodotti contraffatti, e lavoriamo duramente per farlo.

Secondo le stime di Netcomm, oggi 29 milioni di italiani acquistano abitualmente online[6]. Tutti meritano di ricevere i prodotti autentici che hanno acquistato. Il sistema di competitività del paese deve essere protetto e i contraffattori non dovrebbero poter praticare una concorrenza sleale nei confronti degli imprenditori onesti e privare i proprietari di marchi del valore della loro proprietà intellettuale.

La pandemia ha giocato da acceleratore del commercio online, ma ha anche attirato malintenzionati che hanno cercato di trarre vantaggio da questa situazione. Nonostante i loro tentativi, abbiamo continuato a fare notevoli progressi e a garantire ai nostri clienti un'esperienza di acquisto affidabile attraverso solidi controlli proattivi e potenti strumenti di protezione per i marchi, aumentando l'impegno nei contenziosi e la collaborazione con le forze dell'ordine.

Nel solo 2020, Amazon ha investito più di 700 milioni di dollari (600 milioni di euro) nel mondo, e abbiamo impiegato oltre 10.000 dipendenti esclusivamente in attività di contrasto a frodi, contraffazione e abusi. Queste attività hanno permesso di fermare oltre 6 milioni di tentativi di creare un account di vendita prima che venisse pubblicato un solo annuncio, e hanno fatto si che meno dello 0,01 per cento dei prodotti venduti su Amazon lo scorso anno generasse una lamentela da parte dell'acquirente per motivi di contraffazione. Pur essendo fieri dei progressi compiuti, sappiamo che la contraffazione rimane un problema persistente nel settore retail e che i malintenzionati non si fermeranno, ma sposteranno le loro operazioni su altri canali, inclusi i loro siti Web, mercati online, canali offline e altro ancora.

La complessità della contraffazione online aumenterà di pari passo ai cambiamenti del mercato e all'innovazione tecnologica. Riteniamo di importanza strategica indagare i nuovi scenari e comprendere la portata e la natura dei legami esistenti con altri fenomeni criminali. Come ha affermato il Ministero dello Sviluppo Economico, «un moderno approccio alla protezione della proprietà industriale non può limitarsi a "giocare sulla difensiva"»[7], è necessario approfondire la conoscenza della contraffazione online al fine di adattare e indirizzare efficacemente le politiche di prevenzione e contrasto.

Inoltre, è sempre più evidente che dobbiamo apportare cambiamenti profondi nel modo in cui collaboriamo tra settori per fermare i contraffattori. In Amazon, crediamo fermamente che sia necessaria una partnership rafforzata tra l'industria e i governi nazionali per proteggere meglio le nostre frontiere dalle merci contraffatte e per fermare i contraffattori accertati nel settore della vendita al dettaglio.

Allo stesso modo, riteniamo che l'azione penale per contraffazione debba essere considerata una priorità, ancor più perchè talvolta è il presupposto di attività molto più efferate. A tal fine, dovrebbero essere assegnate maggiori risorse alle autorità di contrasto, e riteniamo che il reinserimento della contraffazione tra le priorità della piattaforma multidisciplinare dell'Unione europea contro le minacce criminali (EMPACT) sia un passo importante in questa direzione.

6. https://www.consorzionetcomm.it/il-lockdown-triplica-i-nuovi-consumatori-online-in-italia-tra-gennaio-e-maggio/
7. Ministero dello Sviluppo Economico. 2021. Linee di intervento strategiche sulla proprietà industriale per il triennio 2021-2023, pag. 7. https://uibm.mise.gov.it/images/LINEE_DI_INTERVENTO_approvate.pdf

Il progetto FATA nasce da una profonda riflessione su tutto quanto sopra e dalla necessità di comprendere a fondo le caratteristiche dell'attuale mercato della contraffazione online.

Due eccellenti istituzioni hanno collaborato a questo fine, il Servizio Analisi Criminale del Ministero dell'Interno, impegnato nella raccolta e analisi dei dati e nella elaborazione di atti di indirizzo a livello nazionale, e Crime&Tech dell'Università Cattolica del Sacro Cuore di Milano, centro di ricerca di fama internazionale. Siamo fieri di aver avuto l'opportunità di sostenere il loro lavoro, e speriamo di collaborare con loro per promuovere sinergie, incoraggiare politiche di prevenzione integrate e facilitare l'aggiornamento della normativa affinché i contraffattori siano indagati e rispondano di fronte alla legge.

Amazon

Amazon è guidata da quattro principi: ossessione per il cliente piuttosto che attenzione verso la concorrenza, passione per l'innovazione, impegno per l'eccellenza operativa e visione a lungo termine. Amazon punta ad essere l'azienda più attenta al cliente al mondo, il miglior datore di lavoro al mondo e il luogo di lavoro più sicuro al mondo. Le recensioni dei clienti, lo shopping 1-Click, le raccomandazioni personalizzate, Prime, Logistica di Amazon, AWS, Kindle Direct Publishing, Kindle, Career Choice, i tablet Fire, Fire TV, Amazon Echo, Alexa, la tecnologia Just Walk Out, Amazon Studios e il Climate Pledge sono alcune delle innovazioni introdotte da Amazon. Per maggiori informazioni, visitate il sito www.aboutamazon.it e seguite Amazon.it su Instagram, Facebook e Twitter.

1.

Introduzione

1.1 Perché questo studio

La globalizzazione dei mercati, la diffusione delle **tecnologie dell'informazione (ICT) e la crescita dell'*e-commerce*** hanno fortemente rivoluzionato il settore del commercio negli ultimi anni. Questi cambiamenti hanno rappresentato un'**opportunità unica sia per le imprese**, che hanno avuto accesso a nuovi mercati, sia per i **consumatori**, che hanno oggi la possibilità di acquistare una maggiore varietà di prodotti, a prezzi più competitivi, e tramite modalità più veloci e sicure di approvvigionamento.

Dall'altra parte, questi mutamenti hanno creato anche **nuove opportunità per la distribuzione di beni di natura o origine illecita**, in particolare di beni contraffatti. Oltre ai canali tradizionali di vendita - bancarelle, venditori ambulanti, negozi abusivi - e, in misura minore, la filiera produttiva legale (Guardia di Finanza 2020b) - negli ultimi anni la vendita di 'falsi' è cresciuta anche sui **mercati online** (Europol 2021). Se da una parte i canali tradizionali di vendita sono ancora predominanti, dall'altra i contraffattori utilizzano anche l'*e-commerce* e le aste sul web per sfruttare la crescita degli acquisti online (vedi Box 1), e quindi dell'ampio potenziale bacino di vittime, ma anche una serie di fattori che ne agevolano l'utilizzo a scopi illeciti (Consiglio Nazionale Anticontraffazione 2019). In particolare:

- una relativa facilità per gli autori degli illeciti di **occultare la propria identità**, ad esempio dietro società di comodo o soggetti prestanome utilizzati come *seller*;

- l'**ampia scelta** di piattaforme/canali da utilizzare, anche in maniera contestuale, e la relativa facilità di muoversi tra gli stessi;

- la possibilità di raggiungere velocemente un **numero sempre crescente di consumatori**, non sempre consapevoli e comunque caratterizzati da una scarsa cultura della sicurezza informatica.

Questi fattori - che saranno poi discussi nel dettaglio nei prossimi paragrafi - oltre a favorire la vendita di prodotti contraffatti, espongono i consumatori ad altre forme di criminalità, e sono anche in grado di ostacolare in modo significativo l'efficacia delle **azioni di prevenzione e di contrasto**.

Box 1. La crescita dell'*e-commerce* durante la pandemia

Secondo l'ultima rilevazione dell'indagine *E-commerce statistics for individuals* (Eurostat 2021), circa il 73% degli utenti di internet ha fatto acquisti online nel 2020, una percentuale in aumento rispetto al 62% del 2015, con un'incidenza elevata tra gli individui di età compresa tra i 16-24 anni (78%) e i 25-54 anni (79%). In aggiunta, come riportato dall'OECD (2020), la diffusione del COVID-19 ha avuto un forte impatto sulla crescita dell'*e-commerce*. Nell'aprile 2020, gli acquisti di prodotti online nell'Unione Europea sono aumentati del 30% rispetto all'aprile all'anno precedente. Il COVID-19 ha inoltre modificando alcuni *pattern* d'acquisto, spingendo anche consumatori non abituali (es. persone anziane) ad acquistare prodotti online. Anche se la maggior parte degli acquisti sono effettuati ancora tramite canali fisici, la pandemia ha accelerato la diffusione dei canali online per la vendita di beni.

Come segnalato da un recente rapporto congiunto di Censis e Ministero dello Sviluppo Economico (2021), la pandemia di COVID-19 ha avuto una forte ricaduta anche sul mercato della contraffazione. Sebbene i beni contraffatti siano ancora venduti prevalentemente tramite canali fisici, i contraffattori si sono adeguati al nuovo scenario (es. rallentamento dei collegamenti internazionali, rafforzamento dei controlli stradali, difficoltà nello spostamento di grandi carichi di prodotti) e l'offerta dei prodotti contraffatti si è spostata sui mercati online dove, accanto ai 'falsi' tradizionali, sono comparsi prodotti altamente richiesti dalla clientela durante la pandemia (es. dispositivi di protezione individuale, igienizzanti, farmaci e test diagnostici). Numerose le indagini e gli studi che hanno svelato l'immissione massiva di dispositivi medici contraffatti sui mercati a livello nazionale ed internazionale (OECD e EUIPO 2020; Ministero dell'Interno 2021), così come intensa è stata l'attività da parte dei *marketplace* e la collaborazione con le forze dell'ordine. Ad esempio:

- Amazon nel 2020 ha rimosso proattivamente oltre 6.5 milioni di prodotti sanitari (es. disinfettanti, mascherine) perché fraudolentemente venduti come efficaci contro il COVID-19 ed ha chiuso gli account di più di 10.000 seller che vendevano invece prodotti sanitari ad un prezzo molto più elevato del normale (ICE 2020). Amazon ha inoltre preso parte (insieme a Pfizer, 3M, Citi e Alibaba) alla task-force organizzata dall'*Homeland Security Investigations* (HSI) e il *National Intellectual Property Rights Coordination Center* (IPR Center) per constrare le frodi legate alla pandemia COVID-19 (ICE 2020);
- Alibaba nel 2020 ha supportato l'attività di enforcement delle forze dell'ordine di 29 province cinesi in 1.711 casi riguardanti la vendita di prodotti contraffatti legati alla pandemia, contribuendo attivamente all'arresto di 716 contraffattori (Alibaba Group 2020).

Nonostante la rilevanza di questo tema, lo studio di come la contraffazione utilizzi l'*e-commerce* è ancora ai minimi termini. In Italia nessuna ricerca ha mai analizzato in modo sistematico l'evoluzione e i *modi operandi* della contraffazione sui mercati online, né delle contromisure messe in atto da autorità pubbliche ed imprese private per prevenirla. Da una parte, questo gap conoscitivo mina la capacità di individuare, indagare e perseguire legalmente i contraffattori; dall'altra, mina la fiducia dei consumatori che spesso non sanno da chi stanno realmente acquistando i loro prodotti e potrebbero perdere la fiducia negli acquisti online.

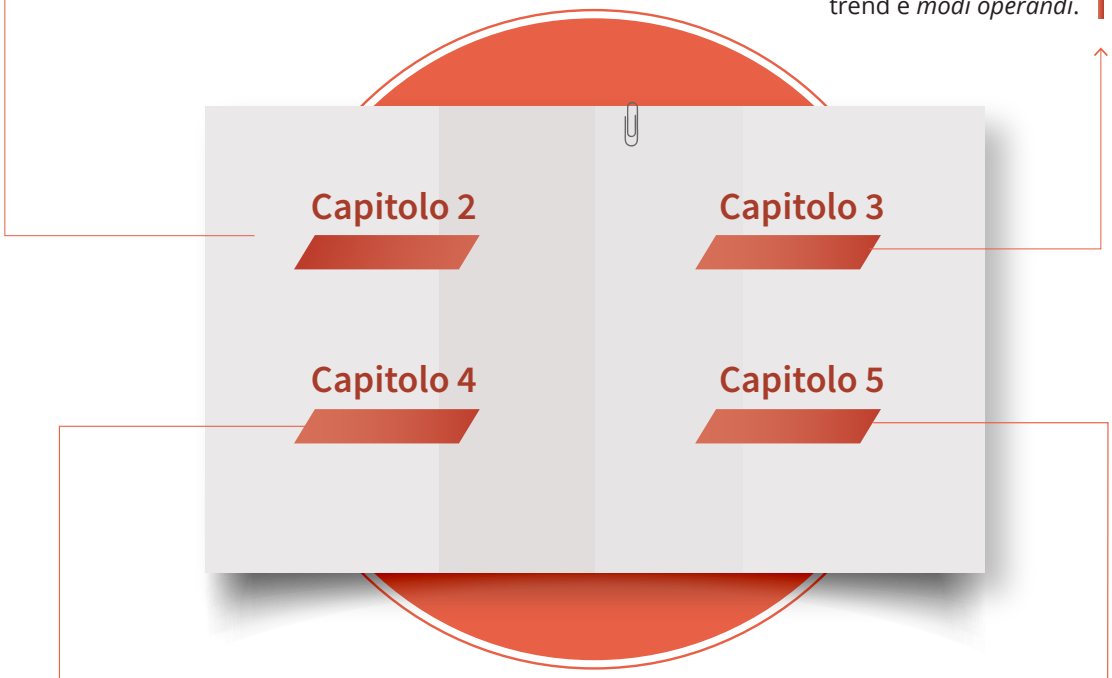
Da qui nasce il progetto FATA – From Awareness to Action, risultato della collaborazione tra mondo della ricerca, autorità pubbliche e settore privato. In particolare, questo studio, realizzato da Crime&tech, spin-off dell'Università Cattolica del Sacro Cuore-Transcrime, e dal Ministero dell'Interno, con il supporto di Amazon, si pone i seguenti obiettivi:

- fare luce sulle **nuove forme e *modi operandi*** legati alla contraffazione nell'*e-commerce*, in particolare sull'utilizzo contestuale di canali diversi e di strutture societarie fittizie per la vendita di beni contraffatti;
- aumentare la **consapevolezza** sui forti legami tra la contraffazione e altre forme di criminalità organizzata, finanziaria e *cyber*;
- migliorare la **collaborazione tra settore pubblico** e privato (operatori di *e-commerce*, titolari di diritti intellettuali, aziende di logistica);
- promuovere **nuove iniziative e strumenti** per aumentare l'efficacia delle azioni di contrasto al fenomeno.

Il report è organizzato come segue:

Il **Capitolo 2** illustra brevemente la metodologia e le fonti dati utilizzate dallo studio.

Il **Capitolo 3** fornisce una panoramica sulle principali caratteristiche del fenomeno contraffazione nell'*e-commerce*, concentrandosi in particolare sugli attori, i canali utilizzati e i nuovi trend e *modi operandi*.



Il **Capitolo 4** presenta le principali sfide alle attività di prevenzione e contrasto, e le buone pratiche a livello pubblico e privato.

Il **Capitolo 5** fornisce delle raccomandazioni e discute alcune direzioni future di ricerca, di *policy* e collaborazione in questo ambito.

1.2 Le dimensioni della contraffazione sui mercati online

1.2.1 Un fenomeno sottostimato?

Le stime esistenti sul mercato della contraffazione derivano da metodologie, più o meno raffinate, basate su statistiche legate al **consumo** (*demand-based*) o ai **sequestri di merce** contraffatta (*seizure-based*). Tra le ultime, il report di OECD-EUIPO (2021b) stima il volume dei beni contraffatti, al 2019, pari a 461 miliardi di dollari a livello globale (il 2,5% del valore del commercio mondiale). In Europa, uno studio di Transcrime del 2015 (Camerini, Favarin, e Dugato 2015), utilizzando dati sui sequestri doganali e sui *pattern* di acquisto dei consumatori di prodotti contraffatti sui canali online e offline – quest'ultimi raccolti dall'OHIM tramite una

survey (OHIM 2013) - stimava il valore complessivo del consumo di beni contraffatti pari a circa 41 miliardi di euro all'anno. Nonostante siano già sintomatiche della gravità e delle dimensioni del problema, queste misure **non riescono quasi mai a distinguere la nuova componente online** della contraffazione da quella 'fisica' tradizionale e rischiano quindi di **sottostimare un fenomeno che appare** invece, a giudicare da altri segnali discussi di seguito, in aumento.

Anche le statistiche amministrative sui **reati di contraffazione denunciati** e sui **soggetti deferiti all'autorità giudiziaria** (vedi Box 2) non forniscono una rappresentazione adeguata dell'entità del fenomeno a causa dell'elevato *numero oscuro* (cioè del tasso di non denuncia) e dello spostamento della contraffazione sui mercati online:

- da un lato, i consumatori vittime di frodi e di vendita di 'falsi' sul web hanno ancora meno incentivi a riportare i comportamenti illeciti alle autorità competenti. Questo avviene per varie ragioni, tra le quali l'ampio ricorso al *chargeback* (rimborso) che disincentiva la denuncia all'autorità competente;
- dall'altro, per le autorità, come illustrato nel capitolo 3, è molto difficile individuare autori di reato che si nascondono dietro account e pseudonimi virtuali e che sono in grado di muoversi tra canali di vendita e giurisdizioni diverse.

La scarsa rappresentatività delle statistiche ufficiali è stata ulteriormente esacerbata, negli ultimi anni, dall'esclusione, nel triennio 2018-2021, della contraffazione dall'**EMPACT** (***European Multidisciplinary Platform Against Criminal Threats***),[8] che ha inevitabilmente dirottato risorse e attenzione delle forze dell'ordine verso altri fenomeni criminali ricompresi tra le priorità dell'azione anticrimine europea, e che può in ultima istanza avere impattato sulla riduzione del numero di reati e di soggetti denunciati per reati di contraffazione.

1.2.2 I segnali dell'aumento della contraffazione online (ma l'offline è ancora predominante)

Nonostante l'assenza di stime affidabili sulle dimensioni dei 'falsi' sul web, sono diversi i segnali e i numeri - di diversa natura - che suggeriscono come la **contraffazione sui mercati online sia in espansione**. Allo stesso tempo, ci sono dati che indicano come, sia in termini di volume che di valore, i canali di vendita fisici siano ancora predominanti:

- un recente report di OECD ed EUIPO (2021b) sul **traffico di beni contraffatti collegati ad acquisti *e-commerce***, basato sui sequestri condotti dalle autorità doganali degli Stati Membri dell'Unione Europea, fa emergere che:
    a. il **56%** dei beni contraffatti sequestrati nell'Unione Europea nel periodo 2017-2019 è attribuibile a prodotti venduti online. Tuttavia, in termine di valore economico, **solo il 14% dei beni contraffatti sono attribuibili ai canali online** (Figura 1);
    b. mentre per la contaffazione online le *small parcel*[9] sono diventate fondamentali (vedi Capitolo 3), la maggior parte dei beni contraffatti sequestrati nell'Unione Europea sono legati alla contraffazione offline e spediti tramite altri canali (es. *container*) (OECD e EUIPO 2021a);

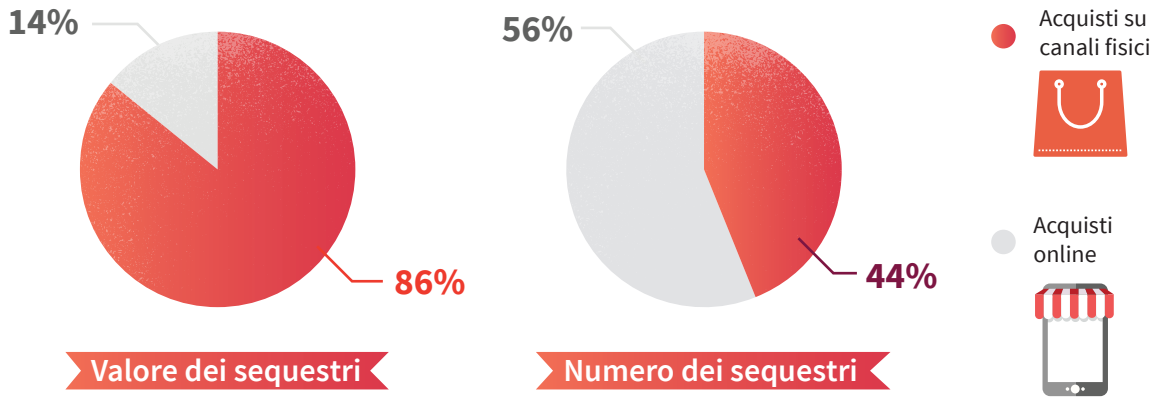
8. L'EMPACT rappresenta l'approccio integrato alla sicurezza interna dell'Unione Europea. L'EMPACT definisce periodicamente delle priorità di azione congiunta, rappresentando lo strumento *flagship* per la cooperazione operativa multidisciplinare e multilaterale al contrasto e alla prevenzione della criminalità organizzata a livello UE (https://www.europol.europa.eu/empact).

9. Il termine 'small parcel' fa riferimento a pacchi contenenti meno di tre oggetti che possono essere sequestrati tramite la procedura semplificata.

c. è anche importante sottolineare che, in questo report, OECD e EUIPO utilizzano la definizione di contraffazione contenuta nel 'Trade-Related Aspects of Intellectual Property Rights' del *World Trade Organization* (vedi sezione 2.1 per maggiori informazioni), che si riferisce ad un più ampio insieme di beni che violano marchi registrati, diritti d'autore e brevetti.

Purtroppo, lo studio – il primo nel suo genere dedicato al mondo dell'*e-commerce* – non riporta dati per l'Italia, ma solo aggregati a livello europeo.

Figura 1. Distribuzione di valore e numero dei sequestri di prodotti contraffatti acquistati online e su canali fisici.
Fonte: OECD e EUIPO (2021b)



- **l'11% delle conversazioni sui *social network* che hanno a che fare con prodotti fisici** si riferiscono a dei 'falsi', secondo un altro recente studio di EUIPO (2021c);

- uno studio recente (Stroppa et al. 2019) ha individuato su Instagram ben 56.769 account utilizzati per vendere prodotti contraffatti, un **aumento del 171%** rispetto ai 20.892 account individuati nell'edizione precedente dello studio, condotta con la stessa metodologia (Stroppa e Di Stefano 2016). Questi account, nel solo 2019, avrebbero pubblicato oltre 64 milioni di post e, in media, 1.6 milioni di storie ogni mese, avendo la possibilità di raggiungere, solo tramite i propri follower, già più di 20 milioni di utenti;

- su TikTok, i post con *hashtag* riferiti a prodotti contraffatti hanno superato le **100 milioni di visualizzazioni** a livello mondiale (Lince 2020);

- da un'analisi di EUIPO (2021b) di 1.000 domini sul web relativi a 20 *brand owner* selezionati, il **49% sono 'sospetti'** e associati, tra gli altri, alla **vendita di prodotti contraffatti**, la diffusione di malware e la sottrazione di informazioni personali (tramite *phishing*).

Per quanto forniscano una visione incompleta e parziale del fenomeno e nonostante il ruolo ancora prevalente della contraffazione offline, sia le statistiche ufficiali che i dati presentati sopra evidenziano che la contraffazione è **in aumento sui mercati online**, con nuovi schemi, *modi operandi*, canali di vendita, strategie di trasporto e di occultamento. Indagare questa evoluzione è esattamente lo scopo di questo studio.

Box 2 – L'andamento dei reati di contraffazione in Italia (2015-2021)

Paragrafo a cura del Servizio Analisi Criminale della Direzione Centrale della Polizia Criminale - Dipartimento della Pubblica Sicurezza - Ministero dell'Interno

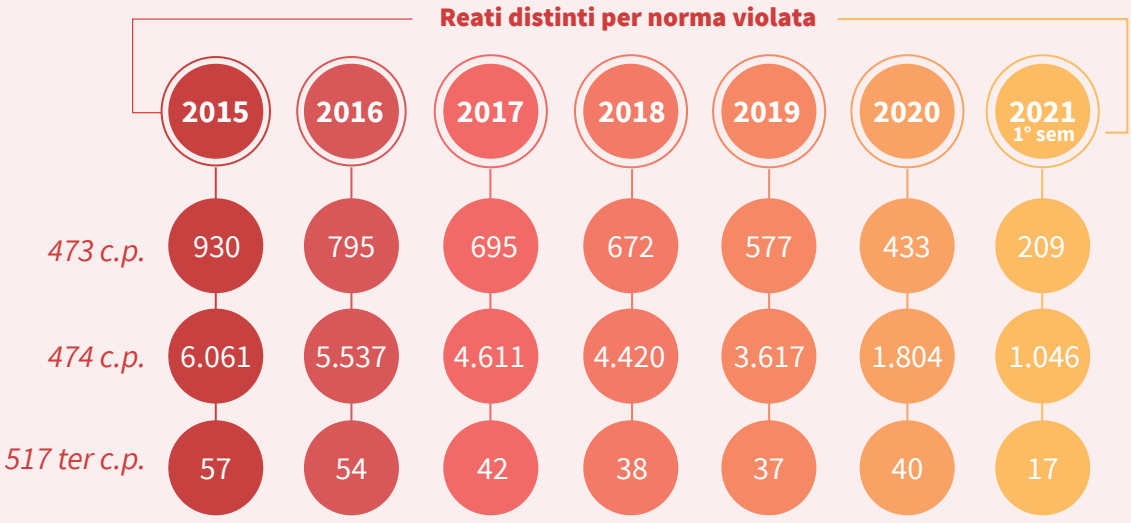
L'incessante attività di contrasto al fenomeno criminale in argomento, condotta dalle Forze di polizia e dalle Polizie locali sull'intero territorio nazionale, ha evidenziato come il numero dei reati, nel periodo 2015 – 2021 (per il 2021 i dati sono riferiti al primo semestre e sono suscettibili di ulteriori variazioni in attesa di consolidamento), abbia una curva tendenzialmente discendente.

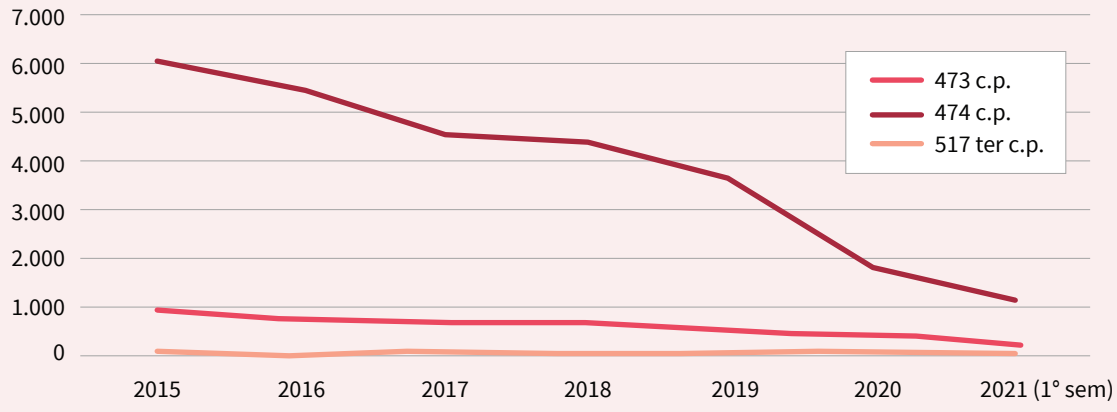
I reati considerati sono quelli previsti dagli articoli 473 c.p. "Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni", 474 c.p. "Introduzione nello Stato e commercio di prodotti con segni falsi" e 517 ter c.p. "Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale".

