

Combating Trafficking in Counterfeit and Pirated Goods

Il 24 gennaio il *Department of Homeland Security* degli Stati Uniti (DHS) ha pubblicato il report *Combating Trafficking in Counterfeit and Pirated Goods*, che fa seguito al Memorandum per il contrasto al traffico di prodotti contraffatti e piratati dell'aprile 2019 con cui il Presidente Trump ha diramato una "call to action" per studiare il fenomeno e gli strumenti da adottare per arginarlo.

Succede, inoltre, all'ordine esecutivo emanato dallo stesso Presidente il 31 gennaio 2020 a svariati organi e agenzie governative per l'adozione di misure efficaci ad assicurare un mercato digitale sicuro e legittimo per consumatori, business, filiera e diritti di proprietà intellettuale.

Il rapporto del DHS va ampiamente in questa direzione, senza ridursi a mero documento di *overview* sull'attuale situazione in materia contraffazione, ma facendosi invece preciso *vademecum* di azioni concrete e *best practices* di settore. Assistiamo ad una prima assoluta, di uno Stato – tra l'altro culla di numerose realtà di *e-commerce* – che nero su bianco detta azioni immediate che le autorità governative devono intraprendere per fronteggiare contraffazione e pirateria, che sembrano così assumere una posizione di assoluta priorità che non è frequente riscontrare nelle agende politiche della stragrande maggioranza degli Stati.

Ma l'aspetto più diromponente consiste certamente nella serie di *best practices* rivolte alle piattaforme di *e-commerce* che ospitano *marketplace* in cui soggetti terzi promuovono e vendono prodotti e altri intermediari online affini. Il rapporto afferma che l'adozione di tali pratiche verrà raccomandata, incoraggiata e monitorata dal *National Intellectual Property Rights Coordination Center* (IPR Centre), guidato dall'*United States Immigration and Customs Enforcement* (ICE).

Di nuovo, nulla di simile è stato mai messo a punto da un governo nazionale e ciò rende il rapporto del DHS un incredibile passo in avanti nel riconoscimento della responsabilità degli intermediari digitali per i contenuti illeciti caricati dagli utenti. Un passo avanti cui il resto del mondo, Unione Europea in *primis*, deve saper guardare e far proprio, iniziando col delineare un *framework* normativo chiaro che tenga conto dell'evoluzione che ha interessato i giganti del web da vent'anni a questa parte.

Certamente la natura di raccomandazioni esclude il riconoscimento di una vera e propria responsabilità legale in capo alle piattaforme, ma in ogni caso si conferma un'inversione di tendenza rispetto al concetto di "safe harbour" nel quale i grandi players dell'online si crogiolano da tempo, in forza di leggi obsolete che impongono una reazione da parte della piattaforma solo in caso di "conoscenza" della violazione e di "controllo" sui contenuti.

Ciò che invece emerge dal rapporto del DHS è un ampio spettro di azioni che gli intermediari digitali possono attuare proattivamente, a partire da "Termini di Servizio" completi ed esaustivi, che esplicitino il divieto di pubblicizzare e vendere prodotti che violano diritti di proprietà intellettuale, fornendo in tal modo alla piattaforma uno strumento legale per agire velocemente nei confronti dei trasgressori. Parimenti, viene raccomandato l'inserimento di un elenco di ripercussioni che l'utente subirà in caso di violazione: in prima istanza, la sospensione, l'eliminazione e l'interdizione dell'account senza che sia necessaria una decisione da parte di una corte. Si richiede, inoltre, la presenza di una struttura di *enforcement* "a scalare" per gli *infringements* più gravi o per le infrazioni

ripetute: dall'eliminazione permanente del profilo del venditore e dei profili a questo associato, alla confisca e distruzione dei beni in violazione presso magazzini e centri logistici gestiti dalla piattaforma.

Infine, i Termini di Servizio dovrebbero permettere alle piattaforme di imporre limitazioni appropriate sui prodotti listati, di richiedere informazioni sul paese di origine della merce, oltre che requisiti bancari e d'indennità e di migliorare l'identificazione dei *sellers* prima che questi vendano i prodotti. Ed è proprio l'identificazione dei *sellers* il punto focale su cui insiste a più riprese il DHS nell'elencazione delle *best practices* che le piattaforme sono invitate ad adottare.

