La posizione di FIMI sulla proposta di regolamento del Digital Service Act (DSA)

FIMI, federazione dell'industria musicale italiana, rappresenta le principali imprese del settore discografico per un totale di oltre 2500 marchi tra i più famosi nella storia della musica internazionale ed italiana.

Come è noto, il mercato discografico è tra i settori che hanno più di ogni altro è stato protagonista della rivoluzione digitale, e le imprese associate a FIMI hanno sviluppato modelli di business innovativi con partner tecnologici che hanno portato oggi la quota di consumi online a rappresentare oltre l'80 % del totale con oltre 70 milioni di brani musicali a disposizione di oltre 150 milioni di fan abbonati ai servizi streaming.

Per tale motivo FIMI ritiene che se da un lato l'offerta digitale sia stata la grande protagonista della ripresa del settore, dall'altro resta fondamentale la tutela dei contenuti digitali e il ruolo delle piattaforme nel contrasto dell'illegalità.

INTRODUZIONE

La proposta della Commissione europea (la "Commissione") per un regolamento sui servizi digitali (la "proposta DSA") conferma la chiara intenzione della Commissione di garantire una maggiore responsabilità e trasparenza dei servizi digitali e di introdurre obblighi effettivi per contrastare i contenuti illegali online.

Siamo pienamente d'accordo con gli obiettivi della Commissione e riteniamo che la legislazione proposta fornisca un punto di partenza per raggiungerli.

Riconosciamo che la proposta DSA è uno strumento orizzontale che copre tutti i tipi di contenuti illegali e che mira tra l'altro a chiarire concetti generali rilevanti per il regime di responsabilità degli intermediari e ad armonizzare i processi volti a contrastare efficacemente i contenuti illegali. Sottolineiamo, tuttavia, che è fondamentale garantire che le norme proposte non peggiorino la situazione in nessun settore o rispetto a qualsiasi tipo di attività illegale, ad esempio rispetto alle violazioni del diritto d'autore.

Concordiamo con l'obiettivo della Commissione di preservare nel DSA il quadro dei principi chiave stabiliti nella direttiva UE sul commercio elettronico 2000/31 / CE (la "direttiva sul commercio elettronico").

È quindi essenziale non adottare interpretazioni o approcci che potrebbero rischiare di alterare inavvertitamente l'attuale quadro di responsabilità limitata.

La Commissione mira inoltre a rafforzare la responsabilità di tutti i tipi di servizi della società dell'informazione e ad aggiornare le loro responsabilità e obblighi per contrastare i contenuti illegali online in modo più efficace. Tuttavia, allo stato attuale, la proposta DSA non riesce a raggiungere questi obiettivi e quindi trarrebbe vantaggio da alcuni miglioramenti in queste aree.

SINTESI

1. **Il DSA deve preservare la portata del regime di responsabilità di cui agli articoli 12-14 della direttiva sul commercio elettronico.**

Sebbene la proposta DSA mantenga le categorie di servizi che possono essere idonee per la protezione del "safe harbour" (caching, mero conduit e hosting), il considerando 18 della proposta DSA implica una soglia più alta per stabilire che un servizio sta svolgendo un " ruolo attivo" e quindi non eleggibile per i privilegi dell'assenza di responsabilità. Ciò sarebbe incoerente con l'acquis dell'UE.

Qualsiasi chiarimento sulla distinzione tra intermediari "tecnici, automatici e passivi" e quelli che svolgono un "ruolo attivo" deve essere rigorosamente in linea con l'acquis comunitario esistente, in modo da evitare di ampliare l'applicazione dei "safe harbour".

2. **Il DSA non deve diluire le condizioni per l'idoneità al "safe harbour".**

Una volta che un servizio ha soddisfatto i criteri di ammissibilità della soglia, deve soddisfare determinate condizioni per godere dei privilegi di responsabilità "safe harbour". Queste condizioni non devono essere diluite.

Una condizione cruciale esistente per quanto riguarda i fornitori di hosting e stabilita nell'articolo 14 della direttiva sul commercio elettronico è che il fornitore di servizi non deve avere alcuna conoscenza o consapevolezza effettiva delle attività illegali. La conoscenza

effettiva è chiaramente uno standard diverso dalla consapevolezza, o cosiddetta "conoscenza costruttiva". È essenziale che questi standard non siano confusi.

La proposta di DSA sembra fondere la conoscenza effettiva con la consapevolezza, con l'effetto di aumentare la soglia per stabilire che un servizio è a conoscenza di attività illegali. Ciò amplierebbe l'applicazione del "safe harbour", il che sarebbe contrario agli obiettivi dichiarati della Commissione e altamente dannoso per qualsiasi individuo o entità che cerchi di impedire la diffusione di contenuti illegali.

3. **Il DSA dovrebbe includere obblighi positivi significativi per tutti i servizi della società dell'informazione.**

Per aumentare l'efficacia delle misure per bloccare e prevenire i contenuti illegali online, tutti i servizi digitali devono fare di più. Per raggiungere questo obiettivo, la proposta DSA dovrebbe:

- **Applicare gli opportuni obblighi positivi a tutti i servizi della società dell'informazione** che consentono o facilitano il funzionamento di siti web illegali fornendo loro servizi o mezzi per operare.

