

Aprile 2020 - REPORT INDICAM

ONLINE REGULATION



EXECUTIVE SUMMARY

A cura di:
Claudio Bergonzi
Mariachiara Anselmino

INDICAM

Istituto di Centromarca
per la lotta alla contraffazione

Indice

3 **PREFAZIONE**

4 **RAPPORTO DEL DEPARTMENT OF
HOMELAND SECURITY**

6 **THE SHOP SAFE ACT**

8 **THE DIGITAL POLITICAL GUIDANCES
OF THE EU**

11 **CONSIDERAZIONI CONCLUSIVE**

Prefazione

Il Rapporto INDICAM sul digitale è un'analisi di tre spunti di discussione attuali in materia di online regulation: il rapporto e le raccomandazioni del DHS USA in tema di responsabilità degli intermediari, una proposta di legge USA e il Documento programmatico dell'UE in tema di digitale. In tutti e tre i capitoli emerge chiaro un obiettivo: dare al mercato digitale un set di regole più adeguate delle attuali, andando a prevedere una maggiore dovere di diligenza per coloro che, efficacemente, la Commissione Europa chiama "gate keeper", ovvero coloro che detengono il controllo del nostro accesso, come cittadini e consumatori, al mercato online.

E' necessario, quindi, che anche in Europa si avvii rapidamente la discussione in materia, ormai troppo a lungo e forzatamente tenuta fuori dai processi di revisione in materia di digitale. A una platea abituata all'analisi di INDICAM in tema di digital commerce il rapporto (di cui questo è l'executive summary) potrà riportare alla mente punti e posizioni già condivise. Si tratta, tuttavia, di un aggiornamento alla luce degli ultimi passaggi sia in USA che in EU, e di un rapporto destinato non solo al pubblico, principalmente imprese, che sono l'audience privilegiata dell'associazione per la tutela dei diritti IP, ma ad un pubblico più vasto, composto da stakeholder del settore, policy makers, istituzioni.

Buona lettura

Claudio Bergonzi

Segretario Generale INDICAM

RAPPORTO DEL DEPARTMENT OF HOMELAND SECURITY

In gennaio 2020 il 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 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 è un vademecum di azioni concrete e best practices di settore. L'aspetto più diromponente consiste certamente nella serie di indicazioni rivolte alle piattaforme di e-commerce che ospitano marketplaces in cui soggetti terzi promuovono e vendono prodotti e altri intermediari online affini.

Ciò che in sostanza emerge dal rapporto del DHS è un ampio spettro di azioni che gli intermediari digitali possono attuare proattivamente, a partire da "Termini di Servizio" 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.

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.

Tale concetto è declinato in una raccomandazione di "Controllo significativamente rafforzato sui venditori terzi".

È chiaro, dunque, che la direzione verso cui gli Stati Uniti stanno andando – pur se attraverso raccomandazioni e non ancora grazie a norme di legge - è quella di non ammettere più alcuna opacità nel mondo dell'e-commerce: su chi 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 la 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.

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 piratate.

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.

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).

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.,

Vengono poi previste sanzioni civili e penali (multe) 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.

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 in relazione a quanto deciso dalla giurisprudenza. Oltreoceano, così come in Europa, i Tribunali sono infatti ed in più occasioni giunti a riconoscere una responsabilità in capo ai soggetti che ospitano nei loro spazi digitali i contenuti in violazione, anche in costanza delle attuali norme di limitazione di responsabilità/safe harbor.

THE SHOP SAFE ACT

LA PROPOSTA DI LEGGE 6058 PER MODIFICARE LA LEGGE MARCHI USA

Con l'atto 6058 della House of Representatives, il 2 marzo 2020 sei deputati USA hanno presentato una proposta – bill - di amendment del Trademark Act del 1946, volto a dare maggiore aderenza alla struttura legislativa in un'epoca di grande espansione dell'e-commerce.

Il bill 6058 che presenta parecchi spunti interessanti verso un maggiore equilibrio di azioni in capo alle piattaforme online per un maggiore controllo e screening delle offerte poste in essere da venditori terze parti che ne sfruttino le infrastrutture. Il bill si presenta tecnicamente come una proposta di amendment al Trademark Act del 1946 quindi dando già chiaro il perimetro entro il quale esso si debba muovere, ossia la materia degli infrangements a danno dei marchi.

L'obiettivo del provvedimento è di identificare quali responsabilità siano in capo alle piattaforme come co-responsabili per attività di vendita, di pubblicità, di offerta o di distribuzione da parte di terze parti di prodotti recanti marchi contraffatti e che siano di impatto sulla salute e sulla sicurezza.

Le azioni che si chiede alla piattaforma di intraprendere al fine di dimostrare la sua noncorresponsabilità nell'illecito commesso dal terzo sono quelle caratteristiche di una due diligence accurata, come da anni INDICAM chiede sia fatto obbligo agli intermediari online.

Un passaggio fondamentale per un operatore e-commerce sarebbe una corretta e completa identificazione del seller.