Know your customer. Assicurati che chi promuove e vende sulla tua piattaforma sia un soggetto affidabile che offre prodotti leciti. E, qualora non lo sia, rimuovine la presenza.

Tale concetto è declinato in una raccomandazione di "Controllo significativamente rafforzato sui venditori terzi", per cui le piattaforme dovrebbero raccogliere informazioni sufficienti per l'identificazione del *seller*, dei suoi *listing*, dei suoi account e dei luoghi dove ha sede il suo business, prima che il venditore abbia modo di muoversi sulla piattaforma. Altre informazioni rilevanti dovrebbero poi riguardare lo storico del *seller*: è mai stato "bannato" o rimosso da altre piattaforme? È già stato implicato nella vendita di prodotti contraffatti e/o piratati? Oltre che il riconoscimento del *seller* come soggetto non titolare dei diritti di proprietà intellettuale posti sui prodotti che sta vendendo.

L'assenza di tali dati, che la piattaforma dovrebbe ottenere anche tramite l'uso di strumenti tecnologici, di analisi, di *risk assessment* e di audit per trasgressori recidivi e ad alto rischio, escluderebbe la possibilità per il *seller* di iscriversi alla piattaforma oppure la sua violazione dei Termini di Servizio.

L'esigenza di avere contezza dell'identità del venditore risponde poi ad un ulteriore scopo: quello di permettere ai consumatori di prendere azioni informate nel momento di scelta del prodotto e finalizzazione della transazione. Tale grado di trasparenza può essere ottenuto solo se la piattaforma rende il consumatore edotto dell'identità del *seller* e di coloro che sono responsabili per il completamento della transazione.

Ad oggi è possibile, per qualunque utente, creare più account sulla medesima piattaforma, senza che sia evidente alcun collegamento tra gli stessi e questo può chiaramente ostacolare l'individuazione di profili in violazione. Il DHS raccomanda quindi alle piattaforme di richiedere ai *sellers* di fornire informazioni precise su tutte le vendite che fanno capo allo stesso soggetto: questo anche per agevolare il monitoraggio, che, come si sa, è un'attività onerosa e complessa che grava sui titolari di diritti.

È chiaro, dunque, che la direzione verso cui gli Stati Uniti stanno andando è quella di non ammettere più alcuna opacità nel mondo dell'*e-commerce*, dove invece oggi regna spesso l'incertezza: sui chi ti sta vendendo il prodotto, sul prodotto stesso, sull'affidabilità di uno spazio senza frontiere nel quale chiunque può costruire il proprio profilo ad arte.

Tra le *best practices*, inoltre, un attento sguardo è dedicato al noto meccanismo del "*Notice and take down*", per il quale la piattaforma rimuove il contenuto *infringing* dopo aver ricevuto una notifica da parte del titolare di diritto. Si tratta di un metodo che richiede tempo e un impiego non irrisorio di

risorse da parte dei *rightholders*, sui quali, come già detto, grava l'onere di identificare i *sellers* in violazione per effettuare poi la notifica alla piattaforma.

Per porre rimedio a questa evidente asimmetria di obblighi tra titolari di diritti e piattaforme, si raccomanda a queste ultime di creare e mantenere un sistema di *enforcement* chiaro, preciso e veloce caratterizzato da: a) minimi requisiti di registrazione perché i *rightholders* possano prendere parte al processo di *N&TD*; b) regole ragionevoli che considerino i profili che pubblicizzano un ampio numero di prodotti su piattaforme *C2C* come delle imprese; c) massima trasparenza nei confronti dei titolari di diritti rispetto alla gestione delle loro notifiche e a tutte le altre attività nelle quali il *seller* in questione è implicato.

Il flusso di dati, poi, non si ferma qui: le piattaforme sono invitate a condividere con i *rightholders* danneggiati tutti i dettagli relativi ai beni in violazione e le informazioni sullo stock rimanente di prodotti contraffatti e piratati fermo nei loro magazzini. Parimenti dovrebbero essere poste in essere tutte le misure, nelle possibilità della piattaforma, che comportino la rimozione dei beni e la loro estromissione dal mercato lecito, anche per il tramite di un ingaggio immediato con le forze dell'ordine, cui saranno forniti dati di intelligence e informazioni di rilievo.