- **Introdurre un obbligo di "stay down" per i servizi di hosting**. Il "notice & take down" è inefficace per proteggere i titolari dei diritti. È necessario un obbligo di "stay down" per trovare il giusto equilibrio tra la necessità di fermare le attività illegali online e la necessità degli intermediari online di certezza commerciale.

- **Migliorare le disposizioni sui "segnalatori attendibili" (trusted flaggers) per fornire vantaggi significativi ai "segnalatori attendibili"**, obbligando tutti i servizi, compresi quelli micro e piccoli, ad accettare i loro avvisi "alla lettera", per agire immediatamente e, se disponibili, per fornire accesso a strumenti gratuiti per aiutare a individuare contenuti illegali su larga scala (ad esempio, un'interfaccia di programmazione dell'applicazione ("API")).
- **Migliorare le disposizioni in materia di recidiva per imporre a tutti i servizi della società dell'informazione che consentono o facilitano attività illegali di adottare e attuare efficacemente una politica adeguata per i trasgressori recidivi.**
- **Ampliare l'obbligo di "KYBC – know your business customer" a tutti i servizi della società dell'informazione** (non solo i mercati online e le micro e piccole imprese) e fornire un meccanismo per consentire alle persone interessate di accedere a tali informazioni, in modo tempestivo e su larga scala, per scopo di indagare sugli autori di attività illegali e far valere i loro diritti.

4. **Il DSA dovrebbe chiarire che la disposizione sulle misure proattive volontarie (articolo 6) si applica alle attività intraprese esclusivamente per rilevare, identificare e intraprendere azioni contro i contenuti illegali.**

Sebbene siamo d'accordo con l'approccio proposto dalla Commissione per rimuovere i disincentivi affinché i servizi adottino misure proattive per identificare e rimuovere i contenuti illegali, tale disposizione deve essere chiaramente definita per quanto riguarda la

sua portata ed effetto, per evitare che venga abusata dai servizi e diventi una nuova forma di "safe harbour".

5. **Gli obblighi positivi ai sensi del DSA dovrebbero essere associati a misure di applicazione efficaci.**

Sebbene i siti web pirata operino indiscriminatamente in tutta Europa, i titolari dei diritti devono agire paese per paese in base al sistema legale di ciascuno Stato membro. I titolari dei diritti e le altre parti lese dovrebbero avere accesso a meccanismi di ingiunzione efficaci in tutta l'UE, senza la necessità che alcun individuo o entità, che stia cercando di fermare o impedire la diffusione di contenuti illegali, di intraprendere azioni in ogni singolo Stato membro contro lo stesso servizio illegale, la stessa attività illecita o contenuto in violazione.

La proposta non include alcuna disposizione significativa riguardo alla questione citata. Attendiamo con impazienza di collaborare con il colegislatore dell'UE per migliorare la proposta a tale riguardo.

FEDERAZIONE INDUSTRIA MUSICALE ITALIANA

IV. COMMENTI DETTAGLIATI

1. **Il DSA deve mantenere i criteri di qualificazione esistenti per i privilegi di responsabilità.**

Sebbene la proposta DSA non modifichi sostanzialmente l'ambito di applicazione del regime di responsabilità, che è stato stabilito nella direttiva sul commercio elettronico, implica una soglia ridotta per stabilire che un servizio è idoneo per i privilegi di responsabilità `` safe harbour '', quindi potenziale estendendo il loro campo di applicazione. Questi elementi, descritti di seguito, devono essere affrontati, in modo da mantenere l'equilibrio esistente nell'acquis dell'UE.

1.1 Il DSA dovrebbe mantenere categorie di servizi che possono essere ammissibili al regime di responsabilità dell'intermediario.

Come punto di partenza, siamo d'accordo con la proposta della Commissione di non modificare le categorie di servizi intermedi ammissibili per i `` safe harbour '' (servizi di `` mere conduit '', `` caching '' e `` hosting '') (capitolo II, articoli 3-5 la proposta DSA), come attualmente stabilito nella direttiva sul commercio elettronico.

1.2 Il DSA non deve modificare l'ambito o l'applicazione del regime di responsabilità dell'intermediario.

La direttiva sul commercio elettronico stabilisce privilegi di responsabilità per determinati tipi di servizi (servizi di "mere conduit", "memorizzazione nella cache" e "hosting"), ma l'idoneità

per le limitazioni di responsabilità non si pone semplicemente perché il servizio rientra nel "semplice trasporto", "memorizzazione nella cache" e "servizi di hosting".

Per essere ammissibili, le attività di un servizio devono essere, come affermato nel considerando 42 della direttiva sul commercio elettronico e riflesso nel considerando 18 della proposta DSA, "di ordine meramente tecnico, automatico e passivo, il che implica che il prestatore di servizi della società dell'informazione non conosce né controlla le informazioni trasmesse o memorizzate.", vale a dire che il servizio non dovrebbe svolgere un ruolo attivo. Nelle cause Google France (cause riunite da C-236/08 a C-238/08), la CGUE ha affermato che l'articolo 14 della direttiva sul commercio elettronico si applica laddove il fornitore di servizi "non abbia svolto un ruolo attivo di tipo per dargli la conoscenza o il controllo sui dati memorizzati…". La CGUE ha inoltre stabilito nella causa L'Oréal / eBay (C-324/09) che un servizio svolge un "ruolo attivo di un tipo tale da consentirle di conoscere o controllare i dati relativi a tali offerte di vendita [...] non può quindi invocare, nel caso di tali dati, l'esenzione dalla responsabilità di cui all'articolo 14, paragrafo 1, della direttiva 2000/31 / CE". Questi principi sono stati applicati anche dai tribunali degli Stati membri.

