INDICAM

PER LA TUTELA DELLA PROPRIETÀ INTELLETTUALE

INDICAM POSITION – DIGITAL SERVICES ACT

INDICAM accoglie positivamente la proposta "*Digital Services Act*" (DSA) della Commissione Europea, come primo importante passo per assicurare un ambiente digitale più trasparente e sicuro per i consumatori e più attento alla tutela dei diritti di proprietà intellettuale e al *know-how* delle aziende, senza con ciò limitare i diritti e le libertà fondamentali.

Le trasformazioni che da vent'anni a questa parte hanno interessato il mondo online hanno garantito opportunità di business e sono state stimolo per la conoscenza, la crescita e lo sviluppo di nuove forme di impresa e accesso a beni e servizi per il pubblico. Tuttavia, è innegabile che l'era digitale abbia presentato, allo stesso tempo, rischi e sfide sotto il profilo della sicurezza dei prodotti offerti sul web, sollecitando la comunità di portatori di interesse a chiedersi cosa potesse essere migliorato nel corrente assetto normativo per garantire agli utenti di fruire delle opportunità di Internet senza l'ombra di un'informazione opaca e ingannevole e della minaccia posta da *cybercrimes* e commercio illegale.

Per tale motivo, il DSA rappresenta un'occasione cruciale per assicurare da un lato la protezione dei consumatori nell'accesso a prodotti leciti e sicuri, dall'altro la tutela delle imprese e del loro patrimonio di investimenti, perché, come affermato dalla stessa Commissione, "**ciò che è illegale offline deve essere illegale online**" e i fornitori di servizi digitali costituiscono un tassello essenziale per garantire ciò.

A tal proposito, è importante rilevare la sussistenza di una profonda separazione tra prevenzione del commercio di prodotti illegali e tutela della libertà di espressione: includere **misure proattive** tra le misure richieste agli *online service providers* per mantenere un ecosistema digitale sicuro e trasparente è qualcosa di significativamente differente dal monitoraggio sulle opinioni o i contenuti generati dagli utenti. Un prodotto illecito non può costituire nulla di controverso dal momento in cui la sua illiceità sia stata accertata e, d'altro lato, tali garanzie sono le medesime cui devono sottostare i venditori tradizionali: non ci sono quindi ragioni per cui le regole dovrebbero essere differenti quando parliamo di *e-commerce*.

Per il medesimo motivo, si ritiene che, per assicurare l'accesso ad un mercato pulito da beni illeciti, **a prescindere dalla grandezza, tutti i fornitori di servizi digitali siano tenuti a garantire la tutela del consumatore e dei diritti di proprietà intellettuale**: e questo è possibile solo attraverso una **appropriata *due diligence*** per avere contezza di chi sono i soggetti che sfruttano tali servizi digitali (il c.d. protocollo "**Know your Business Customer**" - **KYBC**) e trasparenza nei confronti degli utenti. Sono elementi che dovrebbero costituire la soglia minima da sostenere per fare business, indipendentemente dal fatto che si tratti di piccole, medie o grandi piattaforme.
Infatti, se è impensabile un qualsiasi tipo di esenzione per le piattaforme più piccole in caso di traffico di stupefacenti o armi, lo stesso deve valere anche per i prodotti contraffatti, parimenti rischiosi sotto il profilo della salute e della sicurezza.

Oltretutto, le misure di KYBC vengono già implementate da alcune piattaforme, sono rese possibili da diverse tecnologie di verificazione (es. *Onfido, Jumio, Ubble, IDnow*, etc.) e sono obbligatorie in altri ambiti (si vedano le Direttive UE 849/2015 e 843/2018 sull'antiriciclaggio, la Direttiva UE 83/2011 sui diritti del consumatore e, anche oltreoceano, gli Stati Uniti si stanno muovendo nella

medesima direzione, come dimostra la legislazione adottata dallo Stato dell'Arkansas e l'*INFORM Consumers Act* in discussione a livello federale).

Un'ulteriore nota sul tema *KYBC* riguarda le comprensibili preoccupazioni riguardo all'utilizzo dei social media sia come piattaforme di *e-commerce* che come piattaforme di condivisione di opinioni. Mentre raccomandiamo di estendere la disposizione *KYBC* a tutti gli intermediari coinvolti nella promozione o nella vendita di prodotti, crediamo fermamente nell'importanza di salvaguardare la libertà di espressione. Perciò non si richiederebbe una verifica generalizzata dell'identità per tutti gli utenti, ma solo per coloro che utilizzano i social media per promuovere o vendere prodotti, cui le piattaforme dovrebbero richiedere la creazione di un account "*business*" separato, l'unico ad essere verificato perché non sia sfruttato per commercializzare merce illecita.