I dati riportati nella tabella che segue sono stati estrapolati dal Servizio per il Sistema Informativo Interforze, che gestisce il Centro Elaborazione Dati (C.E.D.) del Ministero dell'Interno, ed elaborati dal Servizio Analisi Criminale, articolazioni della Direzione Centrale della Polizia Criminale.

Tabella 1 e Figura 2 – Reati di contraffazione denunciati dalle forze dell'ordine all'Autorità giudiziaria (i dati per il 2021 si riferiscono al primo semestre dell'anno)

Fonte: Elaborazione del Servizio Analisi Criminale su dati del C.E.D. del Ministero dell'Interno.





L'andamento del fenomeno criminale, pur in presenza di un apparato di prevenzione e contrasto tra i più evoluti, fa ritenere che il commercio dei beni contraffatti si stia spostando sulla rete internet, che rende più difficoltosa l'identificazione dei responsabili ed il perseguimento dei reati sopra indicati.

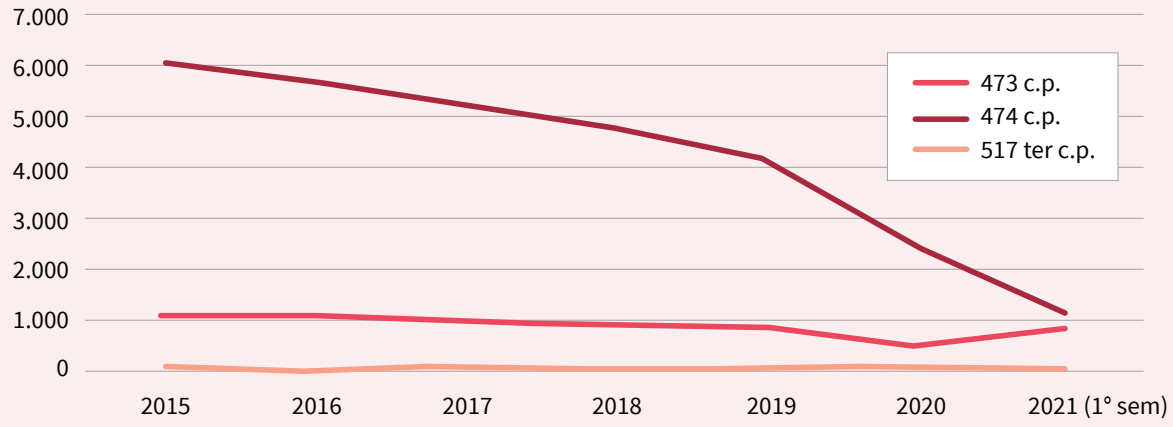
Sempre per il periodo di riferimento, il numero delle persone perseguite penalmente presenta un andamento statistico difforme; infatti, il numero dei soggetti deferiti all'Autorità giudiziaria registra una costante flessione per il reato di cui all'art. 474 c.p., un trend sostanzialmente stabile per l'art. 517 ter c.p., mentre per l'art. 473 c.p. si rileva una decrescita sino al 2020 ed un incremento notevole nel primo semestre del 2021.

Tabella 2 e Figura 3 – Soggetti deferiti all'Autorità giudiziaria per reati di contraffazione (i dati per il 2021 si riferiscono al primo semestre dell'anno)

Fonte: Elaborazione del Servizio Analisi Criminale su dati del C.E.D. del Ministero dell'Interno.

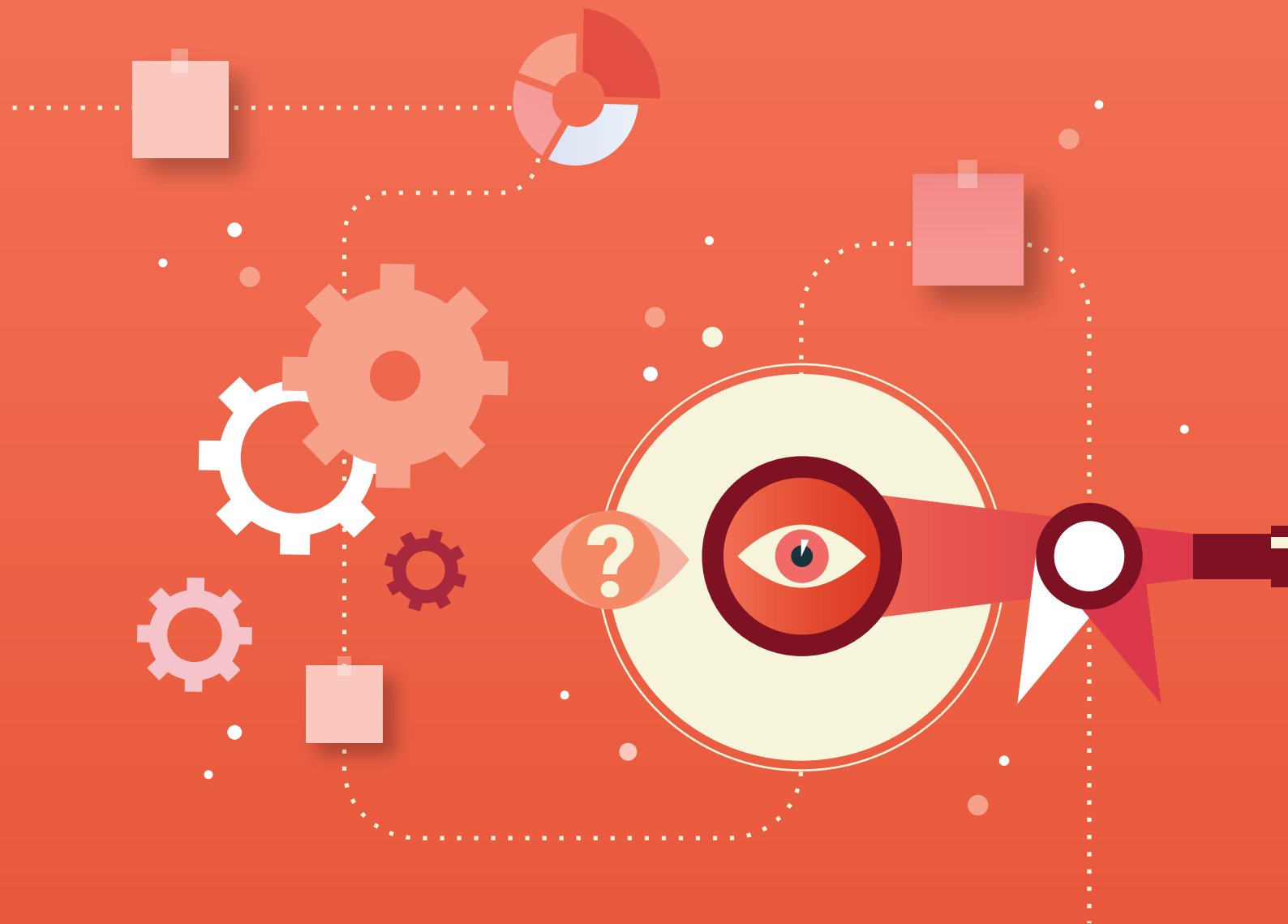
Persone perseguite penalmente

	2015	2016	2017	2018	2019	2020	2021 1° sem
473 c.p.	1.048	1.030	938	896	793	480	753
474 c.p.	6.051	5.606	5.153	4.690	4.131	2.379	1.151
517 ter c.p.	68	67	43	50	47	65	47



2.

Metodologia



2.1 Definizioni

Come anticipato, il presente studio si concentra sull'analisi della contraffazione nei mercati online. È utile fornire una definizione operativa di questi due concetti chiave, utilizzata ai fini dell'analisi.

Contraffazione

Con questo termine intendiamo la violazione di proprietà intellettuale tramite la riproduzione illecita di un bene e la relativa commercializzazione *uti originalis* (Senato della Repubblica Italiana 2017, 12). In particolare, si fa riferimento alla definizione di contraffazione fornita dagli articoli **473 c.p.** (Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni), **474 c.p.** (Introduzione nello Stato e commercio di prodotti con segni falsi) e **517 ter c.p.** (Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale).

È importante precisare che la definizione di contraffazione utilizzata in questo studio differisce da quella adottata dall'OECD nei suoi report, avendo quest'ultima un respiro più ampio del Codice Penale italiano. L'OECD adotta infatti la definizione di contraffazione proposta nella sezione 'enforcement' del *Trade-Related aspects of Intellectual Property Rights* (conosciuto anche come accordo TRIPS), negoziato dal *World Trade Organization*. Questo accordo prevede che i beni contraffatti sono 'qualunque tipo di bene, incluso l'imballaggio, che rechi, senza autorizzazione, un marchio di fabbrica identico a quello validamente registrato per lo stesso genere di prodotto, o che non possa essere distinto nei suoi elementi essenziali dal marchio autentico, e che, di conseguenza, violi i diritti del legittimo titolare del marchio medesimo' (WTO 1994, 342).

Mercati online

Con questo termine intendiamo in maniera ampia **l'insieme dei canali sul web** attraverso cui vengono condotte attività connesse alla pubblicizzazione e vendita di prodotti e servizi, e in particolare:

L'adozione di una definizione ampia si rende necessaria data la crescente interazione tra contraffattori e consumatori su canali che non sono pensati specificatamente per la vendita di beni e servizi, come *social media*, forum e chat (Kennedy 2020). Il Capitolo 3 dimostrerà in maniera chiara questo trend.

2.2 Fonti e dati

Considerata la novità del tema, e l'assenza di precedenti ricerche e statistiche, il presente studio si avvale di un approccio metodologico 'ibrido' che utilizza **tre fonti dati principali**:

- **documenti e atti giudiziari** e di polizia legati a procedimenti giudiziari e indagini, in Italia e all'estero;
- **report, pubblici o ad uso interno**, di autorità pubbliche e soggetti privati (es. *marketplace*, *social media*, operatori di logistica e postali, titolari di diritti intellettuali);
- **interviste con testimoni privilegiati** del settore pubblico e privato.

In particolare, sono state condotte interviste telefoniche e/o scambi via e-mail per la condivisione di materiali e documenti con **25 professionisti ed esperti, in Italia e all'estero**, appartenenti a diverse categorie di *stakeholder*:

- forze dell'ordine e altre autorità pubbliche;
- *marketplace* e aste online;
- *social media*;
- titolari di diritti di proprietà intellettuale, appartenenti a diversi settori, e associazioni di categoria;
- operatori di logistica;
- operatori di servizi postali;
- centri di ricerca e università.

Le interviste hanno seguito una traccia di domande personalizzata rispetto al ruolo e alla posizione degli intervistati, e condivisa in precedenza con gli stessi. Durante o in seguito alle interviste sono stati condivisi ulteriori documenti e materiali che sono stati utilizzati ai fini di questo studio, in forma esplicita (in questo caso saranno menzionati in bibliografia) o anonima[10].

10. Non tutti i soggetti intervistati, o le organizzazioni di appartenenza, hanno acconsentito ad essere menzionati esplicitamente. Tra quelle che hanno autorizzato ad essere citate, si ringraziano: il Ministero dell'Interno, ed in particolare il Dott. Stefano Delfini, Dirigente Superiore della Polizia di Stato e Direttore Servizio Analisi Criminale della Direzione Centrale della Polizia Criminale - Dipartimento della Pubblica Sicurezza, la Dott.ssa Loredana Stamato, Primo Dirigente della Polizia di Stato, Servizio Analisi Criminale della Direzione Centrale della Polizia Criminale - Dipartimento della Pubblica Sicurezza, e il Ten. Col. CC Alessandro Giordano Atti, Direttore della V Sezione – III Divisione "Interpol" Servizio per la Cooperazione Internazionale di Polizia della Direzione Centrale della Polizia Criminale - Dipartimento della Pubblica Sicurezza; la Guardia di Finanza, ed in particolare il Ten. Col. Francesco Basile, Comandante 2° sezione del Gruppo Anticontraffazione e Sicurezza prodotti del Nucleo Speciale Beni e Servizi, e il Ten. Col. Giacomo Scilì Bellomo, Capo Sezione Tutela Mercato Beni e Servizi dell'Ufficio Tutela Uscite e Mercati del III Reparto Operazioni del Comando Generale; Amazon; INDICAM, ed in particolare la Dott.ssa Lucia Toffanin, Direttore Generale; Michigan State University, e in particolare il Dr. Jay Kennedy, *Assistant Professor at the School of Criminal Justice and the Center for Anti-counterfeiting and Product Protection*; Poste Italiane, ed in particolare il Dott. Rocco Mammoliti, *Chief Information Security Officer,* e il Dott. Massimiliano Aschi, *Senior IT Security Specialist*; *Yoox-Net-A-Porter Group*, ed in particolare il Dott. Gianluca Gaias, *Chief Security Officer*, e la Dott.ssa Arianna Vitalini, *Corporate Digital Governance Manager*. Si ringraziano altresì per gli input ricevuti tutte le altre persone intervistate, appartenenti ad autorità pubbliche e settore privato, che preferiscono non essere menzionati esplicitamente nello studio.

3.

Contraffazione e mercati online: minacce e trend emergenti

L'evoluzione del fenomeno della contraffazione sui mercati online si può osservare attraverso tre dimensioni:

- quella dei **canali utilizzati**;
- quella degli **attori coinvolti**;
- quella degli **schemi criminali** messi in atto.

La combinazione di queste tre dimensioni genera nuovi forme e *modi operandi* nella produzione e distribuzione dei 'falsi' sui mercati online.

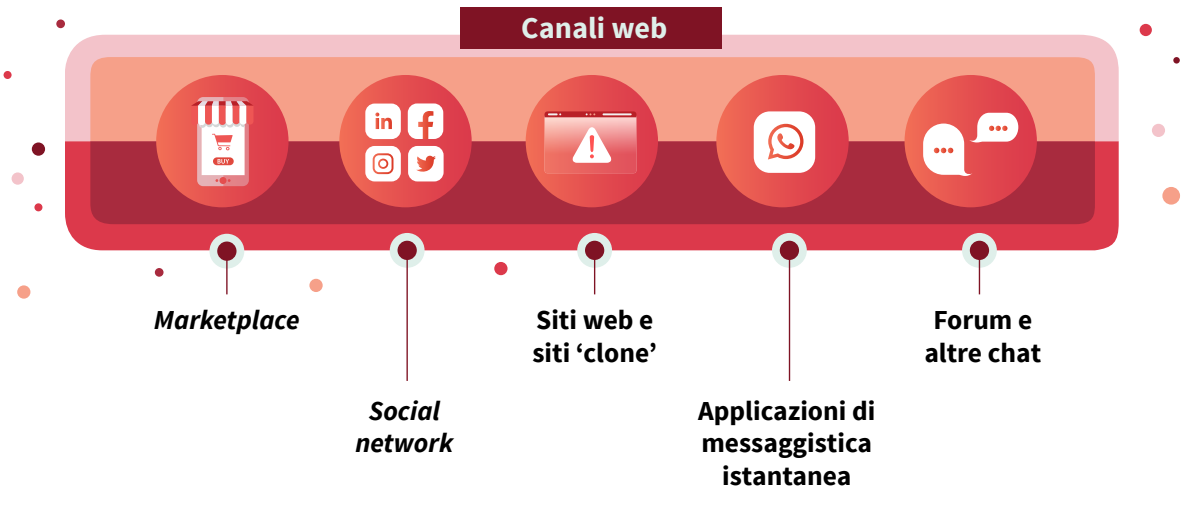
3.1 Canali

Le ultime indagini rivelano una crescente **diversificazione e interconnessione dei canali online** utilizzati per la pubblicizzazione e vendita di prodotti contraffatti. I contraffattori (individuali o in gruppi organizzati) spesso li utilizzano in **maniera contestuale**, con *cross-link* e rimandi tra canali diversi, al fine di:

- raggiungere un numero più ampio di potenziali clienti;
- eludere i controlli dei *provider*;
- ostacolare le indagini sfruttando le differenze tra canali diversi in termini di gestione e condivisione (con le autorità) delle informazioni su clienti, venditori e altri utenti.

Le forze dell'ordine e le autorità pubbliche intervistate hanno infatti segnalato **livelli diversi di cooperazione** da parte di diversi mercati online, soprattutto quando questi sono localizzati all'estero o si appoggiano a server extra-UE. E allo stesso tempo **diverse capacità tecnologiche e sistemi di prevenzione**, ad esempio in termini di monitoraggio delle inserzioni e controllo venditori (vedi Capitolo 4). Le forze dell'ordine e i *brand owner* intervistati concordano che se, da una parte, i *marketplace* più grandi dispongono in genere di sistemi avanzati di rilevamento automatico di beni illeciti, i ***social network***, dall'altra, risultano meno attrezzati nei confronti del contrasto alla vendita di prodotti contraffatti. Allo stesso modo, anche i *marketplace* più piccoli non dispongono generalmente degli strumenti adeguati anche se, al contrario dei *player* più grandi, potrebbero non avere a disposizione le risorse necessarie per questi investimenti.

I prossimi paragrafi approfondiscono i principali canali web utilizzati dai contraffattori. In particolare:



3.1.1 *Marketplace*

I *marketplace* come Amazon, eBay, Alibaba ed altri hanno assunto un ruolo sempre più centrale nelle abitudini di acquisto dei consumatori, attirando di conseguenza anche le attenzioni dei contraffattori. Come già evidenziato da uno studio congiunto di EUIPO e Europol (2019), l'abuso dei *marketplace* sta infatti diventando una fonte di reddito sempre più importante per i gruppi criminali coinvolti nella vendita di prodotti contraffatti. Le interviste e le analisi dei casi studio hanno però evidenziato come questi siano, in realtà, **canali più presidiati e strutturati** rispetto agli altri, rendendoli quindi meno vulnerabili ad attività illecite. Ad esempio, i *marketplace* più grandi, come Amazon, dispongono di controlli automatici a tappeto e sistemi più stringenti di *seller vetting* (vedi Capitolo 4).

Come dimostrato dal Box 3 (vedi sotto), gli schemi fraudolenti individuati sui *marketplace* stanno diventando sempre più complessi proprio per **aggirare i sofisticati controlli** messi in atto dalle piattaforme.

Box 3. Contraffazione online e schemi *cross-channel*

A novembre 2020, Amazon ha avviato un'azione legale negli Stati Uniti d'America nei confronti di due *influencer* che, tramite i propri profili *social* (Facebook, Instagram e TikTok), sponsorizzavano prodotti contraffatti in vendita su diversi *marketplace* tra cui, oltre Amazon, anche Etsy e DHgate (CNBC 2020; Amazon 2021b). Lo schema è stato individuato da Amazon grazie all'attività di *intelligence* svolta dalla *Counterfeit Crimes Unit* (CCU), che oltre al proprio *marketplace*, monitora proattivamente anche altri canali online (es. siti web, *social network*). Le due *influencer* e gli undici *seller* del *marketplace* coinvolti avevano ideato un complesso schema fraudolento che sfruttava i *social network* per aggirare i controlli dei *marketplace*:

- i *seller* postavano sul *marketplace* **inserzioni per prodotti generici**, senza inserire loghi o altri segni distintivi nelle immagini e descrizioni (impedendo quindi ai sistemi di rilevamento automatico del *marketplace* di individuare eventuali violazioni);
- le due *influencer* pubblicizzavano questi annunci sui loro profili *social*, facendo invece riferimento a prodotti di noti *brand owner*. Le foto dei prodotti generici venivano infatti affiancate alle foto dell'equivalente prodotto contraffatto con il testo "***order this/get this***";
- i *follower* sui *social* delle due *influencer* venivano quindi reindirizzati all'inserzione dei prodotti generici sul *marketplace* di Amazon tramite **link nascosti**;
- una volta effettuato l'ordine, al posto dei prodotti generici che avevano ordinato (***order this***), gli acquirenti ricevevano il relativo prodotto contraffatto (***get this***).

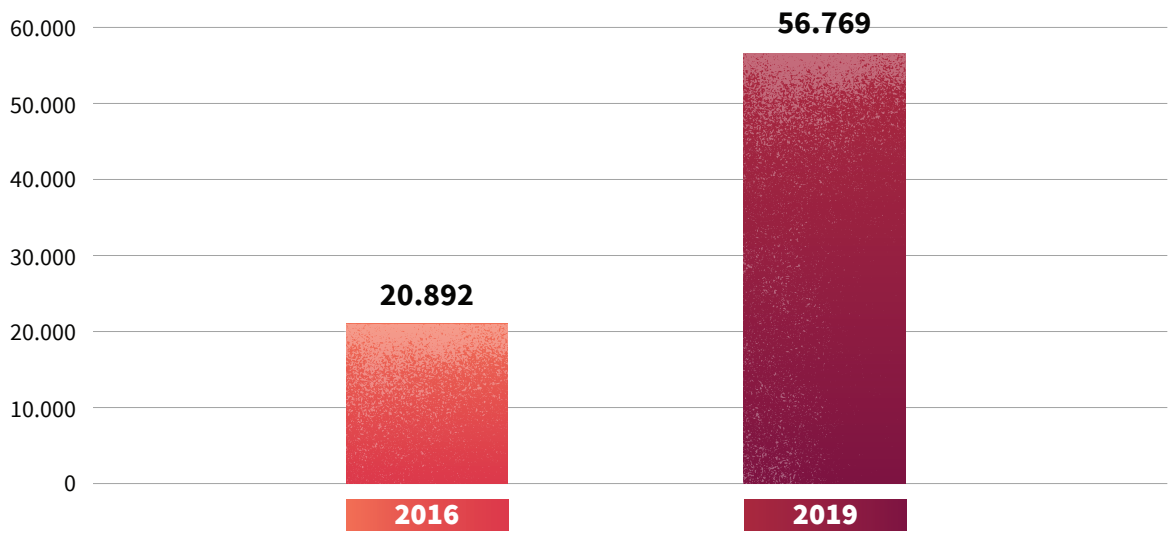
Le due *influencer* hanno recentemente patteggiato, pagando una penale che Amazon ha devoluto interamente allo sviluppo di attività di *brand protection*, incluse campagne di sensibilizzazione sul tema (Amazon 2021b). Amazon si prepara adesso ad avviare un'azione legale anche contro i *seller* coinvolti nello schema che, anche se basati in Cina, avevano fraudolentemente indicato la residenza negli Stati Uniti (CNBC 2021).

3.1.2 *Social network*

Negli ultimi anni molti *social network* si sono dotati di un *marketplace* per offrire ai propri utenti anche la possibilità di acquistare e vendere prodotti (il cosiddetto ***social commerce***). Oltre al successo per il pubblico, si assiste ad un **crescente interesse** dei contraffattori per queste piattaforme di scambio non tradizionali (Kennedy 2020; EUIPO 2021d; EUIPO e OECD 2021b). I contraffattori sfruttano infatti i *social network* per la potenza 'moltiplicativa' che offrono tramite, ad esempio, i *like* e le ricondivisioni di post, che permettono di raggiungere un numero molto elevato di clienti (EUIPO e OECD 2021b). Questo è dimostrato da alcune cifre derivanti da recenti analisi:

- uno studio dell'EUIPO (2021c) ha stimato che su Facebook, Instagram, Reddit e Twitter, circa l'**11% delle conversazioni** relative a prodotti fisici è legato a prodotti 'contraffatti';
- in Italia, il Ministero dello Sviluppo Economico (2020) ha evidenziato come le segnalazioni riguardanti **le violazioni online** dei diritti di proprietà intellettuale, pervenute tramite la '**Linea Diretta Anticontraffazione**' (servizio offerto, in collaborazione con la Guardia di Finanza, ai consumatori e ai titolari di diritti di proprietà intellettuale), siano notevolmente aumentate negli ultimi anni, soprattutto sui *social* come Facebook e Instagram, arrivando a rappresentare ormai l'**86% delle segnalazioni totali**;
- un recente studio a livello mondiale (Stroppa et al. 2019) ha individuato 56.769 account su Instragram utilizzati per vendere prodotti contraffatti – un **aumento del 171%** rispetto ai 20.892 individuati nello studio precedente del 2016 (Stroppa e Di Stefano 2016) – stimando che, già solo grazie ai propri *follower*, sarebbero riusciti a raggiungere circa 20 milioni di utenti. Questi account, durante il solo 2019, hanno pubblicato oltre 64 milioni di post, un aumento significativo rispetto ai 14.5 milioni di post nel 2016;
- i post con hashtag riferiti a prodotti contraffatti hanno superato le **100 milioni di visualizzazioni** a livello mondiale sul solo TikTok (Lince 2020).

Figura 4. Numero di account individuati su Instragram che vendono prodotti contraffatti.
Fonte: Stroppa e Di Stefano (2016) e Stroppa et. al (2019)



Oltre all'inserzione diretta sui *marketplace*, i contraffattori hanno vaccesso a diversi strumenti per pubblicizzare i propri prodotti su questi canali:

- ***post* e storie** su bacheche di profili personali o in gruppi privati: lo studio menzionato sopra ha accertato che i 56.769 profili utilizzati dai contraffattori su Instagram avevano pubblicato 64 milioni di post e, in media, 1,6 milioni di storie ogni mese (Stroppa et al. 2019);

- ***live streaming*** di soggetti (es. *influencer*) con un ampio numero di *follower* (Lince 2020; EUIPO 2021f);
- **campagne pubblicitarie sponsorizzate**: un recente report di TRACIT e AAFA (2020) ha riscontrato come, dal maggio 2017 ad oggi, oltre 70 grandi società di consumo e abbigliamento abbiano segnalato di essere state vittime di campagne pubblicitarie fraudolente sui *social*. Queste, infatti, sfruttano la visibilità dei *social* per reindirizzare gli utenti verso siti web terzi che vendono prodotti contraffatti (EUIPO 2021f). Anche in seguito alla segnalazione (e successiva rimozione), le pubblicità fraudolente ricompaiono nuovamente online in breve tempo ma con contenuti leggermente diversi. Come evidenziato da Carpani (2020), la crescente diffusione di questo fenomeno è dovuta principalmente a:
  - bassi costi di realizzazione di una campagna fraudolenta sponsorizzata;
  - assenza di controlli da parte dei *social network* sugli account utilizzati per le campagne pubblicitarie (es. se l'account è nuovo o esiste da tempo, se la pubblicità è coerente rispetto ai contenuti pubblicati dall'account);
  - assenza di controlli sui siti esterni a cui le pubblicità fraudolente reindirizzano.
- **commenti ai post delle pagine ufficiali** dei *brand owner*, spesso tramite ***burner* account *e spam-bot***[11] (EUIPO 2021f).

Sono numerose le **indagini e le azioni legali**, in Italia e all'estero, che hanno rivelato l'uso contestuale dei *social media* insieme ad altri *marketplace* e siti web (Box 4).

Box 4. Contraffazione online e *social network*: operazione 'Aphrodite II'

L'operazione 'Aphrodite II' nasce dalla volontà manifestata di Europol ed EUIPO di attuare un'azione concreta di contrasto alla violazione dei diritti di proprietà intellettuale sui *social network*. L'idea di base è quella di creare un *network* tra i titolari di diritti intellettuali e le forze dell'ordine per condividere le informazioni di utilità operativa e avviare, di conseguenza, un'azione repressiva 'a tutto campo'.