È essenziale che il DSA mantenga il criterio di ammissibilità "tecnico, automatico e passivo" e non alteri in alcun modo la soglia per stabilire che le attività di un fornitore di servizi non sono meramente tecniche, automatiche e passive. La modifica della soglia potrebbe effettivamente ampliare la portata dei privilegi di responsabilità, il che andrebbe contro l'obiettivo della proposta DSA di preservare il regime di responsabilità stabilito nella direttiva

sul commercio elettronico e porterebbe infine a una minore e non maggiore responsabilità dei servizi.

1.3 Alcuni aspetti della proposta di DSA potrebbero essere interpretati come implicanti una soglia più alta per stabilire che un servizio sta svolgendo un "ruolo attivo".

Considerando 18 della proposta DSA.

Appoggiamo la prima parte del considerando 18, che riflette il considerando 42 della direttiva sul commercio elettronico e la decisione della CGUE in L'Oréal / eBay e intende confermare quali servizi sarebbero ammissibili per il regime di responsabilità mantenendo la distinzione tra servizi attivi e passivi.

Tuttavia, la seconda parte del considerando 18 è preoccupante perché potrebbe - involontariamente - aumentare la soglia per stabilire un "ruolo attivo". Mentre l'affermazione in questa parte è evidentemente corretta in quanto fornisce due esempi di attività che indubbiamente imputerebbero un "ruolo attivo", è facilmente fraintesa come un'alta soglia per stabilire quando un servizio svolge un ruolo attivo. La CGUE ha già confermato quale tipo di relazione con il contenuto caricato è sufficiente per imputare al servizio un ruolo attivo e quindi per squalificarlo dall'idoneità ai privilegi del safe harbour. Nella sentenza L'Oreal / eBay, la Corte ha considerato un ruolo attivo la prestazione di "assistenza che comporta, in particolare, l'ottimizzazione della presentazione delle offerte di vendita in questione o la promozione di tali offerte".

Se la proposta del DSA intende fornire esempi di attività che precluderebbero l'applicazione del regime di responsabilità, dovrebbe farlo codificando le parti pertinenti della giurisprudenza della CGUE (in particolare L'Oréal contro eBay). Non dovrebbe fornire esempi che potrebbero essere erroneamente interpretati come implicanti una soglia più alta per stabilire un ruolo attivo.

I chiarimenti proposti dalla Commissione nel considerando 18 della proposta DSA si basano su un'analisi viziata nella valutazione d'impatto della Commissione ("IA").

Quando si cerca di affrontare il problema percepito secondo cui la distinzione tra ruoli attivi e passivi non è chiara, la Commissione sembra basarsi sulla seguente analisi, che illustra un malinteso della distinzione tra attività attive e passive:

"[...] *esiste ancora un'importante incertezza su quando si consideri che un intermediario, e in particolare un fornitore di servizi di hosting, abbia svolto un ruolo attivo tale da portare alla conoscenza o al controllo dei dati che ospita. Il fatto che non esista un "hosting attivo", ma che un provider possa svolgere un ruolo attivo per quanto riguarda alcuni contenuti, ma non altri (ad esempio perché li presenta o li consiglia in modo speciale) non porta alla necessaria certezza del diritto per fornire servizi di intermediazione legale senza rischiare richieste di risarcimento danni o addirittura responsabilità penale* ". (IA, allegato 9, p 159, corsivo aggiunto) La Commissione fa quindi affermazioni sulla distinzione che non ha alcun fondamento nell'acquis dell'UE:

"La Corte ha interpretato la condizione per i servizi di hosting come" un ruolo passivo e neutrale ", come indicato nel considerando 42 della direttiva sul commercio elettronico per mere conduit e servizi di caching – e i tribunali nazionali hanno successivamente applicato questa giurisprudenza in modi contraddittori. In questo contesto, alcuni tribunali nazionali hanno equiparato il `` ruolo attivo (di tipo tale da conferirgli conoscenza o controllo) '' con una sorta di ``appropriazione *''del contenuto (`` zu eigen machen '') nella misura in cui un utente ragionevolmente informato potrebbe concludere che la piattaforma è l'autore o il responsabile di tali contenuti. Un'interpretazione simile è stata proposta di recente anche dall'avvocato generale Saugmandsgaard in una causa attualmente pendente dinanzi alla Corte. Quando viene applicato ai fornitori di servizi di hosting, è importante creare certezza giuridica e garantire che questo requisito non possa implicare che l'ordinamento, la visualizzazione, la marcatura o l'indicizzazione automatizzati tramite algoritmi dei contenuti archiviati, attività che sono oggi necessarie per rendere tali contenuti completamente reperibili, implichino un ruolo attivo.* " (IA, p. 112, corsivo aggiunto).

Siamo fortemente in disaccordo con questa interpretazione.