Quelle appena descritte sono solo alcune delle azioni che le piattaforme già ora sarebbero in grado di realizzare per supportare la lotta al mercato del falso. I *brand owners* lo sanno, i giganti dell'*e-commerce* lo sanno e anche la politica è a conoscenza delle radicali trasformazioni che hanno riguardato le piattaforme digitali negli ultimi anni e che hanno reso tali soggetti i veri detentori del potere economico della nostra epoca; a partire dal *data-mining*, che attraverso l'intelligenza artificiale, le scienze statistiche e il cosiddetto *machine-learning*, permette alle piattaforme del commercio virtuale l'estrazione di informazioni utili a conoscere utenti e consumatori e, di conseguenza, ad avere il controllo sui contenuti che da questi vengono postati.

Ma se da un lato il Dipartimento per la Sicurezza Interna degli Stati Uniti individua importanti *best practices* che le piattaforme dovrebbero adottare, dall'altro riporta una serie di azioni immediate che il DHS, tramite l'organismo per la sicurezza delle frontiere, l'*US Customs and Border Protection* (CBP), porrà in essere tramite attività di *enforcement* e di raccomandazioni al governo statunitense.

Tra le prime rientrano il riconoscimento di una responsabilità di "*due diligence*" in capo a tutte le entità coinvolte nelle operazioni di importazione (come piattaforme e intermediari che hanno a gestione magazzini e centri logistici), oltre che una raccolta di dati relativi ai diversi modelli di business delle piattaforme di *e-commerce* per valutare eventuali gap normativi e per analizzare i meccanismi di distribuzione e stoccaggio delle merci in magazzini domestici e centri di logistica, oltre che per identificare venditori e natura della merce in import.

Un ulteriore aspetto da segnalare è altresì l'intenzione di rendere responsabili non solo gli intermediari online, ma pure quelli offline, come corrieri, servizi postali, etc., i quali dovranno condividere con le forze di polizia informazioni su importatori che siano stati sospesi o esclusi da una sorta di "*white-list*" realizzata per gli importatori che si trovano sul suolo statunitense.

Vengono poi previste multe civili e penali per gli intermediari che abbiano diretto, assistito finanziariamente, aiutato e incoraggiato l'importazione di prodotti falsi; inoltre, il DHS raccomanda

una modifica normativa che permetta al governo la possibilità di emanare un'ingiunzione contro *marketplaces* e piattaforme sui quali vengono venduti beni contraffatti.

Va poi evidenziata la volontà di dare estrema priorità ai reati connessi alla proprietà intellettuale “a prescindere dalla loro portata” e di investigare e perseguire, ad ogni livello della filiera produttiva, tali violazioni. Non si tratta di un'asserzione di poco conto, considerando quanto questo tipo di crimini sia in genere ampiamente sottostimato e, di conseguenza, affrontato debolmente, sia da un punto di vista politico che di *enforcement*.

Un ulteriore aspetto sul quale il rapporto del DHS insiste è l'esigenza di una maggior collaborazione tra i vari attori coinvolti nella catena distributiva, a partire dall'ente deputato alla gestione dei servizi postali, cui si richiede la condivisione di informazioni essenziali per l'individuazione e il tracciamento dei colli inviati per via aerea. C'è poi l'istituzione di un “*E-Commerce Working Group*”, in seno all'IPR Centre, per la promozione di un maggior flusso di dati tra piattaforme e intermediari come corrieri, spedizionieri, motori di ricerca, servizi di pagamento, etc., e di un “consorzio anti-contraffazione” per lo scambio di informazioni sugli intermediari coinvolti nel traffico di prodotti contraffatti e piratati e sulle tecniche di automazione per la realizzazione di sistemi di *targeting* proattivi che permettano il monitoraggio automatico delle piattaforme.

Ma un più radicale approccio al tema del contrasto alle violazioni di diritti IP passa anche e soprattutto attraverso una modifica del *framework* normativo, per cui il DHS pensa ad una modernizzazione dell'assetto di regole in materia di proprietà intellettuale, arrivando ad auspicare che i beni contraffatti vengano assimilati agli stupefacenti, anche al fine di sottolineare l'importanza che assume la lotta alla contraffazione per lo Stato.