Nell'ambito dell'operazione 'Aphrodite II' (giugno 2019), le forze dell'ordine di 18 paesi membri dell'Unione Europea, con il supporto dell'Europol, hanno sequestrato 4.700.000 prodotti contraffatti e chiuso 16.470 account *social* e 3.400 siti web utilizzati per la relativa vendita (Guardia di Finanza 2019). I criminali coinvolti pubblicizzavano i prodotti contraffatti sui *social* tramite messaggi in chat e gruppi privati, mostrando le relative foto e prezzi. In molti casi, le offerte includevano anche link nascosti che reindirizzavano i potenziali clienti su mercati online extra-UE. I dettagli delle transazioni venivano poi definiti tramite altri canali, principalmente app di messaggistica istantanea, oppure telefonicamente tramite utenze intestate a prestanome. I pagamenti avvenivano tramite carte prepagate, PayPal, *money transfer* o altre forme di pagamento elettronico mentre i prodotti contraffatti venivano spediti direttamente ai clienti tramite corrieri.

In particolare, le indagini hanno beneficiato di un intenso scambio tra forze dell'ordine e titolari di diritti di proprietà intellettuale, soprattutto in merito agli interventi per via stragiudiziale (*take-down*) condotti da quest'ultimi. In particolare, sono state condivise sostanzialmente informazioni su: (a) inserzioni di prodotti sospetti; (b) account coinvolti; (c) siti web terzi a cui le inserzioni reindirizzavano.

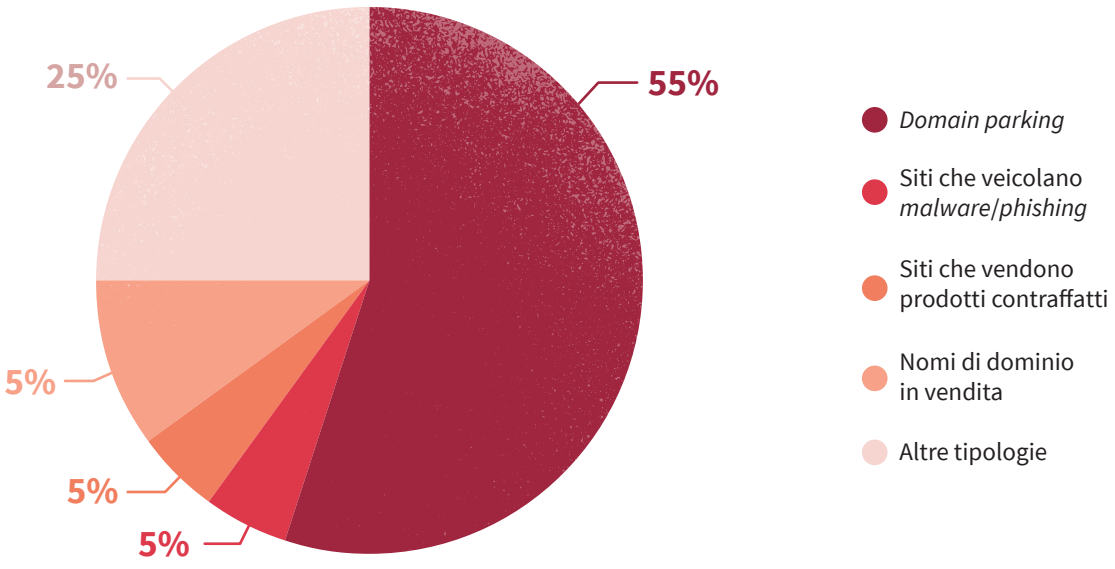
11. I *burner* account sono account *social* (spesso 'usa e getta') che vengono utilizzati per postare contenuti in modo anonimo. Gli *spam bot* sono invece software che permettono di mandare messaggi *spam* su chat, forum o e-mail.

3.1.3 Siti web e siti clone

Tradizionalmente, l'immagine della contraffazione online è stata associata alla vendita di prodotti tramite l'utilizzo di **siti clone**, ovvero siti che, per dominio, contenuti e layout sembrano essere i siti legittimi dei *brand owner* (Consiglio Nazionale Anticontraffazione 2019). La violazione dei domini Internet avviene solitamente attraverso la registrazione fraudolenta, presso la ICANN[12], di un dominio identico (***cybersquatting***) o simile (***typosquatting***) a quello appartenente ad un marchio registrato. Nel primo caso, si tratta generalmente della registrazione di un'estensione di un indirizzo Internet già esistente (es. .com, .info, .net, .org,). Nel secondo caso, vengono invece registrati domini Internet volutamente modificati (es. inversione di due lettere, errori ortografici, inserimento di un prefisso/suffisso) che cercano di sfruttare i possibili errori di battitura degli utenti nelle ricerche web.

Un recente studio dell'EUIPO (2021b) ha analizzato circa 1.000 domini sul web (993) relativi a 20 *brand owner* selezionati, trovando che il **49% di questi (486) erano considerabili 'sospetti'**. Il 55% di questi 486 nomi a dominio risultavano 'parcheggiati' (*domain parking*)[13], il 10% erano in vendita mentre gli altri risultavano impiegati per svariati scopi illeciti come ospitare siti che vendevano prodotti contraffatti (5%) o diffondere *malware*/sottrarre informazioni personali tramite *phishing* (5%). Inoltre, un altro studio dell'EUIPO (2017) ha rilevato come i contraffattori registrino nuovamente ed utilizzino i domini internet che erano appartenuti in precedenza ad altre organizzazioni, al fine di sfuttarne la popolarità (es. indicizzazione sui motori di ricerca, recensioni positive). Ad esempio, lo studio ha evidenziato che, nel Regno Unito, il **71%** dei 14.183 siti web sospettati di vendere prodotti contraffatti erano collegati ad un dominio internet appartenuto in precedenza ad un'altra organizzazione.

Figura 5. Tipologia d'impiego dei nomi a dominio considerati sospetti (N=486).
Fonte: EUIPO (2021b)



12. La *Internet Corporation for Assigned Names and Numbers* (ICANN) è la società senza scopo di lucro che si occupa di amministrare e coordinare il sistema di assegnazione univoca di nomi di dominio e indirizzi IP e delle politiche per garantire la sicurezza e la stabilità di Internet.

13. Il *domain parking* è una pratica che consiste nella registrazione di un nome a dominio che poi non viene effettivamente associato a servizi (es. siti web, e-mail hosting).

Oltre ai siti clone, le interviste hanno evidenziato una crescente diffusione di siti web che, al contrario, **vendono dichiaratamente prodotti contraffatti** e, proprio per questo motivo, presentano degli indirizzi web che includono parole chiave facilmente riconoscibili (es. replica, *simulation, buying fake*, *best fake*). L'offerta di prodotti contraffatti si è infatti adattata alla crescente domanda da parte di una clientela (spesso molto giovane) che non è interessata ad acquistare prodotti originali. Nel 2019, la *International Trademark Association* (2019) ha condotto un'indagine che ha coinvolto 4.712 giovani, tra i 18 e i 23 anni (Gen Z), in 10 paesi diversi. Il 79% di questi giovani ha riferito di aver comprato consapevolmente prodotti contraffatti durante l'anno precedente, principalmente perché più facilmente reperibili rispetto agli originali (58%) e perché non potevano permettersi economicamente quest'ultimi (57%).

Box 5. Pratiche utilizzate dai contraffattori per aumentare il rank dei siti clone

La struttura e la grafica dei siti clone imitano il ***look&feel*** del *brand owner*, inducendo gli utenti a credere che siano riconducibili a quest'ultimo o a rivenditori autorizzati (Heinonen, Holt, e Wilson 2012; Kennedy 2020). I prodotti vengono spesso messi in vendita con **immagini prese direttamente dai cataloghi ufficiali** e con **prezzi verosimili** che possono essere paragonati a quelli offerti dagli *outlet* autorizzati (e non più a prezzi estremamente bassi come avveniva in precedenza). Al di là dei contenuti e del *layout*, il **posizionamento sui motori di ricerca** (**rank**) è spesso l'elemento che inganna gli utenti. Questi siti, infatti, spesso compaiono tra i principali risultati di determinate ricerche grazie a pratiche di:

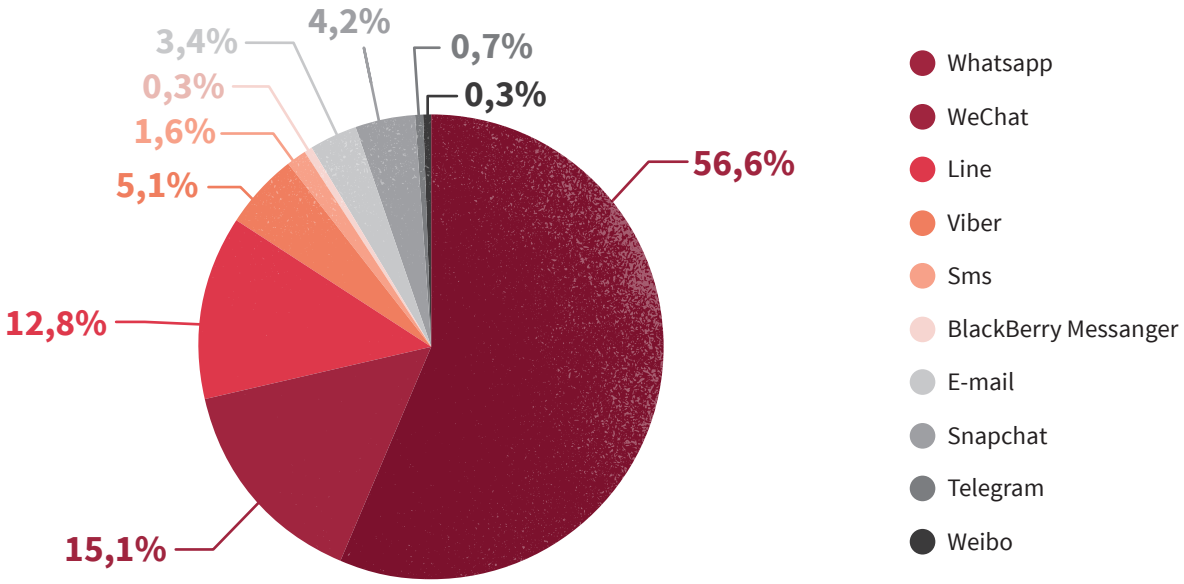
- ***defacement***: un attacco informatico che sfrutta le vulnerabilità informatiche di siti legittimi per inserirvi all'interno pagine web di vendita di prodotti contraffatti, spesso localizzati su server esteri;
- ***keyword advertising***: i marchi registrati di *brand owner* terzi vengono inseriti illegittimamente nella schermata principale del sito in caratteri molto piccoli (o con un font di colore uguale a quello dello sfondo di pagina) oppure direttamente nel codice sorgente HTML (*meta-tag*) e nei codici javascript (*cloacking*) del sito;
- ***linking***: inserimento di un link che rimanda l'utente su un sito terzo rispetto a quello su cui stava inizialmente navigando.

3.1.4 App di messaggistica istantanea

Tra i diversi canali, anche le applicazioni (*app*) di messaggistica istantanea stanno acquisendo un ruolo sempre più rilevante per la vendita di prodotti contraffatti. Lo studio di Stroppa e colleghi già menzionato in precedenza ha rilevato come il 56,6% degli account su Instragram che vendevano prodotti contraffatti comunicasse con i clienti tramite **Whatsapp**, seguito da **WeChat** (15,05%) e **Line** (12,8%), mentre solo il 5% utilizzasse canali più tradizionali come e-mail e sms (Stroppa et al. 2019).

Figura 6. App di messaggistica utilizzate dagli individui che vendono prodotti contraffatti su Instragram (N=56.769).

Fonte: Stroppa et al. (2019)



Queste app permettono, in modo veloce ed efficace, di:

- mostrare il **catalogo dei 'falsi'**, ad esempio in gruppi privati di vendita;
- inviare ai potenziali clienti **link nascosti che reindirizzano** ad altre piattaforme digitali (anche extra-UE);
- fornire informazioni più dettagliate sui prodotti e **metodi di pagamento** ai potenziali clienti;
- ricevere informazioni sugli **indirizzi** a cui spedire i prodotti contraffatti;
- **reclutare soggetti** da coinvolgere, a vario titolo, nella vendita di prodotti contraffatti.

Inoltre, sono più sicure rispetto ai canali tradizionali in quanto, nella maggior parte dei casi, offrono una crittografia *end-to-end* e chiudono raramente gli account per violazione dei termini di servizio. Anche in questi casi, è relativamente semplice e poco costoso ottenere un numero di telefono virtuale per aprire nuovi account (Stroppa et al. 2019).

Box 6. Reclutare soggetti per la vendita di prodotti contraffatti tramite *social network* e app di messaggistica

Nel febbraio 2020, i militari del comando provinciale della Guardia di Finanza di Luino hanno smantellato, nell'ambito dell'operazione 'Falsi online', una complessa organizzazione criminale coinvolta nella vendita di prodotti contraffatti sul web (Guardia di Finanza 2020). Lo schema era il seguente:

- i contraffattori pubblicavano sui *social network* **offerte di lavoro da casa**, con la promessa di facili guadagni e senza la richiesta di esperienza lavorativa pregressa;
- i soggetti che rispondevano agli annunci venivano inseriti in **gruppi chiusi su WhatsApp**;
- all'interno di questi gruppi, i soggetti reclutati venivano **informati sul loro ruolo e sugli step da seguire** per la pubblicizzazione e la vendita di prodotti contraffatti online. In particolare:

a. i soggetti a capo dello schema inviavano alle persone reclutate (*social seller*) le foto dei prodotti contraffatti comunicando i relativi prezzi;

b. i *social seller* provvedevano a pubblicarle sulle **proprie pagine *social***;

c. gli acquirenti effettuavano il **pagamento anticipato tramite ricarica su carte PostePay** intestate ai *social seller* stessi;

d. una volta ricevuto il pagamento e trattenuta una commissione, **i *social seller* provvedevano ad inviare il denaro su carte PostePay** intestate ai soggetti a capo dello schema;

e. i prodotti contraffatti venivano spediti a **casa dei *social seller*** che poi si occupavano direttamente di spedirli o consegnarli agli acquirenti finali.

Come ha funzionato la collaborazione tra forze dell'ordine e titolari di diritti di proprietà intellettuale?

Le condotte illegali sopra descritte sono state individuate grazie ad un'approfondita **attività di *screening*** condotta dalla Guardia di Finanza. In particolare, è stata effettuata una ricerca su siti di *e-commerce* e *social network* di offerte, messe online da individui residenti nella circoscrizione geografica del reparto, relative alla vendita di prodotti a prezzi estremamente vantaggiosi. L'analisi ha permesso di individuare diversi venditori online di cui sono state acquisite le immagini dei prodotti messi in vendita e dei relativi segni distintivi (es. etichette, cerniere, borchie).

A questo punto, **sono stati coinvolti i titolari di diritti di proprietà intellettuale** interessati che, tramite apposite relazioni tecniche, hanno accertato la non autenticità dei prodotti. Successivamente, è stata avviata una mirata **attività di OSINT** per raccogliere le informazioni necessarie per l'identificazione dei soggetti dietro gli account *social* utilizzati (es. foto del profilo, data di nascita, luogo di origine).

3.1.5 Forum e altre chat

Questo canale è spesso legato ad una clientela che si rivolge intenzionalmente al mercato secondario ed acquista quindi prodotti che, per caratteristiche e/o modalità di vendita, sono chiaramente identificabili come contraffatti (***non deceptive counterfeit***). Per questa tipologia di clienti la contraffazione rappresenta la possibilità di acquistare prodotti che desiderano ma ad un prezzo sensibilmente inferiore rispetto a quello del listino ufficiale e i forum sono uno dei canali preferiti per scambiarsi informazioni su dove acquistare i migliori 'falsi', quali sono i *seller* più affidabili e come individuare repliche di bassa qualità (Kennedy 2020). Proprio a questo scopo gli utenti hanno sviluppato una terminologia apposita per comunicare tra di loro. Ad esempio, su r/FashionReps (un *subreddit* con oltre 647.000 membri che è interamente dedicato alle repliche di prodotti di moda) è presente una guida per i nuovi utenti che spiega nel dettaglio i termini più utilizzati, tra cui (Reddit 2018):

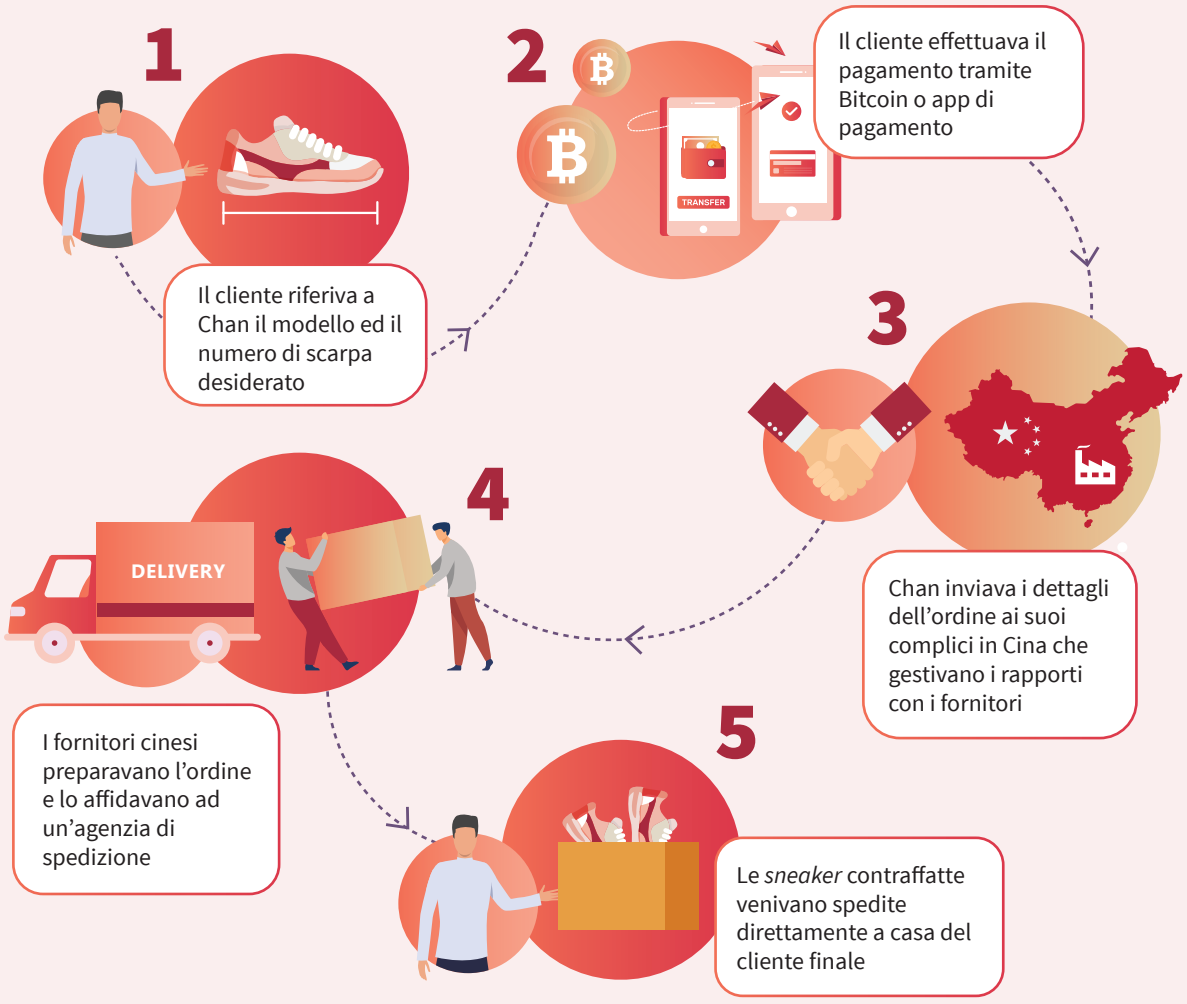
- **QC *(Quality Control)***: utilizzata quando un utente posta l'immagine di una replica che ha acquistato per farne valutare la qualità agli altri utenti;
- **GL *(Green Light)***: utilizzata quando un utente risponde ad una richiesta di Quality Control e certifica la qualità della replica;
- **LC *(Legit Check)***: utilizzata quando un utente posta un'immagine di un prodotto che ha acquistato per chiedere agli altri utenti se è originale o meno;

- **W2C *(Where to Cop)***: utilizzata quando un utente cerca un prodotto specifico;
- **1:1 *(One to One)***: utilizzata quando una replica è considerata identica all'originale;
- **B&S *(Bait & Switch)***: utilizzata quando si vuole segnalare agli altri utenti l'inaffidabilità di un certo venditore.

Box 7. Replica e forum: il mercato parallelo delle *sneaker*

Il mercato delle *sneaker* è contraddistinto da una comunità di appassionati (i cosiddetti *sneakerhead*) disposti a spendere cifre molto elevate per i modelli più ricercati. Il fatto che questi vengano spesso venduti al lancio in edizione limitata e solo in negozi selezionati ha spinto un crescente numero di appassionati – non disposti a spendere cifre elevate – a rivolgersi al mercato secondario. Su Reddit, ad esempio, la pagina *r/Repsneakers* conta circa 480.000 membri che postano spesso le foto delle repliche che stanno valutando di acquistare per sottoporle ad una sorta di 'controllo qualità' degli altri utenti. Se la replica non supera il test, il cliente segnala al venditore le imperfezioni riscontrate, chiedendo di inviargli le immagini di un nuovo lotto migliorato (Wall Street Journal 2019).

Nel 2018, uno studente cinese di medicina nel Regno Unito si rivolse proprio a *r/Repsneakers* per sondare l'interesse della community ad acquistare *sneaker* contraffatte che era in grado di procurare, grazie a contatti con fornitori cinesi a Putian (Vice 2018). Soddisfatto della risposta, Chan aprì un suo *subreddit* dedicato (*r/chanzhfsneakers*) e, in poco tempo, arrivò ad avere 10.000 clienti ed una lista d'attesa di circa 3.000 persone. Lo schema di vendita era il seguente:



Anche **le chat dei videogiochi** possono essere utilizzate per la vendita di prodotti illegali, dai dati rubati fino ai prodotti contraffatti (CBS News 2019). Questo si aggiunge anche ai rischi criminali connessi agli acquisti *in-game*, come il riciclaggio di denaro ed il finanziamento del terrorismo (Moiseienko e Izenman 2019; Wronka 2021).

3.2 Attori

L'analisi dei casi e le interviste rivelano una **ampia varietà** ed una **crescente professionalizzazione** degli attori criminali coinvolti nella vendita di falsi online. Questa non si riscontra solo nella capacità di realizzare copie sempre più simili ai prodotti originali ma anche di mettere in atto schemi di distribuzione sempre più complessi, grazie ad approfondite competenze tecniche, informatiche e societarie/finanziarie. In generale, si possono individuare tre tipi di soggetti:

- ***'influencer':*** attori individuali, spesso di giovane età, attivi sui *social media* come intermediari per i produttori di beni contraffatti;

- ***'broker':*** professionisti, di natura individuale od organizzata, in grado di fornire competenze e servizi informatici o societari/finanziari;

- **criminalità organizzata**: ad ampio spettro, dalle mafie attive sul territorio nazionale ai gruppi delinquenziali di origine straniera, talvolta collegata anche ad attori di matrice terroristica.

3.2.1 *'Influencer'*

Si assiste sempre più frequentemente alla presenza di attori individuali, spesso molto giovani, che fanno da intermediari tra l'offerta (prevalentemente localizzata nel sud-est asiatico) e la domanda, abusando di modelli di ***drop-shipping*** (vedi box 8). Con questo termine si intende una pratica, legale, che permette ad un venditore di commercializzare prodotti senza averli in magazzino, appoggiandosi ad uno o più fornitori. Il venditore raccoglie gli ordini e li inoltra poi ai fornitori, i quali si occuperanno di inviare i prodotti direttamente ai clienti tramite operatori postali o corrieri.

Il crescente utilizzo delle spedizioni puntuali e di piccole dimensioni (*small parcel*) nella contraffazione online è visibile anche nelle statistiche riportate nell'ultimo report OECD-EUIPO (2021). Il **91% dei beni contraffatti sequestrati** nell'Unione Europea, e collegati a vendite *e-commerce*, coinvolge il sistema postale, **contro il 45% dei beni sequestrati** e non collegati all'online, che utilizza in maniera più sensibile anche altri canali di trasporto (es. container). Purtroppo lo studio, che è al momento l'unico a fornire statistiche sui sequestri di falsi legati ad attività sul web, non fornisce dettagli a livello italiano.

Box 8. Vendita dei 'falsi' e *drop-shipping*: operazione 'Bologna Luxury'

L'operazione 'Bologna Luxury' ha permesso di sperimentare, con grande successo, una **forma di collaborazione** tra i titolari di diritti di proprietà intellettuale e le forze dell'ordine.

Come ha funzionato la collaborazione tra forze dell'ordine e settore privato?

Il **punto di partenza** dell'indagine è stata l'**azione di *take-down*** efficacemente messa in atto da un importante *brand* di moda a seguito di attività di '*internet brand protection*'. L'ufficio legale del *brand* ha poi formalmente comunicato al Nucleo Speciale Beni e Servizi della Guardia di Finanza i dati relativi all'attività di enforcement stragiudiziale condotta indicando, in particolare, gli **account *social* coinvolti e i *post* rimossi**. Il percorso investigativo sperimentato ha permesso di utilizzare queste informazioni (considerate qualificate) nelle successive indagini offline, al fine di individuare i responsabili e ricostruire i flussi economici illeciti. Le attività d'indagine hanno poi accertato come dietro uno degli account segnalati (denominato 'follie_di_lusso'), attivato prima su Facebook e poi anche su Instagram, si nascondesse una **giovane *influencer* che agiva da intermediaria** tra un fornitore in Cina e i clienti finali in Italia. Lo schema di vendita, che ha generato oltre 200.000€ in poche settimane, era il seguente:

- il potenziale acquirente sceglieva un determinato capo o accessorio d'abbigliamento dal catalogo pubblicizzato;
- la contrattazione sul prezzo avveniva direttamente in chat privata su WhatsApp;
- l'*influencer*, dopo aver ricevuto il pagamento (tramite bonifico o ricarica PostePay), inviava i soldi ricevuti (trattenendo una commissione) ai conti PayPal dei fornitori in Cina;
- l'*influencer*, sempre tramite WhatsApp, comunicava al fornitore in Cina i dettagli dell'ordine da preparare e gli indirizzi degli acquirenti a cui spedire i prodotti;
- il fornitore in Cina spediva i prodotti contraffatti direttamente al cliente, senza possibilità di reso e/o rimborso.

Nell'ambito dell'indagine, la Guardia di Finanza ha avviato anche **un'interlocuzione con i *social network*** coinvolti, tramite rogatoria internazionale, mirata all'acquisizione degli elementi necessari per individuare la persona che si nascondeva dietro gli account come **file di log, numeri di telefono e strumenti di pagamento utilizzati**. In relazione all'ultimo punto, una volta individuato l'indirizzo e-mail dell'interessata, la Guardia di Finanza ha anche inoltrato a Paypal, tramite il *Safety Hub – PayPal Law Enforcement*, la richiesta per la condivisione dei dati delle transazioni associate all'account, che hanno confermato la movimentazione economica già riscostruita anche grazie all'analisi delle transazioni effettuate con PostePay.