In primo luogo, la Commissione fa un indebito affidamento sulla decisione del tribunale tedesco (OLG Monaco) nella causa GEMA / YouTube e sulle conclusioni dell'avvocato generale nella causa Peterson / YouTube della CGUE. Questo test di "appropriazione" non fa parte dell'acquis dell'UE e quindi non dovrebbe essere incluso nel DSA (come apparentemente è attraverso la seconda parte del considerando 18 proposto). Invece, il DSA

dovrebbe seguire la giurisprudenza della CGUE, in particolare la decisione L'Oreal / eBay4, in cui la Corte ha confermato che i servizi che hanno conoscenza o controllo del contenuto - che si manifesta ad esempio ottimizzando la presentazione del contenuto o promuovendola - svolgono un ruolo attivo e non possono beneficiare dei privilegi di responsabilità nella direttiva sul commercio elettronico. La Corte non fa alcun riferimento nella sua decisione al test di "appropriazione".

Il tentativo di escludere "l'ordinamento automatico, algoritmico, la visualizzazione e la marcatura o l'indicizzazione del contenuto che memorizza, attività che sono oggi necessarie per rendere tale contenuto completamente individuabile" dall'implicare un ruolo attivo è altamente discutibile. Queste attività possono infatti essere necessarie per rendere i contenuti "reperibili", ma non sono coerenti con le attività meramente tecniche, automatiche e passive di un mero hosting provider. Al contrario, sono attività che ottimizzano in modo più efficace la presentazione dei contenuti, che secondo la CGUE dovrebbero squalificare un fornitore di servizi dall'idoneità al privilegio di responsabilità.5

2. Il DSA non deve diluire le condizioni per l'idoneità del "safe harbour" per i servizi di hosting.

2.1 Conoscenza e consapevolezza di attività illegali o contenuti illegali.

Come condizione per l'esenzione di responsabilità, la direttiva sul commercio elettronico e la proposta di DSA prevedono ciascuna che il fornitore di servizi di hosting non deve avere una conoscenza effettiva di attività illegali o contenuti illegali e, per quanto riguarda le richieste di risarcimento danni, non è a conoscenza dei fatti o circostanze da cui è evidente l'attività illegale o il contenuto illegale, o dopo aver ottenuto tale conoscenza o consapevolezza, agisce rapidamente per rimuovere o disabilitare l'accesso al contenuto illegale (articolo 5 della proposta DSA). Nella prima sezione di questo documento, affrontiamo la questione della "conoscenza o controllo" nel contesto della distinzione tra servizi attivi e passivi. In questa sezione trattiamo le circostanze in cui può sorgere una conoscenza o consapevolezza effettiva allo scopo di attivare l'obbligo di cui all'articolo 5 proposto di agire rapidamente per rimuovere o disabilitare l'accesso al contenuto illegale. La conoscenza effettiva è chiaramente uno standard diverso dalla consapevolezza. È essenziale che questi standard non siano confusi, poiché ciò aumenterebbe probabilmente la soglia per stabilire che un fornitore di servizi ha una "consapevolezza" tale da far scattare l'obbligo di rimuovere il contenuto in violazione, in mancanza del quale verrà privato dall'esenzione di responsabilità o safe harbour. Tuttavia, il considerando 22 proposto sembra confondere questi standard a scapito dei titolari dei diritti. Questo considerando cita due esempi di eventi che potrebbero

innescare una conoscenza o consapevolezza effettiva: un'indagine o un avviso. Come per il considerando 18, questi esempi implicano una soglia elevata per stabilire la consapevolezza. Con una corretta costruzione, la consapevolezza potrebbe sorgere senza un'indagine o il preavviso del titolare dei diritti.

Tuttavia, le dichiarazioni della Commissione nella valutazione d'impatto indicano che la Commissione ritiene che la notifica di un titolare del diritto possa essere necessaria per innescare la consapevolezza:

"Quando un fornitore di servizi di hosting riceve un avviso su un contenuto presumibilmente illegale che memorizza, non dovrebbe essere ritenuto responsabile anche se tale avviso ha attivato" conoscenza effettiva "o" consapevolezza "di tale illegalità purché abbia intrapreso un'azione rapida ai sensi del ECD. Tuttavia, non è chiaro cosa sia necessario affinché un avviso attivi tale consapevolezza. C'è anche incertezza sull'acquisizione di una conoscenza effettiva o consapevolezza di contenuti illegali come risultato delle azioni volontarie del fornitore, come spiegato sopra. ""*La formulazione dell'articolo 14, paragrafo 1, lettera a), ECD indica che, affinché il test di sensibilizzazione sia soddisfatto, i fatti e le circostanze in questione devono essere tali che l'illegittimità sia evidente; un caso di illegalità borderline in genere non sembra sufficiente a portare alla "consapevolezza" ai sensi dell'articolo 14, paragrafo 1, lettera a). Una procedura di avviso e azione ben strutturata dovrebbe fornire certezza giuridica a tutte le parti coinvolte per essere efficace e completa* ". (IA, allegato 9, pagina 161, corsivo aggiunto).

Per evitare di fondere conoscenza e consapevolezza effettive, suggeriamo di rimuovere il riferimento alla consapevolezza dal considerando 22 proposto.

2.2 Azioni volontarie / rimozione dei disincentivi.

Siamo ampiamente d'accordo con l'approccio proposto dalla Commissione di chiarire che un fornitore di servizi non dovrebbe essere escluso dall'idoneità ai privilegi del “safe harbour" in ragione del semplice fatto che un fornitore di servizi intraprende attività per rilevare, identificare e agire contro i "contenuti illegali". Tuttavia, dovrebbe essere chiarito che tali attività dovrebbero essere esclusivamente a tali fini. Questo è importante, in modo da evitare che attività che hanno anche altri scopi vengano automaticamente ignorate dalla valutazione dell'idoneità del fornitore di servizi.