È poi sicuramente da lodare l'introduzione di un obbligo per le piattaforme di raccogliere e verificare determinate informazioni sui venditori che utilizzano i loro servizi, ma per ottenere i risultati cui la proposta legislativa ambisce – un ambiente digitale giusto, sicuro, trasparente – si ritiene opportuno **estendere il novero di soggetti tenuti a tale *due diligence***.
Qualunque soggetto voglia sfruttare il web per business, ha bisogno, per esempio, di un nome a dominio, di un sito web accessibile agli utenti, di pubblicità e di un servizio di pagamento: tali intermediari dovrebbero essere tenuti a verificare l'identità della persona con cui entrano in affari, a sapere che si tratta di qualcuno di affidabile che si muove nel rispetto delle regole. Non si tratta di un controllo sul comportamento del cliente, ma di una semplice verifica sull'identità dello stesso, anche sulla base di dati disponibili pubblicamente. Qualora sia accertato che il soggetto menta sulle proprie generalità, è importante che tali intermediari interrompano i loro servizi e informino le autorità.
D'altro canto, i titolari di diritto non hanno contezza circa l'identità di un richiedente di nome a dominio che apre il proprio sito web per vendere prodotti illegali o di un venditore che sfrutta una piattaforma di *e-commerce* per pubblicizzare merce contraffatta. Tali dati sono visibili solamente **ai fornitori di servizi digitali, che, nel rispetto delle norme applicabili, devono essere tenuti a condividere i contatti e l'identità del trasgressore con titolari di diritto e forze dell'ordine**.
Se davvero vogliamo vedere una riduzione significativa – se non una scomparsa definitiva – dei prodotti illeciti online, ciascun anello della catena che si interpone tra *bad actor* e consumatore finale deve essere coinvolto.
Pertanto, se un fornitore di servizi digitali non intenda verificare l'identità dei suoi clienti, non dovrebbe essere ammesso al regime di esenzione di responsabilità.
Si ricorda, infine, come già l'Art. 5 della stessa Direttiva E-Commerce, spesso rimasto inapplicato, prevedeva tali obblighi informativi.

Tornando alla proposta della Commissione, l'Art. 5 condiziona, correttamente, l'esenzione di responsabilità all'assenza di un ruolo attivo da parte del *digital service provider*. Sarebbe però utile chiarire quando si profili un **ruolo attivo** in capo alla piattaforma.

Un ulteriore punto cruciale, che risulta tuttavia assente nel testo della proposta, è l'introduzione di **misure proattive e preventive obbligatorie** per contrastare il traffico di prodotti illegali. Se ciò che è illecito offline è illecito online, come i rivenditori nell'ambiente fisico sono tenuti a offrire e vendere beni leciti e a far fronte ad eventuali infiltrazioni di prodotti vietati dalla legge, la medesima considerazione dovrebbe essere richiesta agli operatori digitali.

La previsione di misure "volontarie" svolte "in buona fede e in maniera diligente", come recita il *consideranda* 25, non può essere sufficiente nella lotta al mercato illegale: è necessario che vi sia una regola vincolante che obblighi i fornitori di servizi online al medesimo *duty of care* richiesto ai venditori offline.