3.2.2 'Broker'

È da segnalare come anche il mondo della contraffazione si avvalga della collaborazione di gruppi specializzati nella fornitura di ***crime-as-a-service* (C-A-A-S)**, così come rilevato in ambito europeo (e non solo) anche per altri reati economici e organizzati (Europol 2020). Negli schemi analizzati sono spesso coinvolti dei professionisti ('*broker*') che forniscono competenze e servizi in ambito diverso, ed in particolare **informatico** e **societario/finanziario**.

Professionisti dell'informatica

Questi *broker* sono spesso attivi come supporto ai contraffattori nello:

- sviluppo e **gestione di siti** fraudolenti;
- sviluppo di **'carrelli' elettronici** e sistemi di *cash-out* (anche fraudolenti) in siti di vendita, legittimi e non;
- fornitura e gestione di **software malevoli** agganciati a siti fraudolenti per rubare le informazioni di clienti a fini estorsivi o di rivendita sul darkweb;
- **sviluppo di *bot*** poi utilizzati in forum e chat per pubblicizzare beni contraffatti o siti fraudolenti (*spam-bot*).

In questo ambito, prevalgono gli attori provenienti dall'**Est Europa e dall'area russofona**, spesso coinvolti anche in altri tipi di frodi digitali e reati *cyber* (Europol 2020). In tal senso, è interessante notare come il **7.6%** dei 56.769 account di contraffattori attivi su Instragram reindirizzasse gli utenti su siti web di *e-commerce* aperti su domini russi (.ru) (Stroppa et al. 2019).

Box 9. Web-developer, siti fraudolenti e contraffazione online

Nell'ambito dell'operazione 'Zombi' (dicembre 2019) i militari del comando provinciale della Guardia di Finanza di Genova hanno sequestrato ed oscurato **475 siti web** utilizzati per commercializzare capi di abbigliamento contraffatti di noti marchi. L'organizzazione criminale coinvolta si avvaleva di **professionisti per la creazione di siti** che utilizzavano domini Internet di aziende fallite o cessate. Quest'ultime, infatti, non avevano provveduto a rinnovare i propri nomi a dominio che, rimasti liberi, erano stati utilizzati per ospitare siti web su cui venivano messi in vendita scarpe contraffatte. I siti erano localizzati su **server esteri** ed erano registrati in capo a **soggetti di origine straniera** che risultavano intestatari di una pluralità di siti fraudolenti (Ministero dell'Interno, 2021).

Intermediari a livello societario/finanziario e società di comodo

Di particolare rilevanza sono anche i soggetti – professionisti e non – che forniscono le competenze necessarie per costituire e gestire società schermo utilizzate a vario titolo nella distribuzione dei beni contraffatti, sia attraverso canali online che offline. In particolare, dall'analisi dei casi studio, illustrati in questo report, emerge un ampio utilizzo di **società di comodo** per finalità diverse, elencate di seguito.

Importare prodotti contraffatti poi venduti sul web

Diverse indagini hanno rivelato l'impiego di società schermo che vengono utilizzate, attraverso **schemi di false fatturazioni e documenti falsi** (es. certificati di origine, bolle di trasporto), per importare e commercializzare beni contraffatti di varia natura (FACT Coalition 2019). In alcuni casi, queste società, spesso registrate all'estero e in paesi con bassi livelli di trasparenza societaria, sono state utilizzate anche per giustificare, tramite fatture false, un presunto acquisto di farmaci poi risultati contraffatti o rubati e rivenduti anche attraverso farmacie online (Savona e Riccardi 2018; AIFA 2021).

Box 10. Rolex falsi, siti web e consulenti d'azienda

Come riportato dal Ministero dell'Interno (2021), nell'ambito dell'operazione 'Right Time' (settembre 2019) i militari della Guardia di Finanza di Viareggio e Pisa hanno arrestato 6 persone responsabili di aver posto in essere un complesso sistema per la contraffazione e ricettazione di orologi di lusso sia in mercati rionali che tramite siti web. L'organizzazione si avvaleva della **consulenza di un commercialista** per l'apertura e la gestione di società di comodo che venivano intestate a **prestanome (soggetti nullatenenti)** ed utilizzate per garantire, tramite una serie di **false fatturazioni**, la tracciabilità delle vendite e il riciclaggio dei proventi illeciti.

Intestare e gestire siti web fraudolenti

Società di comodo, controllate da prestanome, possono essere utilizzate per **aprire e gestire siti web** impiegati per vendere 'falsi' o per sottrarre dati di carte di pagamento, documenti di identità e per diffondere *software* malevoli a consumatori inconsapevoli. Un trend interessante, evidenziato anche da un recente studio di OECD e EUIPO (2021b), è l'utilizzo, da parte dei contraffattori, di società di comodo anche per **l'intestazione dei servizi di pagamento** che permettono di ricevere pagamenti su questi siti web fraudolenti. Questi, conosciuti anche come rogue payment facilitators (McCoy 2016), offrono infatti dei servizi di pagamento che permettono ai contraffattori di non utilizzare i circuti tradizionali ed evitare quindi i relativi controlli e implicazioni fiscali (Tian et al. 2018).

Aprire account di vendita come *seller* sui mercati online

Le società di comodo possono essere impiegate come venditori (*seller*) sui *marketplace* per facilitare o occultare la vendita di beni contraffatti. Sebbene negli ultimi anni le politiche e le procedure di verifica e selezione dei venditori (*seller vetting*) siano state rafforzate in maniera significativa (vedi Sezione 4.2), anche i *marketplace* più grandi non sono immuni dai tentativi di infiltrazione da parte di venditori fraudolenti. Tuttavia, se realtà come Amazon o eBay hanno strumenti avanzati in grado di rilevare e di bloccare tempestivamente questi tentativi, i *marketplace* più piccoli spesso ne sono sprovvisti, diventando vittima e finendo a loro volta per moltiplicare la diffusione di beni contraffatti tra i loro utenti.

Box 11. *Seller* fraudolenti rinviati a giudizio per la vendita di cellulari contraffatti

Nel 2018 dieci persone sono state rinviate a giudizio presso il Tribunale federale dello stato americano dell'Idaho per il tentativo di vendita di cellulari e accessori di telefonia contraffatti sui *marketplace* di Amazon ed eBay. La collaborazione dei *marketplace* con le autorità competenti ha permesso di individuare e denunciare un complesso schema fraudolento, che comportava l'importazione dei beni da Hong Kong, il successivo riconfezionamento sul territorio americano e la vendita tramite account di *seller* intestati a società di comodo (U.S. Attorney's Office 2018; FACT Coalition 2019). Lo schema avrebbe generato circa 2 milioni di dollari di profitti illeciti, in seguito sequestrati dalle autorità governative.

Riciclare e occultare proventi illeciti sotto forma di compravendite online

Società schermo possono essere utilizzate anche per occultare o facilitare il riciclaggio di proventi derivanti dalla vendita di falsi online, secondo le modalità, già ampiamente conosciute e studiate, utilizzate per ripulire il denaro di altri reati tradizionali come il narcotraffico, il traffico di esseri umani e di altri beni illeciti (si veda, per una rassegna, Does de Willebois et al. 2011; Savona e Riccardi 2018; Bosisio et al. 2021). In tal senso, è da segnalare **l'operazione 'Pinar'** del 2016. Condotta dalla *Policia Nacional* spagnola e dalla *Agencia Tributaria* spagnola con il supporto di Europol, l'operazione ha smantellato un'organizzazione criminale impegnata nella **vendita di prodotti contraffatti** e nel successivo **riciclaggio dei proventi illeciti**, portando al sequestro di circa 265.000 prodotti contraffatti, 30 autovetture di lusso, 8 immobili e 150 conti correnti (Europol 2016). Il gruppo criminale aveva riciclato oltre 9 milioni di euro tramite **false fatturazioni tra società schermo (intestate a prestanome)** che permettevano anche di spostare i soldi all'estero. Inoltre, il gruppo si avvaleva anche di quattro consulenti finanziari che li aiutavano nelle operazioni di riciclaggio.

Meno conosciuta, ma ugualmente rilevante, è la possibilità di utilizzare le compravendite sui mercati online per **mascherare pagamenti o transazioni illecite** - il cosiddetto *transaction laundering* (Moiseienko 2020). In questo caso, una società di comodo potrebbe aprire un account come *seller* su un *marketplace* per mettere in piedi una transazione fittizia con un altro soggetto complice, persona fisica o giuridica, la quale procede all'acquisto dei prodotti o servizi pubblicizzati così da soddisfare una o più finalità criminali (Cassara 2016; Miller, Rosen, e Jackson 2016):

- **pagare beni o servizi illeciti** (es. stupefacenti, armi, materiale pedopornografico), ovviamente distribuiti su canali paralleli;
- **mascherare il trasferimento di fondi illeciti**, a fini di riciclaggio o finanziamento del terrorismo, utilizzando anche pratiche di sovrafatturazione (*mispricing*).

Emblematico di questa dinamica è il caso US vs Mohamed Elshinawy (n. 18-4223) che ha scoperto uno schema di **finanziamento del terrorismo tramite false transazioni *e-commerce*** su eBay (US District Court of Maryland 2018). Mohamed Elshinawy, un cittadino americano di origini egiziane, era stato reclutato nel 2015 da S.S. (anonimizzato), un ingegnere pakistano residente nel Regno Unito. Per mandare fondi alle nuove reclute, S.S. effettuava transazioni fittizie su eBay tramite la sua Ibacstel Electronics Limited, un'azienda di elettronica con sede a Cardiff. S. emetteva fatture false per acquisti inesistenti da Elshinawy (che si fingeva un rivenditore di elettronica sulla piattaforma) e gli inviava il corrispettivo in denaro tramite PayPal. Gli investigatori dell'FBI hanno rintracciato, in quattro mesi, transazioni per circa $8.700 che dovevano servire ad Elshinawy per compiere un attacco terroristico sul suolo americano.

A dimostrazione della crescente diffusione del *transaction laundering*, diverse **segnalazioni di operazioni sospette** sono state inviate alle unità di informazioni finaziaria di alcuni paesi esteri, tra cui il Regno Unito, da parte di quei *marketplace* che gestiscono in parallelo anche servizi di pagamento e rientrano quindi tra i soggetti obbligati alla normativa antiriciclaggio (Couvèe 2019; Moiseienko 2020). Il Capitolo 5 fornirà raccomandazioni su come beneficiare dell'esperienza già sviluppata in **ambito antiriciclaggio** anche a fini di prevenzione alla contraffazione sui mercati online.

Box 12. Caratteristiche e fattori di anomalia delle società di comodo impiegate come *seller* online

Dall'analisi dei casi studio, emerge che molte delle società di comodo impiegate come *seller* online per le finalità sopra illustrate presentano **caratteristiche ricorrenti** che riflettono i fattori di rischio e di anomalia individuati dalle linee guida in ambito antiriciclaggio. Tra queste:

- registrazione in paesi con bassi livelli di trasparenza societaria o in *Free Trade Zones* (FACT Coalition 2019; Ministero dell'Interno 2021);
- controllo da parte di veicoli societari opachi (es. trust, fondazioni, fiduciarie) e assenza di informazioni sui titolari effettivi (Bosisio et al. 2021);
- livelli di complessità societaria anomali e non giustificati da dimensioni e settori di attività economica (Jofre et al. 2021);
- sede legale in comune con numerose altre aziende, anche operanti in settori diversi;
- anomalie a livello contabile e indicatori sintomo di attività come 'cartiera' (es. basse immobilizzazioni, flusso di cassa assente, spese per il personale basse) (Pellegrini et al. 2020);
- frequenti ed ingiustificati cambi di ragione sociale, forma societaria e sede legale;
- caratteristiche anomale di soci ed amministratori (es. età anagrafica troppo bassa o elevata, *background* non compatibile con ruolo nell'impresa).

3.2.3 Criminalità organizzata

Sezione a cura del Servizio Analisi Criminale della Direzione Centrale della Polizia Criminale - Dipartimento della Pubblica Sicurezza - Ministero dell'Interno

Le strategie di contrasto alla criminalità organizzata attiva nel settore della contraffazione, per essere efficaci, devono tenere in considerazione alcune fondamentali peculiarità che caratterizzano l'evoluzione del fenomeno criminale su scala mondiale, ovvero:

- la dimensione sempre più **transnazionale** assunta dalle condotte illecite, con lo spostamento della produzione dai tradizionali distretti industriali nazionali a Paesi con economie di dimensioni gigantesche come la Cina e l'India, ai quali si devono aggiungere anche, per specifiche tipologie di merci, la Turchia, l'Egitto e Hong Kong;

- il **mutamento delle rotte** mediante cui le merci contraffatte o usurpative giungono in Italia dai Paesi produttori, le quali non fanno più ingresso prevalentemente via mare, attraverso i grandi porti nazionali, ma seguono itinerari molto articolati: i carichi illeciti possono transitare attraverso Stati quali gli Emirati Arabi Uniti, Singapore, Marocco, essere sdoganati in Paesi dell'Unione Europea, come ad esempio Grecia, Slovenia e Bulgaria, dove i controlli sono ritenuti meno rigorosi e, infine, trasportati via terra fino alle destinazioni finali italiane;
- l'esponenziale aumento della commercializzazione dei prodotti falsificati via 'web', dovuto, fondamentalmente, al fatto che la **rete Internet** consente di disporre di un'ampia scelta di punti vendita virtuali e di rendersi anonimi o simulare la propria identità;
- la tendenza al **frazionamento dei carichi illeciti in partite di piccola entità** portate a destinazione da corrieri, anche occasionali, a bordo di furgoni o autovetture o al seguito di passeggeri in sbarco presso porti e aeroporti, oppure avvalendosi delle grandi compagnie private di servizi di spedizione e consegna;
- la sempre maggiore diffusione della tecnica di apporre, sui prodotti, i marchi e gli altri segni distintivi falsificati in una fase quanto più possibile prossima a quella dell'immissione in commercio, in modo tale che, in caso di controlli durante la spedizione, le autorità di vigilanza possano rilevare solo la presenza di **articoli "neutri"**, identici agli originali ma privi degli elementi della contraffazione;
- l'incremento delle cd. "zone di libero commercio" ('*Free Trade Zone*')[14].

Box 13. Contraffazione e zone di libero commercio

Le *Free Trade Zone* (FTZ) sono zone industriali e commerciali, che, pur potendo assumere caratteristiche differenti, hanno in comune il fatto di essere aree territorialmente delimitate, spesso ubicate in prossimità di grandi infrastrutture aeroportuali o portuali e dotate di impianti e servizi per ogni esigenza aziendale. In queste aree le imprese ivi insediatesi possono svolgere operazioni di importazione, lavorazione ed esportazione di merci godendo di tariffe doganali agevolate, obblighi fiscali, amministrativi e societari più attenuati rispetto a quelli previsti dalla legislazione ordinaria e controlli meno stringenti da parte delle Autorità governative. Le zone di libero commercio possono essere utilizzate dai contraffattori come piattaforme logistiche di transito, al fine di soddisfare varie esigenze:

- occultare la provenienza dei carichi da Paesi che rappresentano un indice di rischio per le autorità doganali;
- costituire "società schermo" che impediscano, in caso di indagini, di risalire agli effettivi responsabili del traffico illecito;
- suddividere le spedizioni in partite più piccole per limitare i danni in caso di sequestro;
- nascondere i prodotti contraffatti sotto carichi "di copertura" leciti;
- applicare i marchi falsi su articoli "neutri", secondo la tecnica sopra descritta.

Secondo lo studio OECD e EUIPO (2018), l'esistenza, il numero e le dimensioni delle zone franche sono correlati al valore dei prodotti contraffatti e usurpativi esportati dall'economia del Paese che le ospita. L'istituzione di una nuova zona franca comporta un aumento medio del 5,9 % del valore delle esportazioni illegali di questo tipo.

14. Le zone di libero commercio, che nel 1975 erano solo 79 ubicate in 25 paesi, oggi sono circa 3.500, distribuite in 130 Stati: per comprendere la loro rilevanza economica, si consideri che nella sola "Jafza Free Trade Zone", istituita a Dubai (EAU) nel 1985, operano attualmente 7.000 imprese di oltre 100 Paesi e vi lavorano 144.000 persone.

In ambito nazionale, si aggiunge l'ulteriore specificità che le attività illegali in questo settore coinvolgono almeno tre diversi ambiti criminali, tra loro collegati: la criminalità organizzata di tipo mafioso, quella non mafiosa e i gruppi delinquenziali di origine straniera.

Le principali indagini condotte dalla fine degli anni '90 ad oggi evidenziano che le associazioni di stampo mafioso maggiormente interessate alla contraffazione ed alla pirateria sono riconducibili alla Camorra campana.

La partecipazione delle organizzazioni criminali qualificate alle attività illegali in esame può, tuttavia, realizzarsi non solo in modo diretto, ossia impiegando in questi affari illeciti i propri esponenti ed affiliati e le risorse finanziarie e strumentali di cui dispongono, ma anche in via mediata, ossia assicurando - in cambio della partecipazione ai profitti conseguiti - finanziamenti, protezioni e contatti ai numerosi sodalizi delinquenziali italiani, specializzatisi in questo settore.

I gruppi criminali di origine straniera, presenti sul territorio nazionale, che operano nel settore, sono rappresentati prevalentemente dai sodalizi cinesi, favoriti nei traffici di merci contraffatte grazie alle stabili relazioni che mantengono sia con la madrepatria che con le comunità insediatesi negli altri Stati dell'U.E., dalle organizzazioni delinquenziali di origine balcanica e dell'Europa orientale, attive nell'importazione e distribuzione dei tabacchi lavorati recanti i marchi falsificati, e dai gruppi criminali africani (magrebini, nigeriani e senegalesi), impegnati nella gestione di capillari reti di vendita al dettaglio nel settore dell'abusivismo nel commercio.

Infine, non si deve trascurare che il traffico di merci contraffatte o pirata può rappresentare un possibile canale di finanziamento di altre gravissime attività criminali, incluso il terrorismo di matrice confessionale.

Box 14. I collegamenti tra la contraffazione ed il terrorismo

Le possibili connessioni tra la contraffazione ed il terrorismo erano già emerse in passato, con riferimento a note organizzazioni estremistiche quali, ad esempio, l'*Irish Republican Army (IRA), l'Euskadi Ta Askatasuna (ETA), le Fuerzas Armadas Revolucionarias de Colombia - Ejército del Pueblo (FARC) e l'Ḥarakat al-Muqāwama al-Islāmiyya (HAMAS)*, risultate coinvolte nella contraffazione di farmaci per uso veterinario e di sigarette e nell'abusiva duplicazione di compact-disk musicali, mentre i vertici di AL QAEDA, in alcuni manuali di addestramento, rinvenuti nel 2002, raccomandavano espressamente alle proprie cellule terroristiche la vendita di prodotti contraffatti quale mezzo di finanziamento (AACP 2002). Tali connessioni si sono riproposte all'attenzione degli analisti anche in tempi più recenti, se si considera che uno dei componenti della cellula terroristica responsabile degli attacchi avvenuti a Parigi, nel gennaio del 2015, era stato sottoposto a sorveglianza dai servizi antiterrorismo, fino a sei mesi prima, risultando dedito all'importazione in Francia di scarpe sportive contraffatte, acquistate via web, dalla Cina e ricevute tramite spedizioni postali (UNIFAB 2016).

In tale contesto, l'attività repressiva deve essere mirata, innanzitutto, ad individuare e disarticolare i sodalizi criminali che gestiscono le diverse fasi della "filiera" illecita, in modo da colpire il mercato del falso nei suoi principali canali di alimentazione e di diffusione.

Alle attività investigative finalizzate alla ricostruzione delle filiere del falso, devono poi accompagnarsi servizi di controllo del territorio, orientati, in linea generale:

- alla vigilanza sui traffici di merci in ingresso nel territorio nazionale, per intercettare carichi di prodotti contraffatti o pirata destinati alla distribuzione nel territorio nazionale;
- al contrasto delle reti distributive organizzate dei beni della specie, nelle aree connotate da particolare attrattiva turistica, culturale e di afflusso di pubblico.

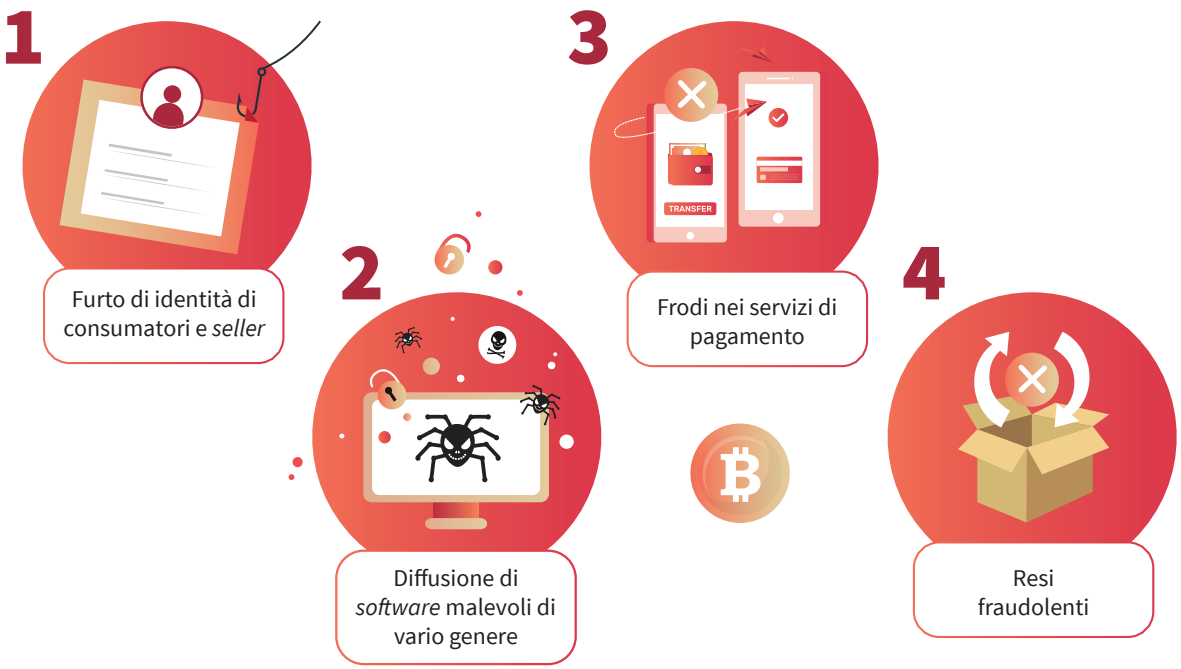
È prevedibile che una strategia di contrasto, così articolata, sia destinata, nel tempo, a determinare:

- una contrazione delle attività illecite "a valle" della "filiera", ossia nella fase dell'immissione sul mercato e della messa in circolazione della merce falsificata, perché diminuirà il numero dei venditori abusivi che affluiranno sui litorali, nei centri storici e nei mercati urbani;
- il conseguimento di risultati qualitativamente più significativi "a monte" della medesima "filiera", perché le attività investigative o gli interventi operativi orientati da preventiva azione di "*intelligence*" si concentreranno nelle fasi della produzione, dell'importazione e della distribuzione all'ingrosso.

3.3 Schemi

La varietà di canali e di attori criminali, sopra discussa, si manifesta nella **crescente interconnessione degli schemi criminali messi in atto**, secondo una natura poli-criminale già ampiamente evidenziata a livello nazionale ed internazionale (Europol e EUIPO 2020; Europol 2021). La vendita di prodotti contraffatti online è ormai solo una parte di una realtà più complessa, in cui i collegamenti trasversali con **altri reati economici e *cyber*** sono diventati sempre più frequenti e rilevanti.

Gli attori criminali coinvolti nella vendita di falsi online cercano di trarre il massimo vantaggio dall'interazione con i mercati online, sfruttando **tutti i servizi offerti**: acquisto, pagamento, reso e creazione account. L'obiettivo di chi distribuisce prodotti contraffatti sui canali web non è solo quello di frodare il consumatore vendendogli dei falsi, ma anche di generare proventi illeciti tramite tutta una serie di attività connesse, tra cui:



Sulla falsa riga del *customer journey*, possiamo parlare di ***fraudster journey***, cioè di 'viaggio fraudolento' che si compone di diverse tappe e reati, non sempre necessari, ma spesso co-esistenti. Queste sono discusse di seguito.

3.3.1 Furto d'identità di consumatori e *seller*

Gli attacchi di ***Account Takeover*** **(ATO)** si verificano quando soggetti malintenzionati riescono a rubare le credenziali di un utente e assumere il controllo dei relativi account *e-commerce*. In un recente studio, TransUnion (2020) ha riscontrato un **aumento del 347%** di questi attacchi a livello globale tra il 2018 e il 2019. Una volta ottenuto l'accesso, i criminali modificano le informazioni associate all'account (es. password), trasferiscono denaro sui propri conti, effettuano acquisti fraudolenti sul *marketplace* o ottengono l'accesso anche ad altri account della vittima. Esistono diverse modalità per la sottrazione di questi dati, tra cui (Vigderman 2021):

- acquisto da soggetti terzi sul ***dark web*** di dati provenienti da *data breach/leakage*;

- sottrazione diretta durante la **navigazione su siti clone e altri siti fraudolenti** (es. *banner* pubblicitari che, se cliccati, avviano il download di *malware*);

- sottrazione diretta tramite **attacchi informatici** (es. e-mail di *phishing*, tecniche di *social engineering*, *business e-mail compromise*, attacchi di *brute force*).

Oltre agli account dei clienti, anche quelli dei venditori dei *marketplace* sono presi di mira dai contraffattori. Anche in questo caso, le credenziali d'accesso vengono generalmente sottratte tramite **tecniche di *social engineering***, in particolare e-mail di *phishing*[11]. Una volta ottenuto l'accesso, i contraffattori modificano:

- il metodo di accredito registrato sulla piattaforma. In questo modo, i clienti procedono normalmente agli acquisti ma i **pagamenti confluiscono sul conto dei contraffattori**;
- il catalogo del *seller*, **inserendo prodotti contraffatti**. In molti casi, i contraffattori stessi procedono poi ad acquistarli, tramite carte prepagate clonate, al fine di effettuare poi il rimborso per merce non ricevuta (*reimbursement fraud*) oppure riciclare proventi illeciti.

3.3.2 Frodi nei servizi di pagamento

Una volta che ottengono fraudolentemente l'accesso ad un account *e-commerce* e alle informazioni dei relativi metodi di pagamento associati (es. numero di carta di credito), i criminali utilizzano spesso ***script*** **o** ***bot*** **per effettuare automaticamente numerosi acquisti online**, generalmente di piccola entità, in modo da verificare che i conti siano ancora validi e determinare eventuali limiti di spesa associati (Canfield 2018). Dopo questi acquisti 'di prova' (***card testing***), vengono invece effettuati vari acquisti di grandi dimensioni fino ad esaurire l'intero credito disponibile oppure i dati vengono rivenduti sul *dark web* (CyberSource 2020).

Quando il titolare effettivo dell'account si accorge della frode, contesta le transazioni al suo istituto di credito che generalmente procede al **rimborso (cosiddetto *chargeback*)** e si rivale nei confronti del venditore. Il cliente, una volta ottenuto il rimborso, non procede a sporgere denuncia alle forze dell'ordine, penalizzando i *marketplace*, soprattutto quando sono estranei alla vendita del falso, e non consentendo alle autorità di monitorare in maniera appropriata il fenomeno. Proprio per evitare questo fenomeno, già nel 2012, è stato lanciato il '**Project Chargeback-Leading the Charge(Back) against fakes!**' (vedi Box 23 nel Capitolo 4).