2.3 Il DSA dovrebbe consentire flessibilità nel meccanismo di avviso e azione e garantire requisiti non gravosi per gli avvisi.

I meccanismi di avviso e azione proposti dovrebbero fornire maggiore flessibilità per i diversi tipi di servizi e contenuti, per tenere conto della natura orizzontale del quadro DSA. Dovrebbero anche consentire specificamente la notifica di più contenuti.

Inoltre, i requisiti per le notifiche di contenuti illegali non dovrebbero introdurre requisiti nuovi e onerosi o requisiti che renderebbero impraticabile il processo. Ciò dovrebbe tener conto dell'elevato volume di violazioni segnalate dai titolari dei diritti. A titolo illustrativo, i titolari di diritti, tramite IFPI e DCP, in Italia, hanno notificato quasi 200 milioni di violazioni dal 2012 su tutte le piattaforme monitorate. Inoltre, i requisiti dovrebbero essere

sufficientemente ampi da comprendere tutti i tipi di contenuto e, per quanto possibile, essere a prova di futuro. Questi principi dovrebbero applicarsi a tutti gli obblighi di notifica ai sensi dell'articolo 14 proposto.

A titolo di esempio, un requisito obbligatorio di fornire un URL (un indirizzo a una risorsa su Internet) imporrebbe al notificante un onere eccessivo per identificare ogni istanza dello stesso contenuto illegale e consentirebbe effettivamente ai servizi di hosting di non essere obbligate a rimuovere tutte le copie in violazione dai loro servizi (ad esempio eseguendo una scansione per le violazioni già esistenti) e implica che tutto ciò che è richiesto è la rimozione della violazione all'URL specifico, quando il fornitore di servizi potrebbe essere obbligato a fare di più. In alcuni casi, un URL non fornisce una posizione precisa per una specifica violazione (ad esempio in un live streaming o su un'app). Un URL dovrebbe essere sufficiente, ma non un mezzo necessario per identificare il contenuto illegale in un avviso.

L'articolo 14, paragrafo 3, della proposta di DSA prevede che gli avvisi conformi ai requisiti di cui all'articolo 14, paragrafo 2, siano considerati suscettibili di effettiva conoscenza o consapevolezza ai fini dell'articolo 5 in merito alla specifica informazione in questione. Come notato nella sezione 2.1 sopra, ciò non dovrebbe portare alla fusione dei concetti di "conoscenza" e "consapevolezza"; dovrebbe essere chiaro che un avviso non è necessario per ottenere la consapevolezza di illegale contenuto o attività e un avviso può dar luogo a conoscenza o consapevolezza di contenuti o attività illegali in un luogo diverso dagli URL specificati in un avviso.

L'azione richiesta ai fornitori di servizi di hosting a seguito del ricevimento di una comunicazione di cui all'articolo 14, paragrafo 6, consiste nel trattare le comunicazioni e prendere decisioni "in modo tempestivo, diligente e obiettivo". Ciò è incoerente e diluisce i criteri di ammissibilità per l'hosting "porto sicuro" ai sensi dell'articolo 5 (1) (b), vale a dire "dopo aver ottenuto tale conoscenza o consapevolezza, agisce rapidamente per rimuovere o disabilitare l'accesso al contenuto illegale".

3. Il DSA dovrebbe includere obblighi positivi significativi per tutti i servizi della società dell'informazione.

3.1 Gli obblighi positivi dovrebbero applicarsi a una più ampia categoria di servizi.

Il campo di applicazione del DSA proposto è limitato ai fornitori di servizi di intermediazione che rientrano negli articoli 3 - 5 della proposta DSA (rispettivamente articoli 12-15 della direttiva sul commercio elettronico). Tuttavia, ci sono molti altri servizi digitali, che facilitano l'attività illegale online, compresa la violazione del copyright, e che esulerebbero dal suo campo di applicazione.

Per aumentare l'efficacia delle misure per bloccare e prevenire i contenuti illegali online, che è l'obiettivo del DSA, tutti i servizi digitali devono fare di più. Per raggiungere questo obiettivo, la proposta DSA dovrebbe:

• Applicare obblighi positivi non solo ai servizi di intermediazione ai sensi del DSA proposto, ma anche ad altri servizi che consentono o facilitano il funzionamento di siti web illegali

fornendo loro servizi o mezzi per operare. Tutti i servizi della società dell'informazione, che vengono utilizzati per fornire contenuti illegali, ad esempio, registri / registrar di nomi di dominio, fornitori di servizi CDN, fornitori di pagamenti, reti pubblicitarie, dovrebbero essere obbligati ad adottare misure ragionevoli per fermare, limitare e prevenire attività illegali. Il contenuto di tali obblighi dovrebbe dipendere dai tipi di servizio. Tuttavia, alcuni obblighi possono essere applicati a tutti i tipi di intermediari, come le politiche "recidivi" e gli obblighi "Know Your Business Customer" (KYBC).