Questa disposizione del bill USA è senz'altro importante pur generando un paio, almeno, di punti da risolvere: la gestione di tutto ciò in un ambito di piena compatibilità con le norme a tutela della privacy – pensiamo al GDPR EU, ad esempio - ed anche il successivo utilizzo di tali dati posto in essere sempre in analoghe condizioni.

Lo spirito del bill prosegue prevedendo che la piattaforma “imponga”, a pena del decadimento dalla non-responsabilità, al venditore terzo di accettare di non utilizzare un marchio contraffatto in connessione con la vendita, l'offerta in

vendita, la distribuzione o la pubblicità di prodotti sulla piattaforma e che esso accetti, con le condizioni di contratto con la piattaforma, di soggiacere alla giurisdizione degli Stati Uniti d’America in relazione ad ogni azione.

Il punto forse di maggiore esplicito interesse del bill è il tema dei meccanismi, anche automatizzati, che debbano essere posti in essere preventivamente - ecco il termine più importante che da anni INDICAM pone avanti a ogni azione di lobbying in materia di digitale – al fine di evitare che siano posti in vendita, o in offerta, o in pubblicità o in distribuzione beni recanti marchi contraffatti.

Due previsioni riguardano la possibilità che un infringer ritorni a pubblicare offerte; in questo caso si prevede che ci debba essere, in sostanza, nuovamente un dovere di diligenza preventivo al fine di attrezzare tools che intervengano con queste finalità.

Interessante che già nella proposta si preveda un obbligo in capo alla piattaforma di condivisione, con organi di enforcement e con i titolari dei diritti violati, delle informazioni di identificazione del seller terzo ritenuto responsabile degli infrangements e, quindi, allontanato in base ai tre strikes dalla piattaforma stessa. La norma si rivolgerebbe a soggetti di commercio elettronico che vengono specificati ed ovviamente balza all’occhio che resta vagamente accennato come soggetti ibridi potrebbero rientrare in tale previsione. Difatti, ad esempio, un marketplace di Facebook rientrerebbe mentre un motore di ricerca, di fatto non venditore direttamente, ne sembrerebbe escluso.

Il bill si riferisce a prodotti pericolosi e non sicuri, e viene precisato che, di fatto, sono prodotti anche non certificati, come di fatto ogni prodotto fake risulta essere. Questo bill è una pietra angolare da cui deve partire la discussione anche Europea di riforma delle norme a tutela dell’e-commerce. Come si vede nella sezione successiva, molta la strada da percorrere nel nostro continente.

THE DIGITAL POLITICAL GUIDANCES OF THE EU

La Commissione presieduta da Jean-Claude Juncker e che ha terminato il proprio mandato nel 2019 non ha brillato nel cercare di adeguare l'obsoleta legislazione Europea sul commercio elettronico, spesso con una narrativa vuota di contenuto al di là del pieno di parole spese.

Ciò che manca in UE ormai - è evidente anche alla luce delle evoluzioni legislative anche negli altri grandi scenari economici e sociali del mondo come gli USA e perfino la Cina pur tra molte contraddizioni - è un sistema di norme che sia almeno adeguato all'attuale stadio evolutivo del commercio elettronico, radicalmente diverso - anche e soprattutto per la forza economica dei suoi protagonisti, anche in rapporto a quella dei titolari di diritti - rispetto a quello proprio delle sue origini che è ancora fedelmente riflesso nelle molte limitazioni di responsabilità previste nella Direttiva 2000/31/CE.

I pilastri con cui la Commissione ora identifica le necessità di intervento nel digital sono proprio orientati a questo fine, e sembra un quadro complessivo esaustivo quello che si affronta. AI, sicurezza della rete, sicurezza dei dati, loro tutela e immense possibilità da loro concesse, contenuti e responsabilità. Un framework, insomma, di ampia portata che dovrebbe portare a colmare il gap dell'Europa rispetto ad USA e Cina.

Il primo punto che il documento affronta è quello dei dati, cui anche in altre fonti della Commissione si dà ampio risalto.

Il riconoscere il ritardo europeo è un punto di partenza. E' interessante notare come nei documenti la Commissione in più di un passaggio faccia sempre riferimento a una "via Europea" per ogni aspetto.

Trattando di dati la Commissione menziona l'importanza di un'infrastruttura di sicurezza più ampia e forte di quella attuale, anche in previsione dei massicci investimenti nel digitale che intende porre sul tavolo, arrivando a credere fortemente in tecnologie 5G (e successive 6G come si accenna già). Un totale di 65 miliardi di Euro che dovrebbero accrescere il PIL Europeo di oltre 14 punti entro il 2030.

Le linee generali di avanzamento in queste aree per la Commissione passano da un white paper su AI, su investimenti massicci per soluzioni all'avanguardia in ambito tecnologico per analisi di dati, infrastrutture al servizio di tali attività e industria della componentistica adatta a procedere verso questo obiettivo. Altri passaggi menzionati sono un importante investimento su cybersecurity, sempre più a rischio in un mondo interconnesso, e su una digital education pervasiva a livello comunitario, con target sia i singoli cittadini che le imprese.