Box 15. Uso di carte di credito clonate in schemi fraudolenti

Tra maggio 2019 e ottobre 2020, un *marketplace* (che ha preferito non svelare il proprio nome) ha individuato movimenti sospetti da parte di alcuni account di recente costituzione durante il monitoraggio continuo delle attività relative agli ordini e ai resi. Lo schema era il seguente:

- i criminali aprivano un account come clienti sul *marketplace*;
- **a distanza di qualche minuto**, dallo stesso account venivano effettuati **ordini per un importo significativo** con carta di credito, richiedendo la **spedizione veloce**;
- **ad ordine non ancora consegnato**, veniva inoltrata una **richiesta di reso**, con rimborso tramite credito da spendere sulla piattaforma (trasferibile però anche su altri metodi di pagamento indicati dal cliente);
- al momento della consegna, il corriere non trovava nessuno all'indirizzo di spedizione indicato e il **telefono di cellulare fornito risultava inesistente**;
- il collo spedito tornava nei magazzini e, dopo qualche giorno, veniva accettato per il reso (trattandosi di un ordine mai consegnato) ed il **rimborso erogato**;
- **il credito erogato veniva poi trasferito** a stretto giro sul profilo PayPal associato all'account.

Dopo un'analisi approfondita, il *marketplace* ha accertato che le carte di credito italiane utilizzate per gli acquisti **erano risultate frodate** e l'istituto di credito coinvolto aveva già provveduto a risarcire i propri clienti. Individuata la frode, il *marketplace* ha contattato PayPal per chiedere un controllo approfondito sull'account, inviando la documentazione necessaria. Solo dopo un anno e diversi solleciti, PayPal ha provveduto a sospendere l'account. Nonostante la chiusura dell'account, il responsabile **ha continuato ad agire modificando parzialmente la procedura**, creando un nuovo account Paypal per ogni account aperto sul *marketplace*. A questo punto, il *marketplace* ha iniziato ad analizzare i dati delle operazioni per cercare di individuare dei *pattern* specifici che permettessero di anticipare la frode. Incrociando i dati su **zona geografica, indirizzo IP, sistema di pagamento e tipo di spedizione**, il *marketplace* ha individuato svariati ordini effettuati con la medesima procedura, presumibilmente riconducibili ad uno stesso individuo che operava da telefono cellulare (individuato provando a richiedere il cambio password di un account di nuova creazione) e/o da una postazione fissa ad accesso pubblico (gli ordini venivano effettuati sempre tra il lunedì e il venerdì, dalle 9:00 alle 17:00).

3.3.3 Resi fraudolenti

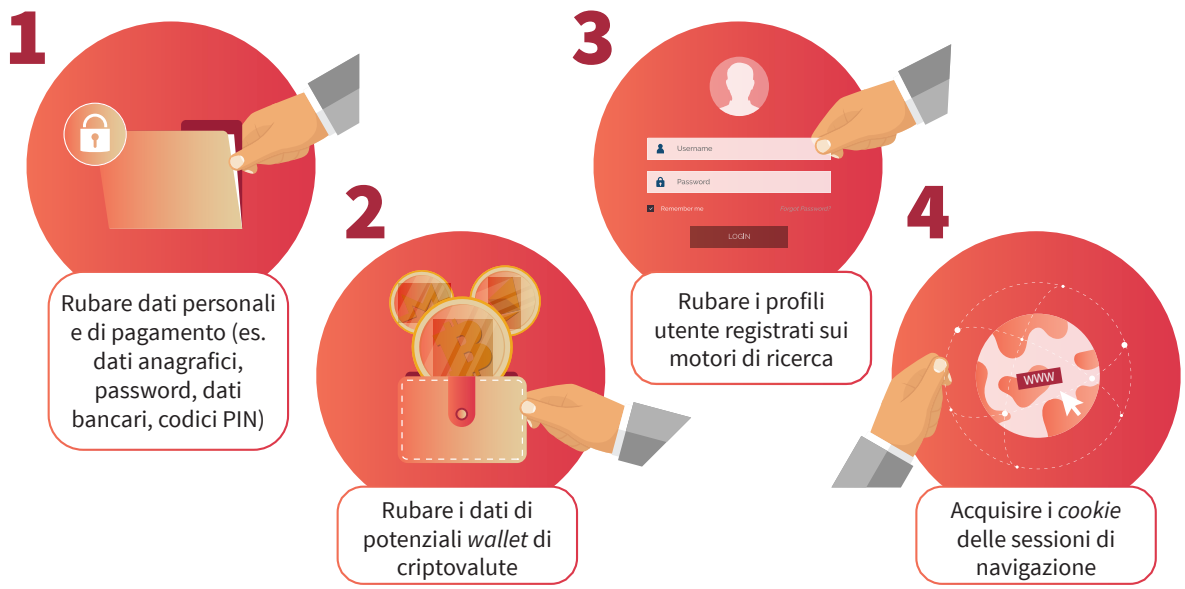
I contraffattori, tramite account creati ad hoc o account violati di consumatori terzi, procedono ad acquistare prodotti sulla piattaforma di *e-commerce* ma, subito dopo aver ricevuto la merce, avviano una richiesta di reso. Al posto dei prodotti acquistati, **restituiscono però versioni contraffatte**. I prodotti originali possono venire poi utilizzati per studiare i segni distintivi ai fini della produzione futura di copie ancora più simili oppure possono essere rivenduti sul mercato secondario (Bosisio et al. 2017). Questi schemi fraudolenti sono inoltre agevolati, come evidenziato dai ricercatori di Flashpoint (2019), dalla diffusione sui forum nel *Deep Web* di individui che vendono numeri seriali di prodotti e false ricevute.

Box 16. Resi fraudolenti e prodotti contraffatti

Tra marzo ed aprile 2021, Yoox-Net-A-Porter Group ha individuato uno schema fraudolento sul proprio *marketplace* che coinvolgeva i resi fraudolenti di prodotti contraffatti. Gli account coinvolti (tutti associati ad indirizzi nel medesimo paese europeo) acquistavano capi d'abbigliamento di lusso sulla piattaforma e, a stretto giro, ne effettuavano il reso, sostituendoli però con delle versioni contraffatte. Quest'ultime venivano prontamente individuate da Yoox-Net-A-Porter Group grazie alle verifiche di operatori specializzati che accertavano come i prodotti restituiti presentassero infatti materiali, etichette, loghi e rifiniture spesso molto diversi dagli originali. In tal senso, Yoox-Net-A-Porter Group ha ulteriormente rafforzato la collaborazione con i titolari di diritti di proprietà intellettuale richiedendo la condivisione di scansioni 2D e 3D dei prodotti, in modo da facilitare l'individuazione automatica dei resi fraudolenti.

3.3.4 Diffusione di software malevoli

I siti fraudolenti e i siti clone istituiti e gestiti dai gruppi criminali per vendere prodotti contraffatti possono essere utilizzati anche per **diffondere *software* malevoli (*malware*)**[15] così da infettare i dispositivi di utenti inconsapevoli al fine di:



15. I *malware* (o *software* malevoli) è un termine generico che comprede tutti i programmi o file che sono pensati intenzionalmente per danneggiare computer, network o server.

Box 17. *Software* contraffatti per veicolare *ransomware*

A settembre 2021, la *Cybersecurity and Infrastructure Security Agency* (CISA) e il *Federal Bureau of Investigation* (FBI) hanno osservato una diffusione dell'utilizzo del *ransomware-as-a-service* (RaaS) 'Conti' in attacchi *cyber* a diverse organizzazioni in tutto il mondo (CISA 2021). Tra le varie modalità d'attacco utilizzate per ottenere l'accesso ai dispositivi (es. spear *phishing*[16], *vishing*[17]) i criminali utilizzavano anche *software* contraffatti, pubblicizzati tramite portali opportunamente predisposti, che venivano scaricati dagli utenti. Una volta ottenuto l'accesso ai dispositivi degli utenti, i criminali utilizzavano la cosiddetta '*double extortion*', ovvero l'esfiltrazione, la cifratura e la successiva pubblicazione dei dati sensibili rubati in assenza di pagamento del riscatto (solitamente richiesto in criptovalute).

16. Lo *spear phishing* è una tipologia di truffa che ha come bersaglio una determinata azienda o persona. A differenza del phishing, i criminali personalizzano gli attacchi utilizzando informazioni sulla vittima acquisite tramite tecniche di *social engineering*, in modo da rendere i messaggi ingannevoli più precisi ed efficaci.

17. Il *vishing* (o *voice phishing*) è una tipologia di truffa che avviene al telefono o tramite un messaggio vocale.

4.

Attività di prevenzione e contrasto: le sfide e le buone pratiche

Le attività di contrasto ai nuovi schemi e trend della contraffazione online, illustrati nel capitolo precedente, si basano su due linee d'intervento principali:

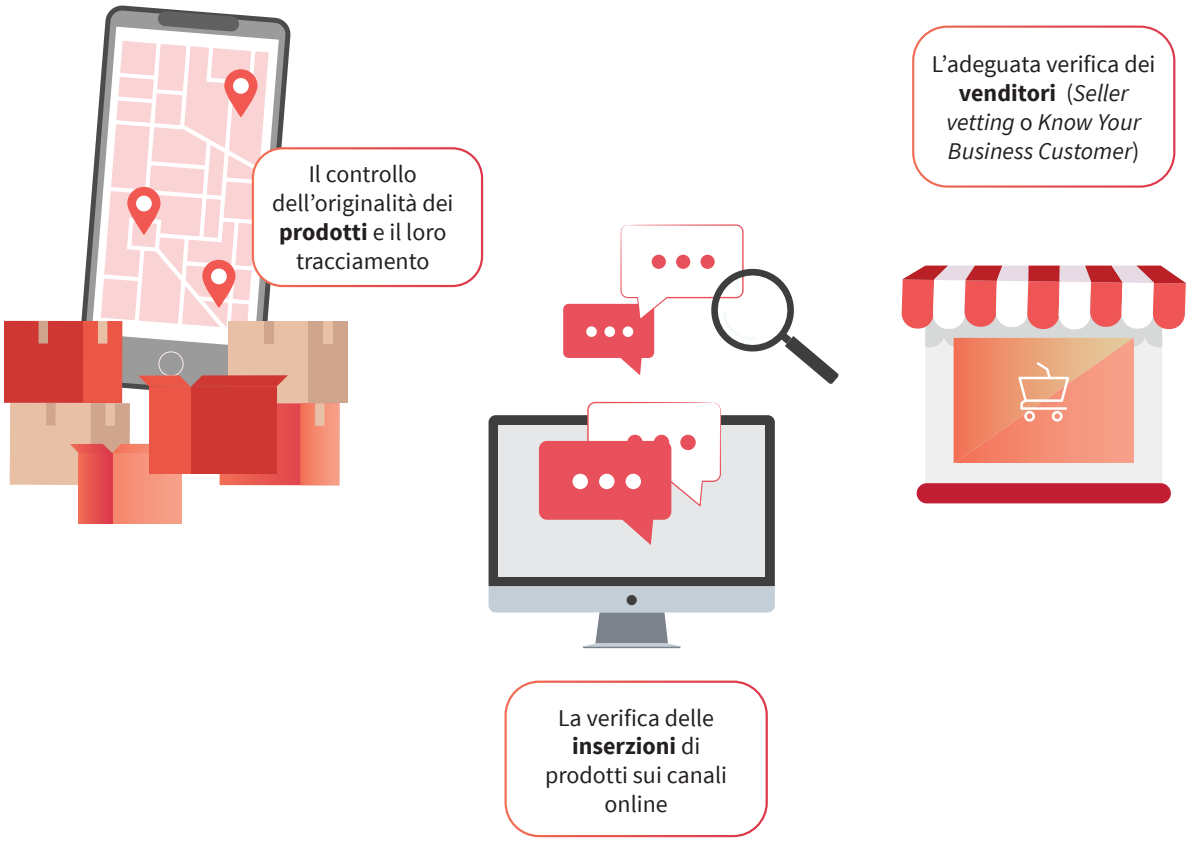
- la **prevenzione** attraverso il controllo dei prodotti, delle inserzioni e dei venditori sui mercati online;
- la collaborazione e lo scambio informativo tra i **diversi *stakeholder***, in particolare tra forze dell'ordine, *marketplace* e titolari di diritti.

Il Capitolo 4 illustra nel dettaglio queste due linee, evidenziando, da una parte, le vulnerabilità che le caratterizzano e, dall'altra, le buone pratiche messe in atto dagli attori in questo ambito. Basandosi su interviste, casi studio e report, laddove disponibili, sono illustrati e discussi:

- i **processi** di prevenzione e collaborazione messi in atto;
- eventuali informazioni sull'**impatto positivo** che alcune buone pratiche hanno generato.

4.1 Prevenzione

Le attività di prevenzione alla vendita di 'falsi' sul web hanno lo scopo di impedire, in prima istanza, ai contraffattori di accedere ai mercati online, minimizzando quindi il numero di prodotti contraffatti in vendita sui canali online, tutelando i consumatori e aumentando la loro fiducia nei confronti dell'*e-commerce*. In tal senso, risultano di particolare rilevanza tre attività:



Box 18. Linee guida dell'OECD per affrontare le sfide emergenti della contraffazione online

A dicembre 2021, l'OECD ha pubblicato lo studio '*E-commerce* Challenges in Illicit Trades in Fakes: Governance Framework and Best Practices' (OECD 2021) fornendo una panoramica delle contromisure, a livello pubblico e privato, per contrastare l'abuso delle piattaforme online da parte dei contraffattori. L'OECD suggerisce di tenere in considerazione i seguenti aspetti nelle revisioni periodiche di queste contromisure:

- coinvolgere attivamente i *marketplace* nell'individuare le transazioni illecite e nel prendere provvedimenti contro i responsabili;
- promuovere soluzioni come, ad esempio, codici di condotta adottati volontariamente dagli *stakeholder* nel settore privato per mostrare la loro eccellenza;
- promuovere la *self-regulation* del settore privato per affrontare le minacce emergenti;
- revisionare e modificare le *policy* in materia di anticontraffazione, sia nazionali sia internazionali, in modo da cambiare significatamente la percezione dei rischi e dei benefici da parte dei contraffattori;
- promuovere la condivisione delle informazioni tra i diversi *stakeholder* in modo da superare le barriere giurisdizionali ed istituzionali;
- coinvolgere tutti gli intermediari, compresi gli operatori postali, i corrieri, i fornitori di servizi di logistica per i *social media* e i fornitori di servizi di pagamento;
- revisionare l'adeguatezza delle informazioni riguardanti le spedizioni di piccole dimensioni e il ruolo degli intermediari di vendita;
- applicare l'esenzione de *minimis*, contenuta nell'articolo 60 dell'Accordo WTO-TRIPS, solo ai beni posseduti dai passeggeri in entrata e non alle *small parcel*;
- rafforzare le procedure di *vetting* delle terze parti;
- tutelare la privacy dei diversi *stakeholder* online.

4.1.1 Controllo dei prodotti

I sistemi di tracciamento anticontraffazione dei prodotti adottati dagli *stakeholder* si basano su **diverse soluzioni tecnologiche** che garantiscono l'autenticità del bene, dalla produzione fino all'arrivo al consumatore finale. Le principali sono discusse di seguito, presentando anche le relative *best practice*.

Soluzioni per la tracciabilità dei prodotti

Per assicurare l'integrità della catena di produzione e la tutela dei diritti di proprietà intellettuali, sono state sviluppate una serie di soluzioni tecnologiche che permettono di identificare univocamente un prodotto, garantendone l'autenticità. In particolare, come riportato da un recente studio dell'EUIPO (2021a), queste si dividono in:

- **soluzioni di tipo materiale**: includono codici a lettura ottica (monodimensionali e bidimensionali), inchiostri, filigrane e segni identificativi univoci;

- **soluzioni elettroniche:** includono RFID (Radio-Frequency Identification)[18], NFC (Near Field Communication)[19], bande magnetiche e chip a contatto;
- **soluzioni chimico-fisiche**: includono tecnologie di *Surface Fingerprint e Laser Surface Analysis*[20], codifica tramite colla e altri traccianti;
- **soluzioni per media digitali**: includono i sistemi di *Digital Rights Management* (DRM)[21].

Alcune delle principali *best practice* in quest'ambito sono elencate nella tabella di seguito. I titolari di diritti sono molto attivi nel controllo della loro filiera produttiva (es. fornitori, grossisti, rivenditori autorizzati) per evitare che, consapevolmente o inconsapevolmente, eventuali prodotti contraffatti possano essere venduti ai clienti finali, e sono spesso supportati in questa attività dai *marketplace*.

Tabella 3. Principali iniziative di *marketplace* e titolari di diritti di proprietà intellettuale per la tracciabilità dei prodotti.

▶ Iniziativa: **Amazon 'Transparency'**
Nel 2019, **Amazon ha lanciato 'Transparency'**, un servizio di serializzazione dei prodotti che attualmente copre 10 paesi al mondo ed include più di 15.000 marchi registrati (*Amazon 2021b*). I *brand owner* che aderiscono al programma applicano sull'imballaggio esterno di ogni singola unità di prodotto un codice 2D alfanumerico, univoco e non sequenziale che viene scansionato da Amazon prima di spedirla al cliente. Anche i venditori terzi devono fornire ad Amazon i codici per ogni prodotto di un marchio registrato a Transparency che gestiscono. Se i prodotti scansionati non superano questo controllo di autenticità, vengono bloccati e sottoposti ad ulteriori indagini. Il codice 2D permette inoltre ai clienti, tramite l'*app* di Transparency, di verificare l'autenticità del prodotto e di ottenere ulteriori informazioni se condivise dal venditore (es. data di fabbricazione, luogo di produzione, data di scadenza). Al tempo stesso, i *brand owner* registrati hanno accesso al report che permette loro di monitorare l'efficacia di Transparency, fornendo informazioni sul numero di: • unità di prodotto che sono state bloccate perché non riportavano il codice Transparency; • scansioni dei codici non riuscite a causa di una discordanza tra il prodotto ed il codice applicato; • tentativi di offerta che sono stati rifiutati perché i venditori non sono stati in grado di fornire codici Transparency validi;

18. È una tecnologia che permetta l'identificazione automatica, tramite onde radio, di tag applicati ai prodotti.

19. È una tecnologia che, contrariamente ai più semplici dispositivi RFID, consente una comunicazione bidirezionale tra un initiator e un target.

20. Sono tecnologie che analizzano la composizione delle superfici dei materiali, identificando potenziali difformità strutturali e consentendo di identificare univocamente il prodotto.

21. L'insieme delle tecnologie informatiche che si occupano della gestione in forma digitale dei diritti di proprietà intellettuale.

• notifiche di sospetta contraffazione.

I benefici della partecipazione al programma sono molteplici. Come riferito da Stefano Bolzicco, titolare di LoryArreda, 'Sono su Amazon dal 2016 e ho aderito da subito a Transparency. Nel breve periodo, si è trattato di un beneficio psicologico: mi sentivo protetto. Sul lungo periodo, ho riscontrato un aumento della credibilità del marchio. Il fatturato è cresciuto del 35 per cento' (Il Sole 24 Ore 2021a).[22]

▶ Iniziativa: **eBay 'Authenticity guarantee'**

A settembre 2020, **eBay ha lanciato il programma 'Authenticity Guarantee'** per gli orologi di lusso venduti per più di 2.000$ negli Stati Uniti, estendendolo poi ad ottobre 2020 anche alle *sneaker* vendute a più di 100 dollari (eBay 2021). I venditori che aderiscono al programma, dopo aver ricevuto un ordine, spediscono il prodotto ad un centro di autenticazione di eBay che si occupa di effettuare una serie di accertamenti fisico-tecnici per accertarne l'autenticità. La procedura può avere due esiti:

a. se il prodotto supera le verifiche, il Centro appone un *tag* NFC sul prodotto (che funge da certificato di garanzia) e lo spedisce al cliente finale;
b. se il prodotto non supera le verifiche, eBay si occupa di rimborsare immediatamente il cliente e di avviare ulteriori verifiche con il venditore. Nel caso il prodotto risulti effettivamente non originale, eBay provvede a rimuovere immediatamente le inserzioni sul *marketplace* ed avviare azioni legali nei confronti del venditore.

Il programma offre anche una tutela nei confronti di possibili frodi sul prodotto. Infatti, nel caso in cui il cliente effettui il reso del prodotto, quest'ultimo viene nuovamente esaminato dal centro di autenticazione di eBay prima di essere rispedito al venditore, in modo da evitare la restituzione fraudolenta di un prodotto diverso dall'originale (es. contraffatto).

▶ Iniziativa: **Luxottica GLOW**

Luxottica ha sviluppato GLOW (Guaranteed Luxottica Origin Worldwide), un sistema di tracciabilità basato sulla tecnologia RFID che verifica l'autenticità dei prodotti e la regolarità dei canali di vendita tramite un sensore (tag RFID) incorporato direttamente nelle montature (Luxottica 2017). Il dispositivo contiene le informazioni essenziali per identificare, in modo univoco, ogni paio di occhiali dalla produzione alla destinazione di vendita, impedendo che:

a. prodotti contraffatti entrino nella filiera di distribuzione;
b. prodotti originali vengano dirottati verso canali di vendita non autorizzati.

Altre buone pratiche

Moncler, già dal 2009, apponeva su tutti i prodotti messi in vendita un'etichetta anticontraffazione che poteva essere verificata su un sito apposito (*code.moncler.com*). Dal 2016, oltre a questa modalità di verifica, Moncler si è dotata anche di etichette basate su tecnologia RFID che, tramite *app*, permettono di leggere i QR *code* e tag NFC associati al prodotto.

Salvatore Ferragamo, dopo i primi progetti pilota tra il 2011 e il 2013, ha adottato per quasi tutti i suoi prodotti in pelle dei tag NFC per garantirne la tracciabilità. Il cliente, tramite apposita APP, può verificare l'autenticità del prodotto ed avere accesso a tutta una serie di informazioni ulteriori.

22. Traduzione a cura degli autori.

Brembo, nel 2021, ha sviluppato l'app **'Brembo Check'** per permettere ai clienti e rivenditori di individuare eventuali prodotti contraffatti. Una volta acquistato un prodotto UPGRADE, il cliente/rivenditore può accertarne l'originalità scannerizzando, tramite l'app, il QR code riportato sull'etichetta. Per evitare manomissioni, l'etichetta è stata realizzata tramite una particolare procedura di stampa e di applicazione che rende inutilizzabile il QR code se si cerca di rimuoverla, impedendo quindi che venga apposta su un prodotto diverso da quello originale. Il lancio di questa app potenzia ulteriormente il sistema anticontraffazione di Brembo che, già nel 2016, vendeva determinati prodotti (*performance aftermarket*) insieme ad una card anticontraffazione in un astuccio sigillato. Il cliente doveva grattare la striscia argentata sulla card per ottenere un codice univoco a sei cifre che, una volta inserito nella sezione apposita del sito di Brembo, avrebbe certificato l'originalità del prodotto.

Soluzioni di Distributed Ledger Technology (DLT) e Blockchain

Nell'ambito della gestione della *supply chain*, le tecnologie di *Distributed Ledger Technology* garantiscono una più semplice tracciabilità dei prodotti, consentendo di monitorarne anche l'autenticità. Ogni transazione (dalla produzione fino alla vendita) può essere documentata e registrata in un **registro distribuito**, dove l'inserimento delle informazioni è possibile solo previo riconoscimento dell'utente (es. firma digitale), impedendo eventuali modifiche non autorizzate.

Le potenzialità della Blockchain in ambito anticontraffazione sono state riconosciute anche a livello europeo, portando alla creazione dell'***Anti-counterfeiting Blockathon Forum***. Quest'ultimo, realizzato da Commissione Europea e EUIPO, riunisce esperti con background diversi per realizzare una futura infrastruttura comune basata su Blockchain a cui possono collegarsi tutti gli *stakeholder* coinvolti (es. intermediari, titolari dei diritti di proprietà intellettuale, forze dell'ordine) per condividere dati ed informazioni al fine di tutelare l'integrità delle catene di approvvigionamento dall'infiltrazione di prodotti contraffatti (EUIPO 2019b).

L'utilizzo e l'adozione di soluzioni basate sulla *distributed ledger technology* rimane incerto o solo a livello teorico, con applicazioni limitate come l"IPR Prection Tech Brain' di Alibaba (2020) e l'***Aura Blockchain Consortium*** (lanciato ad aprile 2021 dai Gruppi Prada, LVMH e Richemond) che ha sviluppato una soluzione *blockchain* globale, aperta a tutti i marchi di lusso a livello mondiale, che permette ai clienti di seguire facilmente il ciclo di vita dei prodotti, dalla produzione alla distribuzione. Allo stesso modo, molti *partner* tecnici specializzati sul mercato stanno sviluppando soluzioni di questo tipo (vedi Box 19).

Box 19. Anticontraffazione e soluzioni di blockchain

A ottobre 2021, una *start-up* svizzera attiva nell'ambito della brand protection ha sviluppato una soluzione che, combinando *Blockchain* e tecnologia *Near Field Communication* (NFC), garantisce l'autenticità dei prodotti per il settore della profumeria (Il Sole 24 Ore 2021b). Ogni flacone viene sigillato con un tag NFC, un sigillo di protezione fisico/digitale che protegge, ad esempio, dal rabbocco fraudolento e dalla diluizione. Una volta sigillato, viene creata una copia digitale del prodotto che viene memorizzata sulla *Blockchain*, impedendone la successiva modifica ed alterazione. I tag NFC permettono a produttore e consumatore finale di comunicare *end-to-end*: i produttori possono monitorare la propria *supply chain*, impedendo azioni fraudolente, mentre i consumatori possono verificare l'autenticità dei prodotti in maniera *contactless*.

4.1.2 Soluzioni per il monitoraggio delle inserzioni

Nonostante le soluzioni (procedurali e tecnologiche) adottate, i contraffattori riescono ancora ad operare online. Per impedire la vendita di prodotti contraffatti, alcuni *marketplace* si sono dotati di algoritmi di intelligenza artificiale che permettono di monitorare la grande mole di inserzioni ed **individuare e rimuovere proattivamente quelle che potenzialmente violano diritti di proprietà intellettuale**. Per un elenco e una descrizione esaustiva di queste tecnologie si rimanda al recente rapporto dell'EUIPO (2020) sull'argomento. Alcune *best practice* sono invece elencate di seguito.

Nel 2019, **Alibaba ha lanciato *'IPR Protection Tech Brain'***, una *suite* proprietaria basata su intelligenza artificiale, *cloud computing* e *blockchain*, che monitora proattivamente le inserzioni (Alibaba Group 2020). Gli algoritmi della suite, che dal loro lancio hanno analizzato più di 13,7 miliardi di immagini, sono stati addestrati sulla base delle caratteristiche di un campione di inserzioni che violano diritti di proprietà intellettuale (condivisi dai *brand owner* stessi). Nel complesso, durante il 2020, hanno consentito di rimuovere il 96% delle inserzioni che violavano questi diritti subito dopo la loro pubblicazione. Questi algoritmi hanno anche contribuito a diminuire del 33% le inserzioni rimosse a seguito della segnalazione dei clienti, con il tasso di rimborsi effettuati nei confronti di quest'ultimi per l'acquisto di prodotti contraffatti pari a 1,08 ogni 10.000 transazioni.