Gli obblighi in materia di tracciabilità ("Conosci il tuo cliente aziendale") e "trasgressori recidivi", così come la disposizione di Segnalatori attendibili dovrebbero essere significativi, e dovrebbero applicarsi alle micro e piccole imprese. Ad esempio, alcuni degli intermediari online utilizzati da servizi illegali sono relativamente piccoli e a volte lavorano in combutta con altri piccoli facilitatori di attività illegali. Nel contesto dei fornitori di servizi di hosting, abbiamo visto operare hosting a prova di proiettile nelle reti di piccoli ISP. Inoltre, è comune per i piccoli ISP di nicchia rivendere i server a provider più grandi e, in alcuni casi, operatori di servizi in violazione affittano server per gestire efficacemente il proprio ISP.

3.2 Obbligo di "stay down" per i servizi di hosting.

La semplice rimozione di contenuti specifici non è più sufficiente per prevenire la messa a disposizione di contenuti in violazione su larga scala e non dovrebbe, da sola, garantire l'eleggibilità per i priviliegi del safe harbor agli ISP. Per fare un esempio, sulla base dei dati di IFPI del 2018, l'88% delle notifiche per la rimozione inviate, si riferivano a opere già notificate in passato allo stesso intermediario. Una volta a conoscenza dei contenuti o delle attività illegali o raggiunta la consapevolezza dei motivi per cui un contenuto risulta illegale, gli hosting provider dovrebbero avere l'obbligo di (i) rimuovere o disabilitare l'accesso a tutte le copie delle opere illegali e (ii) assicurarsi che le stesse opere non vengano messe nuovamente a disposizione.

La Commissione rende noto che gli ordini di "stay down" emessi dalle Corti nazionali sono parte integrante della giurisprudenza comunitaria.Le Corti nazionali in Italia, in Germania e in altri stati membri, così come la CJEU hanno disposto obblighi di "stay down" in relazione a casi di violazione del copyright e in casi di diffamazione online.

Si tratta di un obbligo appropriato e proporzionato che può essere applicato tramite una serie di diversi mezzi, inclusi i già diffusi sistemi di riconoscimento automatici (ACR).

3.3 Vantaggi significativi per i "Segnalatori attendibili" (trusted flaggers)

L'introduzione del concetto di "segnalatori attendibili" è benvenuta, ma dovrebbe offrire vantaggi reali a coloro a cui viene concesso questo status e non dovrebbe diminuire gli obblighi dei prestatori di servizi in relazione agli avvisi presentati al di fuori di questo regime. L'articolo 19, paragrafo 1, della proposta di DSA prevede che le piattaforme online adottino le misure tecniche e organizzative necessarie per garantire che le comunicazioni presentate da "segnalatori attendibili" attraverso i meccanismi di cui all'articolo 14 siano trattate e decise "con priorità e senza indugio ". Grazie al loro stato di fiducia, dovrebbero essere in grado di richiedere la rimozione immediata dei contenuti e i fornitori di servizi dovrebbero accettare le loro notifiche al valore nominale e, se disponibili, fornire accesso a strumenti gratuiti per aiutare a individuare contenuti illegali in scala (ad esempio, un'API) .

3.4 "Politiche per violazioni ripetute" solide.

L'articolo 20 della proposta DSA stabilisce che "le piattaforme online sospendono, per un periodo di tempo ragionevole e previo avviso, la fornitura dei loro servizi ai destinatari del servizio che forniscono frequentemente contenuti manifestamente illegali".

L'obbligo di attuare un'efficace politica sul "recidivo" dovrebbe applicarsi a tutti gli intermediari e non solo alle piattaforme online. Se un intermediario sa o viene a conoscenza che un destinatario dei suoi servizi (sia un rivenditore che un utente finale) ha utilizzato ripetutamente i suoi servizi in relazione ad attività illecite, deve anche, in circostanze appropriate, interrompere la fornitura dei propri servizi a tale destinatario. Ciò dovrebbe

applicarsi a tutte le istanze di contenuto illegale, senza il requisito aggiuntivo che sia "manifestamente" illegale.

La politica del "recidivo" dovrebbe essere applicata con il vero obiettivo di prevenire e scoraggiare l'uso dei servizi in relazione ad attività illegali ripetute e sistematiche. Gli intermediari devono assicurarsi di disporre di misure adeguate per individuare i trasgressori recidivi. Nel valutare se un utente è un `` recidivo '', è necessario tenere conto di tutti i casi di attività illegale da parte di tale utente, indipendentemente dal fatto che i casi di illegalità siano stati rimossi e nel contesto dell'articolo 20, paragrafo 1, ciò dovrebbe essere in riferimento alla quantità assoluta di contenuto illegale e non alla proporzione relativa di cui all'articolo 20, paragrafo 3, lettera b).

Questo processo di verifica ai sensi dell'articolo 22, paragrafo 2, della proposta DSA (vedere di seguito) dovrebbe garantire che qualsiasi utente che è stato sospeso dalla piattaforma in base alla politica del "trasgressore recidivo" non sia autorizzato a utilizzare il servizio, anche con un nome diverso.

I termini di servizio degli intermediari online dovrebbero consentire e definire in modo chiaro e trasparente il diritto e la discrezione dell'intermediario di sospendere e terminare i trasgressori recidivi in conformità con i principi di cui sopra.