La parte che più interessa i titolari di diritti IP, tuttavia, è quella che si apre sotto il titolo "Una società aperta, democratica e sostenibile". La fiducia è il tema introduttivo, la pietra angolare della lotta agli illeciti online: un prodotto recante un marchio contraffatto per definizione è una minaccia per l'utilizzatore.

Il secondo concetto importante è quello dell'equiparazione tra online ed offline, che ritorna in un paio di passaggi. Tradotto in termini pratici, significa, ad esempio e se n'è trattato nella sezione precedente, che un seller terzo di una piattaforma dovrebbe essere identificato in maniera inequivocabile, attraverso i dati disponibili, e queste informazioni dovrebbero poi essere mantenute in capo agli ISPs, in Europa ovviamente secondo le regole imposte dal GDPR, per ulteriori necessità.

Equiparare offline ad online significherebbe, anche ed oltre la raccolta di dati identificativi, attuare un conseguente sistema più efficace di responsabilizzazione. Di fatto, ad esempio, un seller terzo identificato con efficacia, anche ricorrendo alla banca dati UE di partita IVA per citare anche solo una delle fonti, e di cui la piattaforma tracci con rigore anche altri elementi caratteristici (filiera, solidità finanziaria, certificazioni di autorizzazione commerciali e di utilizzo di altri contenuti protetti da diritti), andrebbe a essere classificato con grande precisione. Quindi la corresponsabilità di ciò che sia messo in atto dal terzo sarebbe a quel punto automatica.

Un aspetto significativo che le modifiche all'attuale schema normativo vorrebbero introdurre è, quindi, quello di porre sotto un riflettore e specificare efficacemente il significato di "ruolo attivo" degli intermediari.

Sin dalla storica L'Oréal vs eBay del 2009, così come la Mediaset RTI vs Vimeo del 2019 in Italia o la Tommy Hilfiger vs. Facebook del 2018, il ruolo attivo degli hosting provider viene riconosciuto in taluni aspetti di servizi che di per sé non comporterebbero tale riconoscimento; la conseguenza, in tutte queste decisioni, fu

l'affermazione di responsabilità dell'ISP. Questi passaggi sono dunque fondamentali nel percorso di revisione della Direttiva, nel considerare il business model di alcuni operatori online. Si tratta, in una visione più allargata, di considerare come avvenga l'accesso alle informazioni contenute in rete. La Commissione, nel suo documento, cita gli operatori intermedi della rete come dei veri e propri gate-keeper, e forse questa definizione rende esattamente il senso della presa di coscienza (finalmente) del significato della loro presenza nelle vite digitali di centinaia di milioni di utenti comunitari.

Considerazioni Conclusive

Nel 2020 il commercio elettronico non è certamente più “l’altro commercio”, fratello minore di quello offline. Tanto più nell’epoca dei primi mesi dell’anno, vissuti in maniera drammatica sulla scia della pandemia da virus Covid-19, in cui il forzato isolamento fa realmente comprendere quanto delle nostre vite ed attività sia ormai possibile affidare alle azioni via web, ci si accorge però che questa interdipendenza con la rete necessita una maggiore definizione del ruolo dei “gate keeper”, come li chiama la Commissione UE, che con la presidente von der Leyen sembra avere cambiato marcia su questi temi rispetto alla precedente. Che li si chiami gate-keeper, intermediari online, piattaforme o OTP, resta il fatto che il loro ruolo nella circolazione di contenuti (informazioni, prodotti, servizi) è la vita stessa della rete. Cosa USA ed Europa stanno facendo e dicendo di voler fare in tema di internet governance e, meno aulicamente ma più prosaicamente, per livellare il terreno di gioco? Il warning del Dipartimento Homeland Security è un segno evidente che la situazione è andata molto lontano senza interventi. Le (troppe) limitazioni di responsabilità previste favore dei gate keeper è diventato molto simile ad una no man’s land, dove in relazione alla lotta ai contenuti illeciti vigono nella sostanza le “leggi” che i più forti operatori online si auto-impongono. La proposta di una legge USA è un segno che qualcosa, anche nel cuore della nazione che più di ogni altra ha visto grandi operatori online prosperare sotto l’ombrello del safe-harbor, può e deve cambiare. L’Europa ha perso terreno nella digitalizzazione, sia essa infrastrutturale, alfabetica, contenutistica, nel corso del tempo. INDICAM, con questo rapporto, vuole svolgere il proprio compito di “assemblatrice” di uno sforzo comune, volto a porre una serie di analisi e di considerazioni alla base del percorso che deve portare l’Europa ad una revisione delle norme in materia di commercio elettronico e ad una presa di coscienza su cosa l’IP rappresenti e come necessiti di supporto e di protezione, anche online.

2020 INDICAM – ALL RIGHTS RESERVED