Inoltre, se a seguito di (1) una misura posta proattivamente in atto dalla piattaforma, (2) un ordine di una corte di giustizia, (3) una notifica del titolare di diritto che accerta la natura illecita di un prodotto, quest'ultimo viene rimosso, si ritiene sia necessario anche impedire che prodotti identici riappaiono subito dopo la rimozione. In questo modo si eviterebbe uno spreco di risorse per la piattaforma che pone in essere controlli e blocchi, per il tribunale che deve emettere un nuovo ordine per ciascun *listing* in violazione, per il titolare di diritto che con ingenti dispendi economici deve effettuare un monitoraggio costante e procedere a notificare le offerte illecite in maniera continuativa. Considerando la massa di dati a disposizione delle piattaforme (es. immagini del prodotto, storico e generalità del seller, dettagli dell'annuncio, etc.), e le comunicazioni di alcuni intermediari online che asseriscono la rimozione proattiva di migliaia di *listing* in violazione, è evidente che un meccanismo di c.d. "***stay-down***" risulti assolutamente fattibile sul piano pratico. Inoltre, la stessa Corte Europea di Giustizia ha affermato, nella causa "Eva Glawischnig-Piesczek v. Facebook Ireland Limited" (C- 18/18), che il diritto comunitario non impedisce a un fornitore di servizi di hosting come Facebook di rimuovere contenuti identici e, in alcune circostanze, equivalenti, precedentemente dichiarati illegali. Perciò, alle piattaforme può essere richiesto di rimuovere proattivamente i contenuti che sono stati precedentemente dichiarati illeciti, in perfetta compatibilità con l'assenza di monitoraggio generale previsto dall'Art. 7 della proposta in oggetto.

Accogliamo poi positivamente l'introduzione di meccanismi di **"*notice & take down*" più snelli e accessibili**, aggiungendo che sarebbe utile permettere di notificare il *seller* trasgressore e a cascata tutti i *listing*s cui questo fanno capo. In tale contesto, sarebbe altresì apprezzabile includere un **obbligo di informazione al consumatore** che abbia acquistato un prodotto illecito, rendendolo edotto della rimozione dell'annuncio e della ragione sottostante tale rimozione. Non si deve assumere che gli utenti siano sempre consapevoli della natura illegale dei beni che acquistano. Inoltre, sensibilizzare i consumatori sull'esistenza di prodotti illeciti sui canali online nei quali rimettono massima fiducia, significa renderli più attenti a futuri raggiri e contribuire a spezzare l'ultimo anello della catena del mercato illegale, che mette la merce direttamente nelle mani dell'utente finale.

Guardando alle misure di trasparenza previste a beneficio dei venditori circa la ragione della rimozione di un contenuto in seguito a notifica, si assiste ad una certa **asimmetria tra quanto richiesto al titolare di diritto che notifica un annuncio in violazione e il *seller*** che asserisce invece che la merce che vende è lecita, ponendo l'onere della prova in capo al primo, senza invece esigere lo stesso obbligo informativo dal secondo.

Inoltre, se da un lato risulta apprezzabile l'istituzione della categoria "**segnalatori affidabili**", dall'altro si ritiene opportuno includervi anche i titolari di diritto e non solo le organizzazioni che li rappresentano: nel caso della contraffazione, proprio i *brand owner* sono i soggetti in grado di confermare la natura autentica o meno del prodotto, velocizzando in tal mondo il processo di rimozione.

Per quanto concerne i **trasgressori recidivi**, si chiede che sia prevista, insieme alla sospensione, la possibilità di estromettere definitivamente dalla piattaforma il soggetto che abbia attuato reiterate

condotte illecite. Fare altrimenti significherebbe non porre alcun vero deterrente a chi agisce in maniera impropria sul web, mettendo in pericolo la salute e sicurezza degli utenti. Per la medesima ragione, tali soggetti non dovrebbero in alcun modo essere avvertiti, di nuovo, della loro imminente sospensione, mentre dall'altro lato chi subisce il danno spende ingenti risorse per contrastare la comparsa di prodotti illegali online, non solo a proprio beneficio, ma anche, se non soprattutto, per tutelare i consumatori. Obbligare le piattaforme ad una verifica dell'identità dei *seller* serve proprio a questo, per evitare che uno stesso soggetto con diversi account offra merce in violazione sottraendosi alle sanzioni e moltiplicando i guadagni.

La contraffazione rappresenta un fenomeno di portata globale, che altera la concorrenza, danneggia l'economia lecita e mette a rischio la salute e sicurezza dei consumatori, alimentando allo stesso tempo le casse della criminalità organizzata. Nel 2016 il valore della merce contraffatta circolante nel mondo era di quasi 510 miliardi di euro, di cui 121 miliardi riferiti al contesto europeo.
E Internet ha rappresentato un canale perfetto per incrementare gli affari illegali e dilatare i profitti. Per questo motivo la proposta DSA costituisce un'occasione unica per migliorare le regole alla base del mercato digitale. Un deciso cambio di rotta che meritano gli utenti che credono e investono nell'esperienza online, le imprese che si presentano in maniera legittima per offrire i propri beni e servizi e l'Europa stessa, per diventare presenza leader dell'era digitale.