Nel 2019, **Amazon ha lanciato 'Project Zero'**, un sistema di anticontraffazione che offre protezione ai clienti e ai brand owner (attualmente più di 18.000 marchi sono registrati) tramite tre strumenti principali:

- **protezioni automatiche**: gli algoritmi di *machine leaning* di Amazon eseguono una scansione continua dei tentativi di modifiche delle inserzioni presenti sul *marketplace* al fine di individuare potenziali abusi. Nel 2020, questi algoritmi hanno analizzato oltre 5 miliardi di aggiornamenti giornalieri effettuati dai venditori (es. modifica titolo, variazione prezzo) (Amazon 2021c);
- **rimozione *self-service* di prodotti contraffatti**: i *brand* iscritti a Project Zero hanno la possibilità di rimuovere in autonomia le eventuali inserzioni di prodotti contraffatti presenti sul *marketplace*. Tutte le inserzioni rimosse vengono poi utilizzate per addestrare gli algoritmi di *machine learning* e migliorare l'individuazione dei prodotti contraffatti in futuro;
- **tracciabilità dei prodotti**: i *brand owner* iscritti a Project Zero possono anche scegliere di applicare, durante il processo di fabbricazione, un codice univoco su ogni unità di prodotto in modo da permettere ad Amazon di individuare più facilmente prodotti contraffatti.

Al momento, **più del 75%** dei *brand owner* iscritti al programma non ha ancora utilizzato lo strumento self-service di rimozione delle inserzioni, grazie alle protezioni automatiche che proattivamente bloccano le inserzioni che costituiscono potenziali violazioni dei diritti di proprietà intellettuale prima che vengano pubblicate (Amazon 2021c).

Nel 2020, **eBay** ha bloccato e rimosso proattivamente circa **31,5 milioni di inserzioni** che violavano diritti di proprietà intellettuale mentre circa **1,9 milioni di inserzioni** sono state rimosse su segnalazioni di terze parti, portando alla **sospensione definitiva degli account di 53.000 utenti** (eBay 2021). Gli algoritmi di intelligenza artificiale utilizzati permettono sia di impedire che inserzioni che violano diritti di proprietà intellettuali vengano pubblicate (inviando anche un messaggio automatico al venditore che indica le *policy* violate) sia di contrassegnare alcune inserzioni per un approfondimento manuale da parte del servizio clienti.

4.1.3 Adeguata verifica dei venditori

Come già discusso in precedenza, i contraffattori cercano di aprire account come venditori sui *marketplace*, in forma individuale o per interposta persona giuridica, così da distribuire beni contraffatti o compiere altri comportamenti illeciti (vedi Sezione 3.3). Questo rischio rende sempre più necessaria **un'adeguata verifica delle terze parti**, in linea con le raccomandazioni emanate in questo settore (Consiglio Nazionale Anticontraffazione 2019) e in ambiti collegati (es. antiriciclaggio, anti-corruzione, 231/2001). Nonostante la rilevanza dell'argomento, **sono carenti le informazioni** sulle prassi attualmente adottate dai *marketplace*:

- da un lato, l'ambito del *Know Your Customer / Know Your Vendor* non è in genere oggetto di osservazione della ricerca scientifica, e quindi non esistono studi approfonditi sul tema;
- dall'altro, gli intervistati su questo argomento hanno giustificato l'impossibilità di condividere informazioni più dettagliate con l'esistenza di vincoli interni al proprio perimetro aziendale. Al contrario, si ringrazia Amazon per la condivisione di informazioni sulla propria procedura di adeguata verifica dei venditori, riportata nel dettaglio nel box 20.

Quando implementata in maniera completa, l'attività di *Know Your Business Customer*, o *Seller vetting*, generalmente si struttura su più livelli, creando un vero e proprio **'imbuto' informativo** che rende difficile ai contraffattori aprire un account di vendita. L'adeguata verifica ha lo scopo di:

- individuare più facilmente eventuali informazioni fraudolente che sono state fornite durante il processo di registrazione. I contraffattori, infatti, insieme ai dati reali di prestanome (es. recapiti e-mail e telefonici, metodi di pagamento) utilizzano spesso anche informazioni fittizie (es. indirizzi), al fine di creare **identità 'sintetiche'** che siano il più possibile verosimili;
- individuare possibili comportamenti anomali all'atto della registrazione, come modifiche ingiustificate a contatti, recapiti, indirizzi;
- individuare possibili collegamenti del venditore con soggetti per cui si osservano **anomalie o precedenti** (es. sanzioni, misure personali o patrimoniali, *media* avversi) che potrebbero essere sintomatiche di comportamenti fraudolenti e che comunque giustificherebbero l'esigenza di ulteriori indagini (*enhanced due diligence*).

Box 20. Le procedure di *Know Your Business Customer* di Amazon

La procedura per verificare l'identità dei potenziali venditori di Amazon combina tecnologie di apprendimento automatico e approfondimenti manuali da parte di operatori. Nel 2020 Amazon ha bloccato oltre 6 milioni di tentativi di aprire un account di vendita - un aumento significativo rispetto ai 2,5 milioni nel 2019 (Amazon 2021c). In media, **solo il 6% delle richieste di registrazione come *seller* supera tutti i processi di verifica.** Per poter completare la registrazione, i potenziali partner di vendita devono effettuare un *on-boarding* da remoto, fornendo un documento di identità dotato di fotografia e una serie di altre informazioni, tra cui l'indirizzo fisico, dati bancari e informazioni fiscali. Le informazioni fornite vengono confrontate con dati di terze parti, inclusi quelli legati a soggetti malintenzionati precedentemente identificati e bloccati. In particolare, Amazon:

a. si collega con ogni singolo potenziale venditore attraverso una chat video o di persona presso un ufficio Amazon per verificarne l'identità e la documentazione fornita;
b. verifica gli indirizzi fisici indicati inviando un codice univoco al loro recapito che deve essere comunicato dai potenziali partner di vendita durante le chat video;
c. verifica con i fornitori di servizi di pagamento i dati bancari dei potenziali partner di vendita per identificare dove vengono erogati i fondi e chi ne è il destinatario.

Una volta autorizzati a vendere sul *marketplace*, i *seller* vengono comunque sottoposti ad un **monitoraggio continuo** al fine di individuare eventuali comportamenti illeciti nel tempo. In tal senso, l'**analisi delle recensioni** dei clienti ricopre un ruolo importante. Gli algoritmi di *machine learning* incrociano automaticamente le recensioni con dati terzi, permettendo di individuare in tempo reale eventuali *cluster* di rischio (es. recensioni generiche, recensioni eccessivamente positive, recensioni ripetitive, numero di recensioni che non corrisponde al numero di prodotti venduti). Come ben noto infatti, queste vengono infatti manipolate dai contraffattori per **aumentare la reputazione** dei loro account come seller (Mayzlin, Dover, e Chevalier 2014; Luca e Zervas 2016). Un recente studio ha analizzato ben 23 gruppi chiusi su Facebook dove i *seller* di un *marketplace* si mettevano d'accordo con clienti compiacenti affinché lasciassero recensioni false (He, Hollenbeck, e Proserpio 2021). Quest'ultimi, infatti, effettuavano l'acquisto sul *marketplace* - in modo che la transazione risultasse a tutti gli effetti – e venivano poi interamente rimborsati, con l'aggiunta di una commissione, dai *seller*.

I controlli di *seller vetting* adottati nell'ambito dell'anticontraffazione prendono ispirazione da meccanismi equivalenti messi in atto in ambito, ad esempio, di ***on-boarding* dei clienti** da parte di banche e assicurazioni e altri soggetti obbligati antiriciclaggio. In questo settore, ai controlli di primo livello – di natura documentale – si accompagnano controlli di secondo livello che possono utilizzare anche sofisticati modelli predittivi e di rischio, capaci di integrare informazioni raccolte in fase di qualifica con dati provenienti da banche dati terze.

Box 21. Sistemi evoluti per il risk assessment delle terze parti

Il centro di ricerca Transcrime dell'Università Cattolica del Sacro Cuore ha sviluppato degli indicatori di rischio che condensano in maniera sintetica delle misure di anomalia relative a diverse caratteristiche delle imprese (es. *pattern* di struttura proprietaria, localizzazione e settore di attività economica, dati economico-finanziari) utilizzabili in attività di *customer due diligence* e di controllo delle terze parti. Tra gli aspetti coperti, ad esempio:

- la complessità della struttura proprietaria non giustificata rispetto ai *cluster* di riferimento (per classe dimensionale e settoriale);
- cambi anomali o ingiustificati di ragione sociale, soci, amministratori, forma giuridica;
- collegamenti con veicoli societari opachi;
- anomalie a livello patrimoniale e contabile.

Gli indicatori e i modelli di rischio sviluppati sono stati testati e validati su alcuni milioni di aziende in nove paesi europei utilizzando come variabile target evidenze di sanzioni e di enforcement sulle imprese o i loro titolari. A questo fine sono stati impiegati diversi metodi di *machine learning* (regressione logistica, naïve Bayes e algoritmi *tree-based*) nell'attività di training e di test. I risultati dell'analisi dimostrano una forte capacità predittiva di questi modelli, capaci di individuare più del 85% delle imprese poi colpite da misure restrittive (Jofre et al., 2021). I modelli, una volta incorporati in applicativi, sono utilizzati sia in ambito pubblico, con finalità di indagine e supervisione, che in ambito privato, ad esempio nel controllo delle terze parti e nella protezione della *supply-chain integrity* e del *procurement integrity*.

Nonostante le buone pratiche di alcuni soggetti, l'attività di *Know Your Business Customer* è spesso ancora approcciata in **maniera poco evoluta** dalla maggior parte delle imprese, soprattutto al di fuori dei settori regolamentati (es. antiriciclaggio, anticorruzione). Al di là dell'acquisizione delle informazioni personali e del controllo di primo livello sulle stesse, sono ancora poco sfruttati:

- l'**intero patrimonio informativo acquisibile** sul venditore, sia da fonti interne (es. collegamenti con altri clienti già censiti, riferimenti in messaggi o recensioni dei clienti) che esterne (es. banche dati di informazioni societarie, fonti aperte);
- le **potenzialità del *data analytics***, che consentono di combinare informazioni di natura diversa e di identificare anomalie sulla base di confronti con gruppi di pari o altri *cluster* di riferimento.

Nonostante le regole stringenti in termini di privacy - si veda ad esempio la Deliberazione del 12 giugno 2019 del Garante della protezione dei dati personali (2019)[23] - è infatti possibile implementare soluzioni efficaci nel pieno rispetto dei dati personali.

23. La deliberazione è consultabile al seguente link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9119868

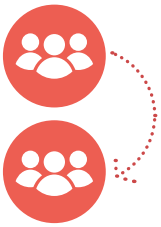
4.2 Collaborazione e scambio informativo

La condivisione di buone prassi, esperienze, dati e conoscenze tra gli *stakeholder* pubblici e privati è essenziale per rafforzare il contrasto alla contraffazione sui mercati online. Negli ultimi anni la collaborazione tra *marketplace*, titolari di diritti di proprietà intellettuale e autorità pubbliche è cresciuta in modo esponenziale. Tuttavia, diversi soggetti intervistati appartenenti sia al settore privato – *marketplace* e *brand owner* – che al settore pubblico hanno segnalato ancora delle difficoltà nell'attivare uno **scambio informativo efficace** tra i diversi *stakeholder* coinvolti. Queste criticità si rilevano su più fronti:

- nella condivisione delle informazioni **dalle autorità pubbliche al settore privato**, ad esempio sui sequestri effettuati da dogane o forze dell'ordine di carichi destinati ad una determinata rete, o sull'esito dei procedimenti giudiziari intentati nei confronti di soggetti o casi segnalati dal settore privato alle autorità. La condivisione di tali informazioni con *marketplace*, operatori di logistica e titolari di diritti potrebbe migliorare le capacità di *early detection* di prodotti fraudolenti e avere un effetto moltiplicatore sull'attività di prevenzione del settore privato;

- nello scambio di informazioni **dal settore privato agli enti pubblici**, che consentirebbe alle autorità di disporre di una più ampia base informativa e di spunti di indagine, e un valido supporto alle attività d'indagine transnazionale. Purtroppo, come anticipato sopra, si osservano diversi livelli di cooperazione e scambio informativo tra *marketplace* e operatori diversi, soprattutto quando questi sono basati al di fuori dell'Unione Europea, e soprattutto nel caso di operatori più piccoli e meno equipaggiati;

- nella condivisione di dati da parte dei **titolari di diritti di proprietà intellettuale** a favore di *marketplace*, società di logistica e autorità pubbliche. Lo scambio potrebbe andare al di là della condivisione delle tradizionali informazioni sui segni distintivi dei prodotti originali, e includere anche forme 'evolute', come tracciati di scansioni 3D dei beni che consentirebbero, tra gli altri, un più immediato rilevamento tramite sistemi di *image recognition* o attraverso gli *scanner* di ultima generazione a disposizione di autorità doganali e operatori di logistica;



- nella condivisione volontaria tra tutti gli ***stakeholder* – pubblici e privati –** di informazioni riguardanti gli attori criminali già identificati, così da evitare che questi possano facilmente muoversi tra canali online diversi. Lo scambio di informazioni potrebbe valere sia per quei soggetti sospetti (società e persone fisiche) che operano come *seller*, che per quelli operanti come consumatori e che già si sono resi protagonisti di attività illecite (es. resi fraudolenti o frodi nei pagamenti).

Purtroppo, nonostante gli sviluppi anche a livello regolamentare e di *policy* (vedi capitolo 5), lo scambio informativo tra questi attori è spesso ostacolato da problemi, reali o presunti, di **protezione dei dati personali, di informazioni sensibili a livello industriale o commerciale, o a livello investigativo**. Questo nonostante esistano ormai anche iniziative simili già lanciate in altri ambiti (es. antiriciclaggio, vedi capitolo 5) e tecnologie evolute capaci di preservare l'integrità e la riservatezza dei dati e l'anonimato dei soggetti segnalati/segnalanti, pur consentendo uno scambio tra le parti (es. *federated learning* ed altri).

Nonostante queste limitazioni, l'analisi della letteratura e dei casi studio ha evidenziato diverse *best practice* che meritano di essere riportate ed analizzate. Queste possono essere divise in tre macrocategorie:

Collaborazione tra stakeholder privati

La condivisione di dati ed informazioni tra titolari di diritti di proprietà intellettuale e *marketplace* permette di individuare, in maniera più efficace, le inserzioni dei venditori che violano tali diritti. In questo senso, gli intervistati hanno però evidenziato come ci sia una sostanziale **assenza di meccanismi appositi** che facilitino questo flusso comunicativo. Di seguito vengono riportate alcune delle principali *best practice* in questo ambito.

Tabella 4. *Best practice* in ambito di collaborazione tra *stakeholder* privati

▶ Iniziativa: **eBay VeRO**
Nel 1998, eBay ha lanciato il programma VeRO (Verified Rights Owner Program) che permette ai brand owner che vi partecipano (attualmente circa 97.000) di segnalare e far rimuovere eventuali inserzioni di venditori che violano i loro diritti di proprietà intellettuale. Nel caso la violazione sia accertata, eBay rimuove immediatamente l'inserzione e valuta eventuali azioni legali nei confronti dei venditori. Come riportato da eBay, attualmente solo il 2,2% dei 19 milioni di venditori attivi sulla piattaforma ha subito una rimozione di un'inserzione a seguito di una segnalazione tramite il programma VeRO.
▶ Iniziativa: **Alibaba 'Intellectual Property Protection Platform'**
Nel 2016 Alibaba ha lanciato '*Intellectual Property Protection Platform*' (IPP), una piattaforma unica che integra AliProtect e TaoProtect, lanciate rispettivamente nel 2008 e nel 2016. I titolari di diritti di proprietà intellettuale possono aprire un account unico su questa piattaforma per inviare richieste di rimozione di contenuti che violano i loro diritti di proprietà intellettuale su tutti e sette i *marketplace* del gruppo. Nel 2020, i titolari di diritti di proprietà intellettuale iscritti all'IPP sono aumentati del 40% rispetto al 2019, con il 98% delle richieste di *take-down* inoltrate che sono state processate entro 24 ore (un dato in aumento rispetto al 96% del 2019) (Alibaba Group 2020).

▶ Iniziativa: **Amazon 'Brand Registry'**

Nel 2017, Amazon ha lanciato 'Brand Registry', un servizio gratuito che mette a disposizione dei *brand owner* registrati l'accesso ad una serie di strumenti che li aiutano a tutelare i propri marchi. In particolare, i brand hanno la possibilità di controllare in maniera accurata i testi, le foto e i contenuti delle pagine di dettaglio dei prodotti, assicurandosi che le informazioni visualizzate dai clienti siano sempre esatte. Inoltre, forniscono informazioni che vengono utilizzate da Amazon per migliorare le proprie misure proattive che riescono così ad invidiare e rimuovere più facilmente le potenziali violazioni. Nel 2020, più di 500.000 marchi si sono iscritti al programma e, in circa 5 anni, si è arrivati in media ad una riduzione del 99% delle segnalazioni di violazioni sospette.

Box 22. Gruppi di lavoro di soggetti privati per il contrasto alla contraffazione online

Nel 2010 la Commissione Europea ha invitato piattaforme di *e-commerce*, titolari di diritti di proprietà intellettuale e associazioni di categoria a firmare un ***Memorandum of Understanding*** **(MoU)** sulla prevenzione della vendita di prodotti contraffatti online (finalizzato nel maggio 2011). Il MoU ha l'obiettivo di definire una nuova prassi per la lotta alla contraffazione online e di **promuovere la collaborazione** tra i firmatari per migliorare l'efficacia delle strategie di prevenzione e contrasto. Incentivando il dialogo tra le parti, il MoU prevede tre linee di difesa per contrastare l'offerta di prodotti contraffatti online:

- sensibilizzazione dei clienti sui rischi e gli effetti negativi derivanti dalla contraffazione. In tal senso, le piattaforme di *e-commerce* si impegnano a fornire ai consumatori tutte le informazioni necessarie per prevenire l'acquisto di prodotti contraffatti;
- adozione di misure proattive (di natura tecnico e/o procedurale) per individuare in maniera tempestiva ed efficace la commercializzazione di prodotti contraffatti;
- previsione di procedure di segnalazione e rimozione dei prodotti contraffatti da parte delle piattaforme di *e-commerce*.

Nel 2017, la Commissione ha pubblicato un documento che riporta i risultati del primo anno di funzionamento del MoU revisionato. I risultati sono basati su alcuni KPI previsti nel MoU e calcolati dai firmatari. Ad esempio, dei primi 100 risultati derivanti da ricerche effettuate sui *marketplace* tra maggio e giugno 2017, il 14,3% riguarda potenziali prodotti contraffatti. Inoltre, il 97,4% delle inserzioni che potenzialmente violano diritti di proprietà intellettuale sono state rimosse proattivamente da parte dei *marketplace* mentre solo il 2,6% a seguito di segnalazioni dei titolari di diritti.

Come riportato in un recente *position paper* di Amazon (2021a), negli Stati Uniti diversi *marketplace* hanno lavorato attivamente per la creazione di un meccanismo di condivisione di informazioni sui contraffattori verificati. I risultati di questa iniziativa sono incoraggianti: Amazon ha accertato come il 16% dei contraffattori verificati dalle altre piattaforme di *e-commerce* avesse cercato di vendere anche tramite il loro *marketplace*.

La collaborazione tra *markeplace* e titolari di diritti di proprietà intellettuale non si limita solo all'individuazione e rimozione di inserizioni di prodotti contraffatti ma riguarda anche la denuncia e l'avvio dell'azione legale, tramite cause civili congiunte, nei confronti dei contraffattori individuati. In tal senso, sono di particolare rilevanza alcune cause civili congiunte come Amazon e Ferragamo (Amazon 2021a), Amazon e HanesBrands (Amazon 2021c) e Facebook e Gucci (Reuters 2021).

È importante comunque sottolineare che l'attenzione non è rivolta esclusivamente ai grandi *player* ma anche alle piccole e medie imprese (PMI). Amazon, ad esempio, sta portando avanti cause congiunte anche insieme a JL Childress, che vende prodotti da viaggio per genitori, o DutchBlitz, un'azienda produttrice di giochi di carte a conduzione familiare (Il Sole 24 Ore 2021a). Il tema in realtà non è secondario perché, secondo una recente indagine dell'EUIPO (2019a), solo il 9% delle PMI ha registrato i propri diritti di proprietà intellettuale rispetto al 36% delle aziende più grandi. Proprio per questo motivo, Amazon ha anche sviluppato l'IP *Accelerator* per aiutare le PMI a tutelare la loro proprietà intellettuale. Come sottolineato da Mary Beth Westmoreland, vice presidente di Amazon con delega a *Technology & Brand Protection*, 'Oltre ad avere collaborazioni in atto con associazioni di imprese locali, abbiamo progettato IP Accelerator pensando specificamente alle piccole imprese, che le mette in contatto con una rete selezionata di studi legali specializzati nella proprietà intellettuale che ha accettato di operare a tariffe fisse e competitive' (Il Sole 24 Ore 2021a). Nel 2020, oltre 7.000 PMI hanno aderito e, oltre ad essere stati messi in contatto con studi legali di fiducia, hanno ricevuto immediato accesso agli strumenti di protezione del marchio previsti da *Amazon Brand Registry*.

Collaborazione pubblico-privata

Di particolare rilievo, come evidenziato anche dalle interviste, è la collaborazione tra *stakeholder* privati e forze dell'ordine e autorità pubbliche, nelle attività d'indagine e di contrasto alla contraffazione online tramite lo scambio d'informazioni. Nonostante l'importanza di questa collaborazione, le interviste hanno anche sottolineato la generale mancanza di meccanismi automatici che facilitino lo scambio di informazioni e dati. Alcuni *stakeholder* privati rappresentano invece delle *best practice* in quest'ambito. Ad esempio, eBay ha sviluppato il '**Regulatory Portal**' tramite cui le forze dell'ordine possono inviare richieste di dati ed informazioni. Durante il 2020, eBay ha ricevuto 38.497 richieste da parte delle forze dell'ordine a livello mondiale ed ha fornito, rispettando i vincoli normativi sulla privacy, informazioni su 42.071 utenti (eBay 2021). Allo stesso modo, PayPal ha lanciato il '**Safety Hub - PayPal Law Enforcement Tool**', una piattaforma web che permette alle forze dell'ordine e autorità giudiziarie registrate di richiedere più velocemente informazioni e dati su utenti PayPal. La piattaforma sostituisce i precedenti metodi per contattare PayPal (es. posta, e-mail, fax) e le richieste pervenute vengono processate manualmente dal *Global Investigations Team* ed evase entro 10 giorni lavorativi dalla ricezione.

Oltre a questi meccanismi per lo scambio d'informazioni, i casi studio hanno evidenziato anche altre *best practice* in questo ambito che hanno permesso l'esito positivo delle indagini e l'individuazione dei responsabili delle condotte illecite.

Tabella 5. *Best practice* in ambito di scambio informativo tra forze dell'ordine e *stakeholder* privati

▶ *Best practice*: **Conduzione di attività di '*internet brand intelligence*'**
▶ Indagine di riferimento: **Bologna Luxury, Aphrodite II**
Le attività di *internet brand protection* condotte da diversi brand hanno permesso l'individuazione e la rimozione di inserzioni sui canali online che violavano i loro diritti di proprietà intellettuale. I risultati di queste attività sono stati poi prontamente condivisi con le forze dell'ordine che, sulla base di questi elementi, hanno avviato le indagini per l'individuazione dei soggetti che si nascondevano dietro gli account *social*. In questo caso, è risultata fondamentale l'iniziativa del *brand* e la tempestiva condivisione con le forze dell'ordine delle informazioni su (a) **post rimossi**; (b) **account coinvolti**.
▶ *Best practice*: **Monitoraggio proattivo della rete internet da parte delle forze dell'ordine**
▶ Indagine di riferimento: **Falsi Online**
Il monitoraggio proattivo dei *social network* da parte della Guardia di Finanza di Luino ha permesso l'individuazione di account che pubblicizzavano e vendevano prodotti contraffatti. Una volta acquisite queste informazioni, la Guardia di Finanza ha coinvolto i titolari dei diritti di proprietà intellettuale interessati per accertare, tramite la redazione di relazioni tecniche apposite, la non originalità dei prodotti messi in vendita. In questo caso, è risultata fondamentale la tempestiva condivisione di: (a) **immagini dei prodotti** messi in vendita; (b) **canali utilizzati** per la vendita; (c) **prezzi di vendita**.
▶ *Best practice*: **Coinvolgimento dei *social network* nelle indagini per raccogliere informazioni aggiuntive sugli account *social***
▶ Indagine di riferimento: **Bologna Luxury**
La Guardia di Finanza ha avviato una serrata interlocuzione con i *social network* coinvolti nell'indagine (Facebook e Instagram) per acquisire informazioni aggiuntive sugli account al fine di circoscriverne il raggio d'azione e permettere l'identificazione dei responsabili. In questo caso, è risultata fondamentale la condivisione da parte dei *social network* di: (a) **file di *log***; (b) **numeri di cellulare**; (c) **metodi di pagamento**.
▶ *Best practice*: **Coinvolgimento dei servizi di pagamento per ricostruire le movimentazioni economiche dei contraffattori**
▶ Indagine di riferimento: **Bologna Luxury**
La Guardia di Finanza, tramite l'utilizzo di appositi *software*, è riuscita ad individuare il nome utente del conto PayPal memorizzato nei *cookie* del *browser* del cellulare sequestrato all'indagata. Questo ha permesso l'inoltro di una richiesta a PayPal (tramite il Safety Hub – PayPal Law Enforcement Tool) per la condivisione dei dati sulle transazioni effettuate dall'account. I dati pervenuti hanno permesso l'individuazione dei pagamenti nei confronti dei fornitori cinesi, confermando di fatto quanto già emerso dall'analisi delle conversazioni su Whatsapp. In questo caso, è risultata fondamentale la condivisione da parte del servizio di pagamento dei **dati sulle transazioni** effettuate dall'account.

Box 23. Collaborazione tra forze dell'ordine e *stakeholder* privati

A fine 2020 Amazon ha fornito all'ente dogale degli Stati Uniti (CBP) e al Dipartimento di Sicurezza Interna (HSI) una serie di informazioni che hanno contribuito a bloccare una partita di prodotti contraffatti prima che passasse attraverso un fornitore logistico. Le informazioni fornite da Amazon, rafforzate dalle successive indagini svolte da CBP e HSI, hanno permesso alle forze dell'ordine di sequestrare i carichi di ben otto camion, composti da radiatori contraffatti di automobili con i marchi di diverse case automobilistiche. È da sottolineare come la collaborazione funzioni anche in senso opposto. Sempre nel 2020 la stessa CBP ha informato Amazon di un sequestro di una spedizione di custodie per auricolari con i loghi non autorizzati della Champion. Amazon ha provveduto a sequestrare gli articoli di quei contraffattori che erano presenti nella loro rete di distribuzione e ne hanno chiuso gli account. La *Counterfeit Crimes Unit* (CCU) di Amazon ha poi lavorato insieme alla società che detiene i relativi diritti di proprietà intellettuale sul marchio, la HanesBrands, per fare causa a 13 contraffattori.