3.5 Obbligo più ampio di "Conosci il tuo cliente aziendale" ("KYBC").

L'applicazione dell'obbligo di "tracciabilità dei professionisti" (articolo 22 della proposta DSA) ai mercati online sarebbe una soluzione incompleta. Questo è così perché, in primo luogo, è di portata troppo ristretta. Per rendere gli obblighi di KYBC veramente efficaci, non dovrebbero essere limitati alle piattaforme che comprendono mercati online.

I contenuti illegali sono disponibili tramite una serie di fonti online e spesso non vengono "venduti" ma piuttosto monetizzati tramite pubblicità o abbonamenti. Inoltre, la fornitura di contenuti digitali illegali si basa inevitabilmente sui servizi di altri intermediari per l'infrastruttura e supporto, ad esempio, registrar / registri di domini, fornitori di servizi di hosting, app store, rete di distribuzione di contenuti e fornitori di sistemi di pagamento. Pertanto, tutti questi intermediari dovrebbero essere soggetti a tale obbligo.

È inoltre essenziale che le informazioni fornite ai sensi dell'articolo 22, paragrafo 1, della proposta di DSA siano verificate non solo al momento della ricezione, ma anche periodicamente per tutto il tempo in cui l'utente continua a ricevere i servizi dell'intermediario.

Un obbligo KYBC deve essere accompagnato da una base per consentire alle persone interessate di accedere a tali informazioni, in modo tempestivo e su larga scala, allo scopo legittimo di indagare sugli autori di attività illegali e far valere i loro diritti (vedere la sezione 3.6 di seguito). L'accesso alle informazioni ai sensi dell'articolo 22, paragrafo 5, della proposta

di DSA non dovrebbe impedire a un intermediario di fornire volontariamente l'accesso alle informazioni, a condizione che sia in grado di farlo in conformità con la legge applicabile.

3.6 Base giuridica per un registro pubblico dei registranti di domini.

A seguito dell'entrata in vigore del GDPR, l'Internet Cooperation for Assigned Names and Numbers (ICANN) 12 ha introdotto una specifica temporanea per WHOIS che richiede ai registrar e ai registri di oscurare la stragrande maggioranza dei dati WHOIS relativi ai registranti di domini europei (indipendentemente dal fatto che siano naturali o legali persone). Il risultato è stato un ritiro quasi totale del registro WHOIS pubblico che ha avuto un impatto significativo sulla nostra capacità di ottenere i dati necessari per le nostre azioni di contrasto e contenzioso. Sono in corso discussioni presso l'ICANN per sviluppare un "modello di accesso", ma c'è una mancanza di fiducia tra le parti interessate riguardo a questo processo e alle prospettive di arrivare a una soluzione praticabile.

È urgentemente necessario un intervento legislativo per chiarire l'interesse pubblico in un registro WHOIS pubblico. Pertanto, il DSA dovrebbe includere una base giuridica esplicita per un registro WHOIS pubblico che dovrebbe, come minimo, contenere tutti i dati già necessari per essere resi disponibili al pubblico ai sensi dell'articolo 5 della direttiva sul commercio elettronico. Attualmente, non esiste nemmeno una base esplicita proposta per l'accesso alle informazioni WHOIS da parte di persone o entità interessate (ad es. Organizzazioni e società del settore privato) per lo scopo legittimo di indagare e far rispettare le attività illegali.

4. Il DSA dovrebbe confermare che è consentito un monitoraggio specifico.

Concordiamo con la proposta della Commissione volta a chiarire che il divieto di obblighi generali di monitoraggio (a) non preclude a un servizio di effettuare un monitoraggio generale di propria iniziativa eb) non preclude l'obbligo per i servizi di effettuare un monitoraggio specifico (considerando 28 della proposta DSA).

4.1 Riferimento inutile e non necessario alla sussidiarietà.

Una caratteristica essenziale del regime di responsabilità dell'intermediario nella direttiva sul commercio elettronico è che i titolari dei diritti o altre vittime di attività illegali possono chiedere un provvedimento ingiuntivo nei confronti di un intermediario. Ciò è descritto nel considerando 45 della direttiva sul commercio elettronico e negli stessi articoli 12-14.

Ciò riflette la realtà che il fornitore di servizi intermediario è spesso nella posizione migliore per terminare o prevenire attività illegali sul suo servizio e le difficoltà pratiche legate al perseguimento degli operatori di servizi impegnati in attività illegali, poiché spesso nascondono deliberatamente la loro identità usando i molti strumenti, compresi i servizi di intermediazione, disponibili nell'ambiente online.

Sebbene la bozza di DSA non modifichi le norme esistenti a tale riguardo, l'affermazione al considerando 26 che "ove possibile, le terze parti interessate da contenuti illegali trasmessi o archiviati online dovrebbero tentare di risolvere i conflitti relativi a tali contenuti senza coinvolgere i fornitori di servizi di intermediazione in domanda ”potrebbe essere frainteso e

interpretato come l'introduzione di una nuova condizione per la concessione di provvedimenti inibitori nei confronti degli intermediari online. In quanto tale, il considerando non solo è inutile, ma è anche inutile.

5. Gli obblighi positivi ai sensi del DSA dovrebbero essere associati a misure di esecuzione efficaci che abbiano effetto transfrontaliero.