Di estrema importanza è infine la raccomandazione che il DHS fa al Governo di valutazione dello stato di *liability* delle piattaforme di *e-commerce* per violazioni di diritti IP stando ai recenti pareri della giurisprudenza. Non è infatti infrequente, come oltreoceano così anche in Europa, che le corti si muovano parallelamente al legislatore, partendo dal caso concreto e particolare di *infringement* e giungendo a riconoscere una responsabilità in capo ai soggetti che ospitano nei loro spazi digitali i contenuti in violazione. Nel nostro continente è successo già nel 2009 con la causa *L'Oréal v. eBay* (C-324/09) portata di fronte alla CGUE, dove è stato confermato il ruolo attivo della nota piattaforma di *e-commerce* e perciò la sua esclusione dal regime del *safe harbour*.

Ma anche diverse corti nazionali si sono mosse in tal senso: lo dimostrano i casi *Mediaset v. Vimeo* (693/19), *Mediaset v. Facebook* (3512/19) e il caso storico di *Mondadori* contro alcuni *mere conduit service providers* (*Tiscali, Vodafone, Wind, Fastweb, Telecom*) che ha imposto un dovere di “*stay-down*” a questi ultimi per qualsiasi contenuto che nel futuro sarebbe potuto essere postato su link “*alias*”.

E non solo Italia, anche i giudici di altri paesi comunitari si sono scontrati contro la nota e ormai da tempo criticata *Direttiva E-Commerce* del 2000, la normativa attualmente in vigore per quanto concerne la responsabilità degli *ISP*: si pensi al caso *Yahoo* (10893/11), *Dailymotion* (342/18), al caso *Tommy Hilfiger v. Facebook* del 2018, nel quale un tribunale civile di Amsterdam ha riconosciuto il ruolo attivo del social network e il suo dovere di prevenire eventuali future violazioni in ambito IP.

Il fatto che le corti comincino a fissare queste piccole ma importanti fondamenta costituisce un argomento che deve necessariamente essere posto al centro della conversazione, perché la revisione

di norme ormai obsolete sia possibile; si tratta di una posizione non negoziabile che anche negli Stati Uniti sta cominciando a prendere vita, al fine di ammettere una cosiddetta “*contributory liability*” in capo alle piattaforme che oltre ad avere ormai un evidente ruolo attivo sui contenuti postati, traggono anche un guadagno considerevole dalle transazioni che avvengono all’interno dei loro spazi virtuali.

Il rapporto del DHS rappresenta quindi una fondamentale conferma di una consapevolezza politica sul ruolo che i giganti del web hanno ormai assunto all’interno dell’ecosistema digitale: a questo *shift* si auspica che si allinei anche l’Unione Europea, per la formulazione di una nuova regolamentazione in materia di responsabilità degli ISP per i contenuti che violano diritti di proprietà intellettuale, con doveri di azione proattiva e non solamente di reazione a fronte della condotta illecita.

I grandi *online players*, come già previamente menzionato, hanno a disposizione tutti gli strumenti per contrastare il fenomeno, ma è chiaramente necessaria la realizzazione di un substrato normativo che renda coattiva la loro azione di *enforcement* dei diritti IP, non solo rispetto alla minaccia presente, ma anche alle trasgressioni che potrebbero in un secondo momento verificarsi all’interno della piattaforma. Su tale punto oltreoceano ci si sta muovendo – ancora una volta - molto più velocemente: è infatti di recente pubblicazione il *Shop Safe Act*, un disegno di legge presentato da legislatori bipartisan della Camera dei Rappresentanti statunitense, che introduce un concorso di responsabilità tra trasgressore e piattaforma per la vendita di prodotti contraffatti con un obbligo, in capo a quest’ultima, di controllo sui contenuti anche per la prevenzione di future condotte illecite. Ci troviamo ormai in un momento cruciale, il punto di non ritorno in cui diventa necessario prendere delle decisioni ferme e coraggiose, per un mercato più trasparente, per consumatori più informati e in maggior sicurezza, e per le aziende legali che soffrono, sia da un punto di vista economico che reputazionale.