Nel 2012, in Canada è stato lanciato 'Project Chargeback-Leading the Charge(Back) againt fakes!', un progetto che vede la collaborazione tra il *Canadian Anti-fraud Centre* (CAFC) (gestito dalla *Royal Canadian Mounted Police*), banche, servizi di pagamento e titolari di diritti di proprietà intellettuale. Il progetto mira a contrastare la vendita di prodotti contraffatti tramite i seguenti step (WIPO 2017):

- il cliente che scopre di aver acquistato un prodotto contraffatto effettua una segnalazione al CAFC, fornendo informazioni in merito, ad esempio, al marchio del prodotto acquistato, al prezzo pagato, al nome del venditore e al canale online dove è stato effettuato l'acquisto;

- il CAFC contatta il titolare dei diritti di proprietà intellettuale per verificare l'originalità o meno del prodotto segnalato;

- se il prodotto risulta non originale, la banca del cliente provvede ad effettuare il chargeback;

- al cliente viene chiesto di non resistuire il prodotto al venditore ma di distruggerlo una volta ricevuto il rimborso;

- l'account del venditore viene chiuso dal servizio di pagamento che addebita anche la tariffa del chargeback;

- sia la banca che il servizio di pagamento possono essere multati in caso di un numero eccessivo di chargeback, con il servizio di pagamento che può anche perdere l'accesso ai circuiti di pagamento.

Dall'avvio del progetto, il CAFC ha gestito oltre 35.000 richieste che hanno portato a rimborsi per 10 milioni di dollari e alla chiusura degli account di 8.000 venditori che vendevano prodotti contraffatti su 25.000 siti web.

Oltre alla collaborazione nelle attività operative, è da segnalare anche quella nelle attività volte a sensibilizzare cittadini ed imprese sui rischi della contraffazione online. Per un elenco esaustivo di queste si rimanda al 'Piano Strategico Nazionale 2019-2020' (Consiglio Nazionale Anticontraffazione 2019). Risulta di particolare interesse segnalare la Settimana Anticontraffazione organizzata dalla DGTPI-UIBM del Ministero dello Sviluppo Economico.

Box 24. Attività di sensibilizzazione: la settimana anticontraffazione

La Settimana Anticontraffazione è una campagna di comunicazione realizzata dalla DGTPI-UIBM del Ministero dello Sviluppo Economico a partire dal 2016, generalmente nel mese di ottobre. Si pone l'obiettivo di generare una riflessione sull'entità e sugli effetti ed implicazioni della contraffazione ed indirizzare i consumatori, in particolare giovani, verso abitudini di acquisto maggiormente consapevoli e responsabili. Durante la Settimana Anticontraffazione vengono organizzati eventi di informazione su tutto il territorio nazionale, con focus territoriali in particolari città per presentare i risultati degli studi locali realizzati dalla Direzione in collaborazione con CENSIS sull'impatto e sulla diffusione del fenomeno nelle province esaminate. Le iniziative, che coinvolgono diversi partner istituzionali e *stakeholder* del settore privato, si focalizzano su diversi temi, tra i quali i reati connessi alle violazioni dei diritti di proprietà industriale, la presenza della criminalità organizzata ed il riciclaggio di denaro nello specifico settore, la contraffazione nella moda ed il contrasto al mercato del falso a livello territoriale.

Collaborazione tra *stakeholder* pubblici

Come illustrato nella sezione 4.1, la compartimentazione di autorità pubbliche e forze dell'ordine non permette una **risposta integrata e un'azione coordinata** contro le nuove forme di contraffazione online. A questo riguardo, è importante menzionare il recente insediamento, a fine ottobre 2021, del **Consiglio Nazionale per la Lotta alla Contraffazione e all'Italian Sounding (CNALCIS)**, già Consiglio Nazionale Anticontraffazione (CNAC). Questo organismo interministeriale si occupa di:

a. individuare le linee strategiche e le relative attività di contrasto alla contraffazione e all'Italian Sounding;

b. elaborare proposte d'intervento congiunte.

Il CNALCIS si avvale anche del contributo della '**Commissione Consultiva Permanente FF.OO**' composta da rappresentanti delle forze dell'ordine impegnate nelle attività di *enforcement* e della '**Commissione Consultiva permanente delle forze produttive**' composta da rappresentanti di associazioni di categoria e consumatori. Questa struttura ha l'obiettivo di rendere operative le strategie delineate dal CNALCIS garantendo, al tempo stesso, la rappresentazione e la tutela degli interessi privati e pubblici. Tuttavia, sarebbe desiderabile la definizione di metriche chiare e di KPIs per monitorare gli *output* e gli *outcome* di queste attività nel tempo. Ad esempio, potrebbe essere utile monitorare il numero di attività operative supportate per ciascuna degli ambiti prioritari della contraffazione definiti dal CNALCIS stesso, permettendo quindi di individuare tempestivamente potenziali criticità da affrontare.

Per quanto riguarda la collaborazione tra forze dell'ordine, di particolare rilievo è il '**Desk Interforze Anticontraffazione**' che si riunisce periodicamente presso il **Servizio Analisi Criminale della Direzione Centrale della Polizia Criminale**. Questo Desk ha il compito di sviluppare sinergie operative e strategiche

nel settore del contrasto alla contraffazione ed elaborare atti di indirizzo condivisi, al quale partecipano rappresentanti dei Comandi Generali dell'Arma dei Carabinieri e della Guardia di Finanza, della Direzione Centrale Anticrimine della Polizia di Stato, dell'A.N.C.I. - Associazione Nazionale Comuni Italiani, per il raccordo con le Polizie locali, e della S.I.A.E. - Società Italiana degli Autori ed Editori, per gli aspetti inerenti la pirateria multimediale.

Box 25. Contrasto alla contraffazione tra online e offline

Paragrafo a cura del Servizio Analisi Criminale della Direzione Centrale della Polizia Criminale – Dipartimento della Pubblica Sicurezza – Ministero dell'Interno

Con specifiche direttive datate, rispettivamente, 8 agosto 2014, 15 novembre 2014, 6 luglio 2015 - con le allegate "Linee guida in materia di prevenzione e contrasto al fenomeno della contraffazione" - e 6 luglio 2018, il Ministro dell'Interno ha disposto una sistematica intensificazione dell'azione di prevenzione e contrasto alla contraffazione e all'abusivismo commerciale, al fine di difendere la libera e corretta concorrenza, tutelare l'economia legale e salvaguardare la salute dei consumatori.

Speciale attenzione, è stata rivolta, con la prima, alle località turistiche e, in particolare, balneari, in cui si registra un sensibile aumento della presenza di soggetti dediti a tali condotte.

La direttiva è stata poi estesa all'intero territorio nazionale nel successivo mese di novembre, divenendo modello permanente di impulso.

Il 6 luglio 2015, il Ministro dell'Interno è nuovamente intervenuto nella materia, allo scopo di sensibilizzare i Prefetti a implementare, in sede di Comitato Provinciale per l'Ordine e la Sicurezza Pubblica, le iniziative di contenimento e repressione dei fenomeni illeciti in esame, ponendo in rilievo la necessità di individuare e disarticolare l'intera filiera del falso, dalle centrali criminali a vario titolo coinvolte nella produzione, importazione, distribuzione e commercializzazione della merce illecita fino ai terminali di questa pervasiva attività illegale.

Nell'occasione è stata richiamata l'importanza di un'azione congiunta fra tutte le istituzioni coinvolte, attraverso la quale poter perseguire le rilevanti finalità di interesse pubblico sopra menzionate.

L'ultima direttiva, in data 6 luglio 2018, infine, ha confermato i precedenti indirizzi e ribadito la necessità di dare un forte e rinnovato vigore all'azione di prevenzione e contrasto della contraffazione e dell'abusivismo commerciale - specie nelle località balneari e in quelle a forte vocazione turistica, artistica e culturale o che siano sede di svolgimento di manifestazioni di particolare rilievo - mediante il rafforzamento delle misure già indicate ed il ricorso ai nuovi strumenti messi a disposizione dalle recenti previsioni normative in materia.

In particolare, alle Autorità prefettizie è stata segnalata l'opportunità che si assicuri, tra l'altro:

- la massima valorizzazione del ruolo delle Polizie locali, in ragione delle loro specifiche competenze in materia di disciplina del commercio e della capillare conoscenza del territorio;
- la verifica dell'eventuale disponibilità, da parte delle Associazioni di categoria dei settori produttivi più danneggiati dal fenomeno, a contribuire finanziariamente ai programmi in materia di sicurezza locale nelle forme consentite dalle norme vigenti;

- l'esecuzione di piani d'intervento operativi che includano, in relazione alle situazioni più complesse, l'attivazione di mirati servizi interforze;
- l'intensificazione dell'attività di controllo sulla presenza di immigrati irregolari;
- l'individuazione, da parte dei Comuni, delle zone nelle quali sia possibile applicare il divieto di accesso (il "D.A.SPO. urbano" o "D.A.C.UR.") previsto dalla normativa in materia di sicurezza urbana;
- l'adeguamento dei protocolli d'intesa, stipulati con tutti i soggetti pubblici e privati interessati alla lotta a queste forme di illegalità, ai modelli che hanno consentito di conseguire i migliori risultati in termini di ridimensionamento del fenomeno e aumento della percezione della sicurezza.

I positivi risultati riscontrati, in attuazione delle suddette linee d'intervento, hanno poi suggerito di destinare[24] una quota del 18% del Fondo per la Sicurezza Urbana ai Comuni litoranei, per il sostegno di progetti, proposti dai Comuni maggiormente esposti agli effetti negativi dei fenomeni illeciti in parola, finalizzati al rafforzamento dell'ordinaria attività di contrasto nel biennio 2019-2020.

24. Con il decreto del Ministro dell'Interno, adottato di concerto con il Ministro dell'Economia e delle Finanze in data 18 dicembre 2018, recante i criteri di ripartizione del Fondo per la sicurezza urbana istituito dall'art. 35-quater del decreto-legge 4 ottobre 2018 n.113, conv. con modificazioni dalla legge 1° dicembre 2018 n. 132.

5.

Raccomandazioni e direzioni future

Le minacce emergenti, i nuovi schemi adottati dai contraffattori, le sfide e le vulnerabilità nei sistemi anticontraffazione richiedono, nonostante le diverse buone pratiche già in atto, un **cambio di paradigma**, e un nuovo approccio in termini di **sensibilizzazione, prevenzione, investigazione e contrasto**. In particolare, emergono tre direzioni future di intervento:

- rafforzare il monitoraggio delle minacce emergenti di contraffazione sui mercati online;
- potenziare le capacità tecnologiche e analitiche degli *stakeholder* pubblici e privati per il tracciamento dei prodotti e la verifica dei venditori;
- espandere la cooperazione e la condivisione di informazioni tra gli *stakeholder* pubblici e privati.

All'interno di queste tre direzioni è possibile individuare proposte specifiche, che sono discusse di seguito.

5.1 Rafforzare il monitoraggio sulle minacce emergenti

Tutti gli attori – pubblici e privati - coinvolti e intervistati nel corso del progetto hanno evidenziato la necessità di disporre di un **sistema più strutturato per monitorare e rimanere aggiornati** sui nuovi schemi della contraffazione online. Come illustrato nel capitolo 3, è in corso una rapida evoluzione delle minacce – in termini di attori e di reati – e solo pochi *stakeholder* hanno una visione completa di questo *fraudster journey*. Questo impatta negativamente sulla capacità degli stakeholder di individuare in maniera tempestiva 'falsi' e attività fraudolente e implementare soluzioni efficaci (a livello procedurale e tecnologico).

Un osservatorio sulle nuove minacce e *modi operandi* della contraffazione online

Questo report è la prima fotografia, almeno a livello italiano, di come si manifesta la contraffazione sui *mercati* online. Per seguirne l'evoluzione, così come suggerito da numerosi intervistati, si potrebbe istituire un **osservatorio scientifico continuo** che possa raccogliere e sistematizzare la conoscenza sull'argomento e metterla a disposizione degli attori (pubblici e privati) in maniera agevole e strutturata consentirebbe di tenere alta la vigilanza, di seguire le minacce in tutta la loro evoluzione, e di monitorare l'efficacia delle soluzioni implementate.

L'osservatorio potrebbe creare, gestire e aggiornare periodicamente una **banca dati online**, accessibile sia da autorità pubbliche e forze dell'ordine, che da attori privati (es. *marketplace*, *social media*, operatori di logistica, *brand owner*) e contenente una **rassegna di schemi e casistiche** (anonimizzate o comunque gestite in *compliance* con la normativa privacy) di contraffazione online e di altri comportamenti fraudolenti nell'*e-commerce*. I casi sarebbero raccolti a livello globale da diverse fonti (documenti giudiziari, report di polizia e istituzionali, letteratura scientifica, fonti aperte), analizzati e classificati con metodo scientifico così da essere cercabili per *tag* e altre chiavi di lettura. La banca data fornirebbero una panoramica sempre aggiornata della contraffazione online, contribuendo a costruire una base conoscitiva trasversale a tutti gli *stakeholder* coinvolti. In particolare, le informazioni contenute all'interno della banca dati potrebbero essere utilizzate per:

• formare il personale preposto al contrasto della contraffazione online;

• aggiornare i modelli di *risk assessment* e *detection* automatici sulla base di evidenze empiriche;

• fornire una conoscenza approfondita.

L'osservatorio, e la banca dati di casi, potrebbero ispirarsi a quanto già realizzato in **ambito antiriciclaggio** a livello nazionale ed internazionale, e che non solo ha aumentato la conoscenza (e la sensibilizzazione) collettiva sul problema, ma è diventata la base per ciascuna soluzione (tecnologica e procedurale) implementata da banche e altri soggetti obbligati.

Box 26. L'utilità del monitoraggio delle misure nell'antiriciclaggio

Da tempo esistono, in ambito antiriciclaggio e di contrasto al finanziamento del terrorismo, delle iniziative coordinate dalle autorità di vigilanza, finalizzate al monitoraggio delle minacce e degli schemi di attività anomala per aumentare la conoscenza e la sensibilizzazione dei soggetti obbligati (banche, professionisti, altri intermediari) sul fenomeno:

- in Italia, UIF – Unità di Informazione Finanziaria, pubblica periodicamente dei report che mettono in luce **modelli e schemi di comportamenti anomali** a livello AML/CFT collegati a settori/tipologie diverse. Ad esempio, si segnalano i report più recenti su modelli e schemi di comportamento legati ad operatività anomala connessa con illeciti fiscali, con carte di pagamento, nel settore dei giochi e delle scommesse e nell'attività di *factoring/leasing*;
- a livello internazionale il **FATF - Financial Action Task Force** elabora e pubblica periodicamente dei **report su "*Methods and trends*"** emergenti collegati al riciclaggio di denaro e al finanziamento del terrorismo. Nel corso degli ultimi anni il FATF ha pubblicato più di 75 report che includono casi (anonimizzati) raccolti da fonti diverse.

Gli schemi e le casistiche di UIF e FATF sono poi utilizzati, tra gli altri, da banche, professionisti e altri soggetti obbligati per **aggiornare i loro modelli di *early-detection*** e di valutazione del rischio (UIF 2021). A questi, si aggiungono poi gli esercizi di valutazione del rischio riciclaggio condotti a livello nazionale dal Comitato di Sicurezza Finanziaria del Ministero dell'Economia e delle Finanze (MEF 2018) e a livello sovranazionale dalla Commissione Europea (2018b).

Secondo una recente survey condotta da Crime&tech con il supporto di SAS su soggetti obbligati pari a circa il 50% del mercato finanziario italiano, di fatto **tutti gli intermediari intervistati utilizzano schemi e casi di UIF e FATF** e gli esiti dei *risk assessment* a livello nazionale ed internazionale come base di partenza delle loro soluzioni interne antiriciclaggio, sia a livello tecnologico che procedurale (Crime&tech 2021).

5.2 Potenziare capacità tecnologiche e analitiche

Nuovi strumenti di analisi, verifica, controllo ed *early-detection*

Marketplace, *social media* e operatori di logistica dispongono di un **volume enorme di informazioni** che, grazie ai nuovi strumenti dell'intelligenza artificiale, del *big data analytics*, e delle nuove tecnologie, e nel pieno rispetto di dati personali e sensibili, potrebbe essere utilizzato per portare le capacità di rilevamento di 'falsi' e comportamenti fraudolenti ad un altro livello. Al momento - a parte qualche eccezione, illustrata nel capitolo precedente – il potenziale di queste informazioni è **sfruttato solo in minima parte**, e solo da alcuni attori e operatori.

Dalle interviste con le autorità pubbliche e altri soggetti privati (es. *brand owner*), infatti, sono emerse **differenze rilevanti** tra i diversi *marketplace* e canali di vendita. Se infatti i *marketplace* più grandi risultano dotati di strumenti più evoluti, dalle interviste emerge che i *social network* sono invece più deboli e meno in grado di rilevare in maniera tempestiva comportamenti e prodotti fraudolenti. Allo stesso modo, anche i *marketplace* più piccoli affrontano una situazione simile, sebbene dovuta a motivazioni diverse. Se per le piattaforme di *e-commerce* più piccole questo è principalmente dovuto alla mancanza di risorse (umane ed economiche) da dedicare al contrasto del fenomeno, per i *social* questa vulnerabilità sembra dovuta principalmente alla difficoltà nel riconoscerla come priorità. Ad esempio, mancano i controlli di *seller vetting* all'apertura di account da parte di società *for-profit*, e le verifiche su quanto creato con le campagne di sponsorizzazione. Queste differenze generano effetti di *displacement* delle attività criminali verso i canali più vulnerabili, indebolendo l'intero sistema dell'*e-commerce* e creando anche problemi di concorrenza sleale.

Così come suggerito dalle buone pratiche illustrate nella sezione 4.1, le capacità tecnologiche e analitiche dei soggetti attivi nel settore possono essere potenziate in tre direzioni:

1. Nel controllo dell'origine dei prodotti,

ad esempio tramite:

a. l'impiego di soluzioni di tracciamento di tipo elettronico, materiale, chimico come RFID, NFC e altri sistemi di serializzazione (vedi 4.1.1);

b. l'impiego di soluzioni di *blockchain* e di DLT, che coinvolgano anche l'intera filiera (fino al consumatore finale);

c. la promozione di un utilizzo condiviso di queste soluzioni tra attori diversi (es. diversi *brand owner*, o tra questi e i *marketplace*), laddove possibile;

d. l'estensione di queste soluzioni anche alle imprese medio-piccole che non dispongono di risorse per l'innovazione, ad esempio tramite incentivi o iniziative 'a ombrello' delle associazioni di categoria;

e. l'impiego di nuove tecnologie di scansione (es. sistemi di scansione in 3D, scanner a neutroni), utili per individuare anomalie nei beni in tutta la catena logistica (es. nel caso di resi fraudolenti con prodotti contraffatti).

2. Monitoraggio di inserzioni e di altra attività sul web

ad esempio tramite un utilizzo più intensivo di:

a. sistemi basati su intelligenza artificiale e *machine learning*;
b. il *text-mining* dei messaggi postati su *marketplace*, *social media* e altri forum per riconoscere inserzioni anomale;
c. l'*image recognition* delle fotografie dei prodotti sul web;
d. la condivisione da parte dei titolari di diritti di proprietà intellettuale di scansioni 2D e 3D più accurate dei loro prodotti così da facilitare l'*image recognition*;
e. lo *screening* su larga scala dei siti web per individuare siti clone e malevoli.

3. Verifica dei venditori e *seller vetting*

ad esempio tramite:

a. l'uso di procedure, durante la fase di *on-boarding* da remoto, utili per essere certi di trovarsi di fronte a società reali e non a 'scatole vuote' usate a fini illeciti (es. verifica della veridicità di indirizzo e casella postale);
b. l'ampliamento del patrimonio informativo sui venditori o i soggetti ad esso collegati, ad esempio tramite l'impiego di banche dati di informazioni societarie e 'liste compliance';[25]
c. l'utilizzo di indicatori e modelli di rischio evoluti, capaci di individuare anomalie nelle caratteristiche dei soggetti (a livello anagrafico, nella struttura proprietaria, contabile e finanziaria) da un confronto con gruppi di pari;
d. il monitoraggio continuo dell'operatività del soggetto, e identificazione di eventuali attività anomale (es. variazioni inusuali o ingiustificate dei prodotti inserzionati, dei contatti, della sede legale);
e. il monitoraggio delle recensioni applicate a certi venditori per verificare eventuali anomalie che possano suggerire comportamenti fraudolenti (es. uso dello stesso testo per lo stesso venditore su piattaforme diverse da parte di account diversi)
f. l'economia di scala con ambiti limitrofi (es. antiriciclaggio, anticorruzione) per prendere spunto dalle buone pratiche implementate dagli intermediari in ambito KYC e adeguata verifica.

25. Queste sono banche dati, molto impiegate in ambito antiriciclaggio, che, a partire da fonti pubbliche (es. liste sanzioni, comunicati stampa di polizie, fonti aperte certificate) forniscono i nominativi di soggetti colpiti da precedenti sanzioni (es. OFAC, UN, EU), da attività di *enforcement* (es. misure personali o patrimoniali, misure amministrative) e inclusi in categorie sottoposte, almeno in ambito antiriciclaggio, a verifica rafforzata (es. PEP – persone politicamente esposte).

Per investire nello sviluppo di questi strumenti, e nell'allargamento a tutti gli attori del sistema *e-commerce*, si potrebbe fare leva sulle risorse messe a disposizione dal **Piano Nazionale di Ripresa e Resilienza (PNRR)**. Ad esempio, il PNRR potrà finanziare la costituzione di *Partenariati estesi* (PE) che coinvolgano università e imprese su alcuni temi specifici individuati dal MIUR, tra i quali sono indicati ***'Intelligenza Artificiale'*** e ***'Made in Italy'***. Nell'ambito di questi due temi potrebbe essere possibile instaurare delle collaborazioni tra università ed imprese così da sviluppare e testare nuovi strumenti e approcci analitici avanzati per migliorare la tracciabilità dei prodotti e potenziare l'*early detection* della 'filiera del falso' – online e offline.

Formazione di soggetti pubblici e privati sui *data analytics*

L'applicazione su ampia scala di queste capacità analitiche e tecnologiche non passa solo da investimenti materiali ma innanzitutto dalla **formazione dei soggetti, pubblici e privati**. Diversi soggetti intervistati hanno sottolineato la necessità di *training* dedicati e corsi di formazione, organizzati con il supporto di strutture accademiche ed associazioni di categoria, che possano, tra gli altri:

- **illustrare gli strumenti disponibili** per il *data analytics* (*machine learning*, reti neurali, text and *image recognition*), e le potenzialità da esse offerte;
- passare in rassegna la varietà di **informazioni e fonti dati potenzialmente utilizzabili** per scopi di analisi e di indagine predittiva;
- illustrare e discutere i vincoli, a livello legale e tecnologico, per l'utilizzo e l'elaborazione di questi dati, innanzitutto quelli in termini di **protezione dei dati personali** e **profilazione automatica**.

Box 27. Intelligenza artificiale, anticontraffazione e protezione dei dati personali

Le soluzioni tecnologiche avanzate hanno enormi potenzialità in ambito anticontraffazione, ma la loro adozione deve sempre tenere in considerazione gli adempimenti previsti dalla normativa in materia di protezione dei dati personali. In particolare, gli algoritmi di intelligenza artificiale devono rispettare specifici requisiti (es. conformità dei criteri usati per l'addestramento, riproducibilità e verificabilità dei risultati).

Questi principi assicurano che gli algoritmi di intelligenza artificiale non siano alla base di decisioni basate unicamente su un trattamento automatizzato, vietato tranne nei casi espressamente previsti dal diritto dell'Unione o del singolo Stato membro interessato. Se, da una parte, questi adempimenti rappresentano sicuramente un vincolo importante da tenere in considerazione, dall'altra, non devono più essere considerati ostacoli insormontabili all'adozione di soluzioni tecnologiche avanzate.

È possibile adottare misure tecniche ed organizzative che garantiscano il rispetto della normativa in materia di privacy e, allo stesso tempo, un utilizzo efficace delle soluzioni avanzate. Da un lato, si può ricorrere alla pseudonimizzazione dei dati personali trattati dai modelli di analisi evoluta; dall'altro, è la stessa intelligenza artificiale a offrire delle nuove opportunità per gestire questi dati in maniera corretta – ad esempio utilizzando soluzioni di *federated learning*.

La possibilità di combinare il rispetto dei dati personali con un impiego efficace di big data e intelligenza artificiale è stata ulteriormente sottolineata dalle pubblicazioni di diversi organi dell'Unione Europea su questa tematica. Tra queste:

- le Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679 (Commissione Europea 2018a);
- la Risoluzione del Parlamento sulle implicazioni dei Big Data per i diritti fondamentali (Parlamento Europeo 2017);
- le Linee guida in materia di intelligenza artificiale e protezione dei dati personali relative alla Convenzione 108 (Consiglio d'Europa 2019);
- il Libro Bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia (Commissione Europea 2019).

5.3 Espandere cooperazione e scambio informativo

Un nuovo gruppo di lavoro multidisciplinare a livello nazionale

L'istituzione, a fine ottobre 2021, del **CNALCIS** rappresenta sicuramente un passo avanti nel coordinamento della lotta alla contraffazione. Tuttavia, la crescente interconnessione dei comportamenti fraudolenti (vendita di 'falsi', frodi nei pagamenti, reati *cyber*) richiede l'istituzione di un **gruppo di lavoro stabile e multidisciplinare** (una 'alleanza') che abbia un taglio prevalentemente operativo e possa includere rappresentanti di tutti gli *stakeholder* e tutte le eccellenze coinvolte nella prevenzione e nel contrasto alla contraffazione online:

- **autorità pubbliche** (forze dell'ordine, agenzie di supervisione e protezione della filiera legale, autorità giudiziarie) coinvolte nella prevenzione e contrasto alla vendita di 'falsi' online;

- **soggetti privati**, ed in particolare:
  a. *marketplace;*
  b. *social media*;
  c. titolari di diritti di proprietà intellettuale;
  d. operatori di servizi postali e di logistica;

- **centri di ricerca** scientifica ed enti universitari;

- rappresentanti di fornitori **di soluzioni tecnologiche e di *data analytics***.

Considerata la connessione sempre più stretta tra contraffazione online e reati finanziari (es. frodi ai servizi di pagamento) e *cyber* (es. furto di identità, *phishing*, *malware*), è opportuno che il gruppo di lavoro includa anche rappresentanti di:

- autorità pubbliche attive nell'**indagine e contrasto dei reati *cyber*** (es. Polizia Postale);
- autorità di *intelligence* in **ambito finanziario** (es. Banca d'Italia – UIF; Guardia di Finanza).

Il gruppo di lavoro, che potrebbe beneficiare anche dell'esperienza positiva di iniziative simili lanciate a livello internazionale (es. Memorandum of Understanding sulla vendita di prodotti contraffatti su internet) nascerebbe con lo scopo di:

- condividere dati e informazioni su **nuovi schemi e *modi operandi*** della contraffazione online, collegandosi anche all'osservatorio già discusso al punto 5.6;
- discutere e progettare nuovi **meccanismi e strumenti per lo scambio d'informazioni** che, da una parte, permettano flussi informativi efficienti ed automatizzati e, dall'altra, assicurino il rispetto di tutti gli interessi coinvolti (es. protezione dati personali, tutela di informazioni sensibili a livello industriale e commerciale);
- incentivare gli attori del settore privato a **collaborare in maniera più stretta** con forze dell'ordine e autorità pubbliche, e queste ultime a condividere più informazioni ed esiti dei procedimenti di indagine con il settore privato;
- costituire **gruppi di *joint-investigation*** su temi, casi, soggetti e settori specifici (es. filiera agro-alimentare, made in Italy, filiera del lusso, filiera meccanica).