5.1 Il problema.

Il provvedimento ingiuntivo è un rimedio fondamentale per i titolari dei diritti sia per quanto riguarda i servizi illegali sia per i servizi di intermediazione che supportano la funzionalità o l'accesso a servizi illegali, ma l'efficacia del rimedio è attualmente compromessa in molti Stati membri perché, mentre i siti web non autorizzati operano indiscriminatamente in tutta Europa, i titolari dei diritti devono agire Stato membro per Stato membro o, se è possibile un'unica azione, per far valere e dimostrare l'illegalità ai sensi della legislazione nazionale di ciascuno Stato membro applicabile14. Ciò è lento e costoso in modo proibitivo per la maggior parte dei titolari di diritti. Inoltre, i sistemi giuridici europei non consentono in modo uniforme ai titolari dei diritti di cercare ingiunzioni "dinamiche" o "a catalogo", rendendo irragionevolmente difficile per i titolari dei diritti proteggere efficacemente i propri diritti in tutta Europa.

L'attuale regime non solo impone un enorme onere ai titolari dei diritti come descritto sopra, ma aggiunge anche inutilmente costi e risorse al carico di lavoro dei tribunali degli Stati

membri in tutta l'Unione europea, con conseguente perdita di tempo. Fondamentalmente, l'assenza di ingiunzioni transfrontaliere è anche intrinsecamente pregiudizievole per il corretto funzionamento del mercato interno.

Sebbene il progetto di DSA preveda la condivisione degli ordini e la cooperazione transfrontaliera tra i coordinatori dei servizi digitali in determinate circostanze15, non fornisce una soluzione agli ostacoli al rispetto dei diritti all'interno dell'UE.

5.2 Possibili soluzioni.

Il DSA potrebbe migliorare la situazione introducendo misure che potrebbero contribuire a garantire l'effetto transfrontaliero di alcune misure protettive e preventive.

In caso di richieste di ingiunzioni di terzi "senza colpa" (disponibili ai sensi del diritto dell'UE applicabile) relative allo stesso servizio non autorizzato ma diversi intermediari rispondenti nazionali, il DSA dovrebbe autorizzare gli Stati membri a introdurre procedure accelerate per garantire che la stessa categoria di intermediari online adotterà le stesse misure in relazione allo stesso servizio in violazione. Ciò potrebbe verificarsi all'interno di un procedimento giudiziario nazionale in cui le sentenze di altri Stati membri dell'UE sono utilizzate come base per la concessione di ingiunzioni simili.16 Gli stessi risultati potrebbero essere ottenuti anche attraverso procedure amministrative che coinvolgono le agenzie competenti che ordinano agli intermediari interessati di adottare tali misure nei rispettivi paesi.

A titolo di esempio, si potrebbe ottenere un'applicazione transfrontaliera più efficace sviluppando ulteriormente le disposizioni relative alla cooperazione tra le autorità di contrasto (ad esempio, ai sensi dell'articolo 8 della proposta DSA), compresi i coordinatori dei servizi digitali, stabilendo procedure accelerate per l'uso / riconoscere ingiunzioni di altri Stati membri. Tuttavia, il problema immediato di tale articolo è che sembra concentrarsi solo su elementi specifici di contenuto illegale17, il che rende l'ambito di applicazione di questa disposizione molto limitato e dovrà essere modificato.

Inoltre, vi è un pericolo nell'approccio "soluzione unica" al contenuto degli ordini delle autorità giudiziarie ai sensi dell'articolo 8, paragrafo 2, della proposta DSA. Soprattutto per il fatto che che i requisiti sono molto prescrittivi, ad esempio, per quanto riguarda l'inclusione di URL che consentono l'identificazione di contenuti illegali specifici. A causa della natura orizzontale dei DSA, questa disposizione sarebbe applicata a molti diversi tipi di attività e contenuti illegali. Nelle circostanze che prescrivono il contenuto degli ordini, come proposto nell'articolo 8, paragrafo 2, non solo è inutile, ma anche inefficace, in quanto non tiene conto delle differenze rilevanti tra le attività e il contenuto in questione.

Esiste anche il rischio di creare confusione laddove esistono già regole e procedure specifiche che si applicano a una particolare area (ad esempio, nel caso del rispetto dei diritti di proprietà intellettuale). L'articolo 8, paragrafo 2, della proposta DSA non deve limitare l'applicazione dei diritti di proprietà intellettuale e la portata dei rimedi disponibili in caso di violazione di tali diritti. Un altro esempio potrebbero essere le disposizioni riguardanti gli

obblighi e i poteri dei coordinatori dei servizi digitali, che potrebbero costituire una base per introdurre norme più solide riguardo a misure aventi un effetto `` transfrontaliero '', in particolare l'uso e / o il riconoscimento di prove provenienti da altri Stati membri .18

5.3 Ingiunzioni dinamiche e di catalogo.

I titolari dei diritti devono avere la possibilità di ricorrere a misure che:

a) sono sufficientemente flessibili da rimanere efficaci nel tempo, vale a dire ingiunzioni o altre misure che coprono la fornitura di un servizio online in violazione senza essere limitate a posizioni online specifiche (URL / domini) in quanto potrebbero facilmente cambiare; e

b. coprire l'intero catalogo del titolare del diritto (al contraffattore è vietato violare opere o registrazioni possedute o controllate dall'attore / ricorrente); e

c. sono realmente disponibili su base rapida laddove le circostanze lo richiedono.