Box 28. Collaborazione di *marketplace* e forza dell'ordine con i fornitori di servizi di pagamento

A febbraio 2021 Amazon ha lanciato il Programma per i fornitori di servizi di pagamento (*Payment Service Provider Programme*) per migliorare ulteriormente la prevenzione, l'individuazione ed il contrasto ai comportamenti illeciti. I seller che decidono di usare un fornitore di servizi di pagamento per ricevere i propri pagamenti sulla piattaforma, devono necessariamente sceglierne uno che partecipi al programma e soddisfi quindi i requisiti previsti in termini di sicurezza e compliance alle normative. Questa prassi, riconosciuta come *best practice* anche in un recente *working paper* dell'EUIPO (2021e), permette di identificare i conti dei venditori, dove sono diretti i pagamenti e chi ne è il reale destinatario, limitando anche l'utilizzo di conti correnti considerati più rischiosi come quelli aperti presso banche virtuali. Amazon condivide poi con i fornitori di servizi di pagamento iscritti al programma le informazioni comunicate dal venditore, al fine di verificarne l'attendibilità. Nel caso di informazioni fraudolente e/o attività illecite individuate successivamente, l'account del venditore viene disattivato e i fondi trattenuti per pagare le transazioni ancora da saldare, inclusi resi e rimborsi.

Nuovi meccanismi di scambio e condivisione delle informazioni

Come anticipato nella sezione 4.1, l'assenza di meccanismi di scambio informativo sicuri e accettati tra tutte le parti rappresenta una delle maggiori sfide ad una collaborazione efficace degli *stakeholder* per contrastare la vendita di 'falsi' sui mercati online. La natura sempre più **ibrida e poli-criminale** degli attori attivi nella vendita di falsi online, spesso presenti contestualmente su più canali (***cross-channel***), richiede invece un approccio investigativo e di contrasto ad ampio spettro, capace di spaziare dalla contraffazione, alle frodi ai pagamenti, ai reati *cyber*. Come segnalato da diversi soggetti intervistati in ambito privato, l'eccessiva **compartimentazione delle autorità pubbliche** rende difficile un contrasto 'totale' ed integrato al fenomeno nelle modalità con cui si presenta oggi. Sebbene esistano infatti unità specializzate, e di eccellenza, all'interno delle forze dell'ordine, non sempre è facile la collaborazione tra queste, e il dialogo con il settore privato.

Le difficoltà sono ancora più grandi quando gli schemi di contraffazione messi in atto dai gruppi criminali hanno una **natura transnazionale**. L'individuazione di chi si nasconde dietro la vendita di prodotti contraffatti online non sempre permette di risalire alla filiera fisica di produzione e stoccaggio della merce, spesso localizzata in altri paesi e gestita da altri soggetti. E spesso anche i **server che ospitano siti** – clone o comunque fraudolenti – utilizzati per vendere 'falsi' sono localizzati in paesi esteri, magari *off-shore* o comunque extra-europei. La difficile individuazione del principio di territorialità nei casi di commissione di reati *cyber*, e comunque le difficoltà che si incontrano nella cooperazione internazionale e nello scambio informativo con alcune giurisdizioni (o con alcuni soggetti privati esteri), ostacolano l'attività di contrasto su scala transnazionale.

Facendo leva su iniziative lanciate dai ***marketplace* online in altri paesi** (vedi box 22), **servizi di pagamento** (vedi box 28) ma anche *stakeholder* in **altri settori**, come l'antiriciclaggio (vedi Box 29), è possibile esplorare nuovi meccanismi e canali di scambio informativo che, basandosi su tecnologie evolute (es. *federated learning*), consentirebbero di scambiare informazioni tra attori pubblici e privati, e tra gli stessi attori privati, anche quando concorrenti, su:

- account coinvolti nei comportamenti illeciti;

- metodi di pagamento associati;

- modalità di vendita e *modi operandi*;

- indirizzi IP.

In questa direzione si muove anche l'"European Commission IP Action Plan' della Commissione Europea che, tra gli elementi fondamentali del futuro 'EU Toolbox against counterfeting', include proprio "la condivisione dei dati pertinenti sui prodotti e sugli operatori commerciali, nel rispetto della normativa in materia di protezione dei dati" (Commissione Europea 2020, 18). I casi analizzati e le interviste hanno dimostrato che i contraffattori, se individuati e bloccati su un determinato *marketplace*, si muovono su altri per la vendita dei propri prodotti illegali. La costituzione di nuovi meccanismi di scambio con i quali condividere informazioni in tempo reale con gli altri *stakeholder* permetterebbe di **ridurre questo effetto di 'displacement'**, contribuendo ad arginare efficacemente i trasgressori recidivi e rendere **l'intero sistema di *e-commerce* più sicuro**. In particolare, la condivisione di queste informazioni beneficerebbe in particolare gli *stakeholder* di piccole dimensioni che non hanno le stesse risorse (umane ed economiche) da dedicare alla lotta alla contraffazione.

In tal senso, sono particolarmente rilevanti le *blacklist* sviluppate da alcuni *newtork* di carte di credito (***i Terminated Merchant Files***) che includono tutti i venditori (e i relativi account) che sono stati sospesi dai sistemi di pagamento per, ad esempio, un alto numero di *chargeback*, riciclaggio di denaro e violazioni di diritti di proprietà intellettuale. Queste liste, aggiornate in tempo reale (come il 'Mastercard Alert to Control High-risk Merchants'), vengono consultate da tutti i servizi di pagamento che devono effettuare l'*on-boarding* di un nuovo esercente. Riconosciuta come *best practice* dall'EUIPO (2021e) per affrontare il fenomeno dei tragressori recidivi, gli esperti dell'*Expert Group on Cooperation with Intermediaries* dell'Osservatorio dell'EUIPO **auspicano la condivisione di queste informazioni anche con i *marketplace***, al fine di aumentare il patrimonio informativo che quest'ultimi possono utilizzare nelle loro attività di contrasto alla contraffazione, con un particolare riguardo al *seller vetting*.

Box 29. Condivisione di informazioni tra soggetti privati diversi: il caso dell'antiriciclaggio

La *Monetary Authority of Singapore* (MAS) ha recentemente annunciato l'introduzione, nel 2023, di una piattaforma digitale centralizzata che permetterà ai soggetti obbligati di condividere, in tempo reale, informazioni su clienti e transazioni, al fine di contrastare in modo più efficace il riciclaggio di denaro e il finanziamento del terrorismo (Monetary Authority of Singapore 2021). La nuova piattaforma, denominata COSMIC (*Collaborative Sharing of ML/TF Information & Cases*), sarà inizialmente utilizzata dalle sei principali banche di Singapore (DBS, OCBC, UOB, SCB, Citybank e HSBC), permettendo di individuare più facilmente schemi complessi di transazioni che uno stesso soggetto può compiere tramite conti in istituzioni finanziarie diverse.

Allo stesso modo, nei Paesi Bassi, le cinque principali banche del paese (ING Bank, ABN Amro, Rabobank, Triodos Bank e de Volksbank) si sono fatte promotrici del *Transaction Monitoring Netherlands* (TMNL), un sistema centralizzato di monitoraggio continuo delle transazioni finanziariarie (Transaction Monitoring Netherlands 2021). TMNL incrocia i dati forniti dalle cinque banche al fine di individuare *pattern* e *red-flag* che possano indicare possibili transazioni sospette.

Conclusioni

Il presente *report* rappresenta la prima analisi sistematica in Italia dei trend e *modi operandi* della contraffazione online e delle contromisure adottate da autorità pubbliche e aziende private per contrastarla. La contraffazione online è spesso percepita come una minaccia crescente a livello mondiale, visto l'interesse dei criminali per le nuove opportunità offerte da internet. Tuttavia, nonostante sia un facilitatore rilevante, la dimensione online è ancora minima rispetto ai canali fisici per quanto riguarda la vendita di prodotti contraffatti. Inoltre, alcuni intermediari, come i *marketplace*, sono in prima linea nella lotta contro i contraffattori, destinando sempre maggiori risorse allo sviluppo di tecnologie all'avanguardia e contromisure aggiornate. I principali risultati del report e le raccomandazioni di *policy* discusse nelle sezioni precedenti possono essere raggruppate in tre macro-aree d'intervento che devono essere affrontate in futuro:

- **attività operative**: rimuovere le barriere nel sistema italiano che non riflettono l'attuale scenario della contraffazione e rendono quindi difficile perseguire legalmente i contraffattori;

- **condivisione di dati**: condividere informazioni aggiornate e di qualità sulle attività legate alla contraffazione è essenziale per smantellare le reti criminali che gestiscono questo mercato. Per incentivare questo scambio, l'Italia potrebbe partecipare attivamente alla definizione dell'*EU Toolbox* che stabilirà l'approccio coordinato dell'Unione Europea in materia di contraffazione. Il *Toolbox* dovrebbe chiarire i ruoli e le responsabilità di tutti gli attori coinvolti nella lotta alla contraffazione, individuando inoltre le modalità per migliorare la condivisione delle informazioni e la cooperazione tra i titolari di diritti di proprietà intellettuale, gli intermediari (online ed offline) e le forze dell'ordine. L'istituzione di un gruppo di lavoro a livello nazionale sul tema permetterebbe inoltre di rafforzare la posizione dell'Italia sul tema a livello internazionale;

- **prevenzione**: definire standard condivisi per prevenire la pubblicizzazione e la vendita di prodotti contraffatti. In questo senso, si consiglia di fare riferimento alle linee guida pubblicate nel recente studio dell'OECD '*E-commerce* Challenges in Illicit Trades in Fakes: Governance Frameworks and Best Practices' (OECD 2021). Allo stesso modo, anche identificare le buone pratiche esistenti, sia nel settore privato che in quello pubblico, aiuterebbe a condividere informazioni utili tra i diversi *stakeholder,* rafforzando quindi la lotta contro i contraffattori.

Bibliografia

AACP. 2002. «Proving the connection: links between intellectual property theft and organized crime».
AIFA. 2021. «Medicinali online: in aumento le segnalazione di prodotti contraffatti acquistati da canali non autorizzati».
Alibaba Group. 2020. «Alibaba Group 2020 Annual Report on Intellectual Property Protection».
Amazon. 2021a. «EU Policy Position Paper - Accountability for Counterfeiters».
———. 2021b. «Press release Amazon Counterfeit Crimes Unit Reaches Settlement with Influencers Who Ran Social Media Counterfeiting Scheme, Permanently Banning them from Amazon's Store and Securing Financial Payments to be Donated to Support Anti-Counterfeiting Awareness September 30, 2021 at 9:16 AM EDT». https://press.aboutamazon.com/news-releases/news-release-details/amazon-counterfeit-crimes-unit-reaches-settlement-influencers.
———. 2021c. «Report sulla protezione dei marchi».
Bosisio, Antonio, Carlotta Carbone, Maria Jofre, Michele Riccardi, e Stefano Guastamacchia. 2021. Developing a Tool to Assess Corruption Risk factors in firms' Ownership Structures - Final report of the DATACROS Project.
Bosisio, Antonio, Lorella Garofalo, Marco Dugato, e Michele Riccardi. 2017. La sicurezza del retail in Italia. Uno studio su furti, rapine e nuovi sistemi di sicurezza. Milano: Crime&tech - Università Cattolica del Sacro Cuore.
Camerini, Diana, Serena Favarin, e Marco Dugato. 2015. «Estimating the counterfeit markets in Europe». Transcrime Research in Brief 3.
Canfield, John. 2018. «The Ever-Changing Landscape of Bots and Credit Cards Testing». https://www.business.com/articles/bots-credit-card-testing/.
Cassara, John A. 2016. Trade-based money laundering: the next frontier in international money laundering enforcement. Wiley & SAS business series. Hoboken, New Jersey: John Wiley & Sons.
CBS News. 2019. «Cybercriminals are doing big business in the gaming chat app Discord». https://www.cbsnews.com/news/cybercriminals-are-doing-big-business-in-the-gaming-chat-app-discord/.
Censis e MISE. 2021. «Rapporto conclusivo sulla contraffazione in 20 province italiane: un'analisi comparata».
CISA. 2021. «Alert (AA21-265A) - Conti Ransomware». https://us-cert.cisa.gov/ncas/alerts/aa21-265a.
CNBC. 2020. «Amazon sues two influencers for peddling counterfeit goods on Instagram and TikTok». https://www.cnbc.com/2020/11/12/amazon-sues-influencers-for-allegedly-marketing-counterfeits.html.
———. 2021. «Amazon settles with influencers who allegedly peddled counterfeits on Instagram and TikTok».
Commissione Europea. 2018a. «Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679».
———. 2018b. «Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities».
———. 2019. «Libro Bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia».
———. 2020. «Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni. Sfruttare al meglio il potenziale innovativo dell'UE. Piano d'azione sulla proprietà intellettuale per sostenere la ripresa e la resilienza dell'UE.»
Consiglio d'Europa. 2019. «Linee guida in materia di intelligenza artificiale e protezione dei dati personali».
Consiglio Nazionale Anticontraffazione. 2019. «Piano Strategico Nazionale 2019-2020».
Couvèe, Koos. 2019. «Fintechs Fuel Surge in UK Defense Against Money Laundering Requests». https://www.moneylaundering.com/news/fintechs-fuel-surge-in-uk-defense-against-money-laundering-requests/.
Crime&tech. 2021. «Next Generation AML: indagine tra le banche e gli altri soggetti obbligati in Italia sull'uso dei big data e dell'intelligenza artificiale in ambito antiriciclaggio».

CyberSource. 2020. «What you need to know about card testing fraud». https://www.cybersource.com/en-us/blog/2020/what-you-need-to-know-about-card-testing-fraud.html.

Does de Willebois, Van Der Emile, Emily M. Halter, Robert A. Harrison, Ji Won Park, e J.C. Sharman. 2011. The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It. The World Bank. https://doi.org/10.1596/978-0-8213-8894-5.

eBay. 2021. «2020 Global Transparency Report».

EUIPO. 2017. «Research on Online Business Models Infringing Intellectual Property Rights - Phase 2. Suspected trade mark infringing e-shops utilising previously used domain names.»

———. 2019a. «2019 INTELLECTUAL PROPERTY SME SCOREBOARD». https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/IP_sme_scoreboard_study_2019/executiveSummary/executive_summary_2019_en.pdf.

———. 2019b. «Anti-counterfeiting Blockathon Forum. Blockchain Use Case». https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Blockathon/Blockathon-Forum_Blockchain-Use-Case.pdf.

———. 2020. Automated Content Recognition: Discussion Paper. Phase 1, Existing Technologies and Their Impact on IP'. LU: Publications Office. https://data.europa.eu/doi/10.2814/52085.

———. 2021a. Anti-Counterfeiting Technology Guide. LU: Publications Office. https://data.europa.eu/doi/10.2814/665780.

———. 2021b. Focus on Cybersquatting: Monitoring and Analysis. LU: Publications Office. https://data.europa.eu/doi/10.2814/14926.

———. 2021c. Monitoring and Analysing Social Media in Relation to IP Infringement: Report. LU: Publications Office. https://data.europa.eu/doi/10.2814/235275.

———. 2021d. «New and existing trends in using social media for IP infrigement activities and good practices to address them». Socila Media - Discussion paper. European Union Intellectual Property Office.

———. 2021e. «Payment - Discussion Paper. Challenges and good practices for electronic payment services to prevent the use of their services for intellectual property-infringing activities».

———. 2021f. Vendor Accounts on Third Party Trading Platforms: Research on Online Business Models Infringing Intellectual Property Rights : Phase 4. LU: Publications Office. https://data.europa.eu/doi/10.2814/279240.

EUIPO e Europol. 2019. «Intellectual Property Crime Threat Assessment 2019».

EUIPO e OECD. 2021a. Global Trade in Fakes : A Worrying Threat. Spain: EUIPO. https://data.europa.eu/doi/10.2814/374693.

———. 2021b. «Misuse of E-Commerce for Trade in Counterfeits». Illicit Trafficking. Paris: OECD Publishing. https://doi.org/10.1787/1c04a64e-en.

Europol. 2016. «MAIN EUROPEAN UNION HUB FOR DISTRIBUTION OF COUNTERFEIT GOODS DISMANTLED».

———. 2020. «Internet Organised Crime Threat Assessment».

———. 2021. «European Union Serious and Organised Crime Threat Assessment. A corrupting influence: the infiltration and undermining of Europe's economy and society by organized crime».

Europol e EUIPO. 2020. IP Crime and Its Link to Other Serious Crimes: Focus on Poly Criminality. Luxembourg: Publications Office. https://data.europa.eu/doi/10.2814/090414.

Eurostat. 2021. «E-commerce statistics for individuals». https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics_for_individuals.

FACT Coalition. 2019. «Anonymous Companies Help Finance Illicit Commerce and Harm American Businesses and Citizens. A need for Incorporation Transparency».

Flashpoint. 2019. «Refund Fraud and Fake Receipts Proliferate on the Deep & Dark Web». https://www.flashpoint-intel.com/blog/refund-fraud-fake-receipts/.

Garante per la protezione dei dati personali. 2019. «Deliberazione del 12 giugno 2019 - Codice di condotta per il trattamento dei dati personali in materia di informazioni commerciali».

Guardia di Finanza. 2019. «Social media e contraffazione - Conclusa l'operazione Aphrodite II». https://www.gdf.gov.it/stampa/ultime-notizie/anno-2019/giugno/social-media-e-contraffazione-conclusa-loperazione-aphrodite-ii.

———. 2020a. «Contraffazione sul web, denunciati 92 responsabili, sequestrato oltre mezzo milione di prodotti illegali». https://www.gdf.gov.it/stampa/ultime-notizie/anno-2020/febbraio/contraffazione-sul-web-denunciati-92-responsabili-sequestrato-oltre-mezzo-milione-di-prodotti-illegali.

———. 2020b. «Smantellata associazione per delinquere dedita al traffico di abbigliamento contraffatto». https://www.gdf.gov.it/stampa/ultime-notizie/anno-2020/maggio/smantellata-associazione-per-delinquere-dedita-al-traffico-di-abbigliamento-contraffatto.

He, Sherry, Brett Hollenbeck, e Davide Proserpio. 2021. «The Market for Fake Reviews».

Heinonen, Justin A., Thomas J. Holt, e Jeremy M. Wilson. 2012. «Product Counterfeits in the Online Environment: An Empirical Assessment of Victimization and Reporting Characteristics». International Criminal Justice Review 22 (4): 353–71. https://doi.org/10.1177/1057567712465755.

ICE. 2020. «HSI partners with Pfizer, 3M, Citi, Alibaba, Amazon, Merck to protect consumers against COVID-19-related fraud». https://www.ice.gov/news/releases/hsi-partners-pfizer-3m-citi-alibaba-amazon-merck-protect-consumers-against-covid-19.

Il Sole 24 Ore. 2021a. «Amazon contro falsi e contraffazioni: bloccate 10 miliardi di offerte sospette».

———. 2021b. «Blockchain ed Nfc contro il mercato miliardario della contraffazione – Il caso Authena-Masque Milano». https://guiomarparada.nova100.ilsole24ore.com/2021/10/20/blockchain-contraffazione-authena/.

International Trademark Association. 2019. «Gen Z Insights: Brands and Counterfeit Products».

Jofre, Maria, Michele Riccardi, Antonio Bosisio, e Stefano Guastamacchia. 2021. «Money laundering and the detection of bad companies: A machine learning approach for the risk assessment of opaque ownership structure». In .

Kennedy, Jay P. 2020. «Counterfeit Products Online». In The Palgrave Handbook of International Cybercrime and Cyberdeviance, a cura di Thomas J. Holt e Adam M. Bossler, 1001–24. Palgrave Macmillan.

Lince, Tim. 2020. «'Dupe culture' grows on TikTok; why this helps counterfeiters and harms brands». World Trademark Review. https://www.worldtrademarkreview.com/anti-counterfeiting/dupe-culture-grows-tiktok-why-helps-counterfeiters-and-harms-brands.

Luca, Michael, e Georgios Zervas. 2016. «Fake It Till You Make It: Reputation, Competition, and Yelp Review Fraud». Management Science 62 (12): 3412–27. https://doi.org/10.1287/mnsc.2015.2304.

Luxottica. 2017. «Il nostro modo di proteggere brand e clienti». https://www.luxottica.com/it/chi-siamo/operiamo/tutela-brand.

Mayzlin, Dina, Yaniv Dover, e Judith Chevalier. 2014. «Promotional Reviews: An Empirical Investigation of Online Review Manipulation». American Economic Review 104 (8): 2421–55. https://doi.org/10.1257/aer.104.8.2421.

McCoy, Damon. 2016. «Bullet-Proof Credit Card Processing». In . San Francisco, CA: USENIX Association.

MEF. 2018. «Analisi nazionale dei rischi di riciclaggio di denaro e di finanziamento del terrorismo elaborata dal Comitato di sicurezza finanziaria». http://www.dt.mef.gov.it/it/news/2019/aggiornamento_analisi_rischio_riciclaggio.html.

Miller, Rena S., Liana W. Rosen, e James K. Jackson. 2016. «Trade-Based Money Laundering: Overview and Policy Issues». Congressional Research Service.

Ministero dell'Interno. 2021. «Contributo del Servizio Analisi Criminale del Dipartimento della Pubblica Sicurezza - Direzione Centrale del Servizio Criminale del Ministero dell'Interno al progetto FATA».

Moiseienko, Anton. 2020. «Understanding Financial Crime Risks in E-Commerce». RUSI, Occasional Paper, .

Moiseienko, Anton, e Kayla Izenman. 2019. «Gaming the System: Money Laundering Through Online Games». Rusi Newsbrief, 2019.

Monetary Authority of Singapore. 2021. «MAS and Financial Industry to Use New Digital Platform to Fight Money Laundering». https://www.mas.gov.sg/news/media-releases/2021/mas-and-financial-industry-to-use-new-digital-platform-to-fight-money-laundering.

OECD. 2018. Il commercio di beni contraffatti e l'economia italiana: Tutelare la proprietà intellettuale dell'Italia. Paris: OECD Publishing.

———. 2021. E-Commerce Challenges in Illicit Trade in Fakes: Governance Frameworks and Best Practices. Illicit Trade. OECD. https://doi.org/10.1787/40522de9-en.

OECD e EUIPO. 2018. Trade in Counterfeit Goods and Free Trade Zones: Evidence from Recent Trends. Illicit Trade. Paris/European Union Intellectual Property Office: OECD Publishing. https://doi.org/10.1787/9789264289550-en.

———. 2020. Trade in Counterfeit Pharmaceutical Products. Illicit Trade. Paris: OECD Publishing.

———. 2021a. Misuse of Containerized Maritime Shipping in the Global Trade of Counterfeits. Illicit Trade. OECD. https://doi.org/10.1787/e39d8939-en.

———. 2021b. Misuse of E-Commerce for Trade in Counterfeits. Illicit Trade. OECD. https://doi.org/10.1787/1c04a64e-en.

OHIM. 2013. European Citizens and Intellectual Property: Perception, Awareness and Behaviour. Alicante: Office for Harmonization for Internal Markets.

Parlamento Europeo. 2017. «Risoluzione del Parlamento europeo del 14 marzo 2017 sulle implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto».

Pellegrini, Antonio, Pierpaolo De Franceschis, Chiara Bentivogli, e Eleonora Laurenza. 2020. «Un indicatore sintetico per individuare le società cosiddette cartiere». Quaderni dell'antiriciclaggio 15.

Reddit. 2018. «[Guide] "Help,I'm New Where Do I start?" FashionReps Newbie Guide + Frequently used Terms!» https://www.reddit.com/r/FashionReps/comments/ae540e/guide_help_im_new_where_do_i_start_fashionreps/.

Savona, Ernesto Ugo, e Michele Riccardi, a c. di. 2018. Mapping the risk of Serious and Organised Crime infiltration in European Businesses Final report of the MORE Project. Milano: Transcrime - Università Cattolica del Sacro Cuore.

Senato della Repubblica Italiana. 2017. Lotta alla contraffazione e tutela del made in italy. Documento di Analisi n.5.

Stroppa, Andrea, e Daniele Di Stefano. 2016. «Social media and luxury goods counterfeit: a growing concern for government, industry and consumer worlwide». A cura di Bernardo Parrella.

Stroppa, Andrea, Davide Gatto, Lev Pasha, e Bernardo Parrella. 2019. «Instagram and counterfeiting in 2019: new features, old problems».

Tian, Hongwei, Stephen M. Gaffigan, D. Sean West, e Damon McCoy. 2018. «Bullet-proof payment processors». In 2018 APWG Symposium on Electronic Crime Research (eCrime), 1–11. San Diego, CA: IEEE. https://doi.org/10.1109/ECRIME.2018.8376208.

TRACIT e AAFA. 2020. «Fraudolent Advertising Online: Emerging Risks and Consumer Fraud».

Transaction Monitoring Netherlands. 2021. «What is TMNL?»

TransUnion. 2020. «Global E-Commerce in 2020: Redefining the Retail Experience as Shopping Patterns Change».

UIBM. 2020. «Rapporto sulle Politiche Anticontraffazione 2018-2019». Ministero dello Sviluppo Economico, UIBM. https://uibm.mise.gov.it/images/documenti/Rapporto_Politiche_Anticontraffazione_20182019.pdf.

UIF. 2021. «Indicatori e schemi di anomalia». https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/index.html?com.dotmarketing.htmlpage.language=102.

UNIFAB. 2016. «Counterfeiting & Terrorism. Report 2016». https://euipo.europa.eu/ohimportal/documents/11370/71142/Counterfeiting+%26%20terrorism/7c4a4abf-05ee-4269-87eb-c828a5dbe3c6.

U.S. Attorney's Office. 2018. «Sixteen Treasure Valley Residents Indicted in Federal Court». https://www.justice.gov/usao-id/pr/sixteen-treasure-valley-residents-indicted-federal-court.

US District Court of Maryland. 2018. «UNITED STATES OF AMERICA, Plaintiff, v. MOHAMED Y. ELSHINAWY, Defendant.»

Vice. 2018. «Uno studente ha creato un impero di sneaker false su Reddit - finché non è sprofondato». https://www.vice.com/it/article/vbjkj4/vendere-repliche-sneaker-reddit.

Vigderman, Aliza. 2021. «Account Takeover Fraud: A Consumer's Guide to Protecting Yourself». https://www.security.org/digital-safety/account-takeover-prevention/.

Wall Street Journal. 2019. «Meet the Sneaker Collectors Who Intentionally Buy Fake Shoes».

Wronka, Christoph. 2021. «"Cyber-Laundering": The Change of Money Laundering in the Digital Age». Journal of Money Laundering Control ahead-of-print (ahead-of-print). https://doi.org/10.1108/JMLC-04-2021-0035.

WTO. 1994. «Annex 1C. Agreement on Trade-Related Aspects of Intellectual Property Rights.»

crime&tech
Powered by Transcrime

UNIVERSITÀ CATTOLICA del Sacro Cuore

con il supporto di

amazon