FAPAV
FEDERAZIONE PER LA **TUTELA** DEI CONTENUTI AUDIOVISIVI E MULTIMEDIALI

Alla c.a.
On.le Raffaella Paita
Presidente IX Commissione
Camera dei Deputati
e per conoscenza
On.le Mirella Liuzzi
Relatore Proposte DSA e DMA

Roma, 18 giugno 2021

Oggetto: ***Regolamento Digital Services Act***

Il Digital Services Act costituisce una grande occasione per rafforzare le azioni e gli strumenti di tutela dei contenuti audiovisivi sul web al fine di porre le basi per lo sviluppo di un ecosistema digitale sano, trasparente e realmente competitivo per tutte le aziende che vi operano. L'industria audiovisiva rappresenta una risorsa strategica per il Paese sia dal punto di vista economico che occupazionale e l'economia digitale offre una grande opportunità per lo sviluppo di un comparto, come quello audiovisivo, i cui modelli di business hanno subìto numerosi cambiamenti nell'ultimo periodo. È necessario però che vengano adottate precise azioni di tutela che risultano ancora più determinanti soprattutto in un momento, come quello attuale, dove le restrizioni legate all'emergenza sanitaria hanno fortemente inciso sul sistema produttivo e distributivo del settore. Le attività di contrasto agli illeciti sono pertanto fondamentali anche nell'ottica di sostenere le aziende e l'intero comparto in questa difficile fase di ripartenza. La nostra Federazione accoglie pertanto con favore e interesse lo sviluppo del Digital Services Act poiché nel contesto attuale assume una rilevanza ancora maggiore per sostenere lo sviluppo della distribuzione digitale delle opere.

La Federazione intende pertanto evidenziare alcuni aspetti principali che si ritengono decisivi in quest'ottica di potenziamento delle attività di tutela dei contenuti audiovisivi sul web ed in particolare sulla r*esponsabilizzazione degli intermediari del web, il Notice and Stay Down ed il Know Your Business Customer (KYBC).*

La responsabilizzazione degli intermediari del web dovrà necessariamente prevedere un coinvolgimento attivo da parte di tutti i soggetti che operano sul web per contrastare la diffusione illecita delle opere. Tali responsabilità devono riguardare *in primis* i grandi operatori che devono garantire la

massima tutela delle opere e contribuire così alla realizzazione di un ambiente online che sia sicuro per tutti. L'assunzione di responsabilità - che la proposta di Regolamento non prevede con sufficiente chiarezza - costituisce infatti uno dei requisiti base per migliorare le attività di *content protection* così da scongiurare le pratiche illegali che avvengono sul web. Come già evidenziato qualche anno fa dalla stessa Commissione Parlamentare di inchiesta sui fenomeni della contraffazione, della pirateria in campo commerciale e del commercio abusivo, si ritiene necessario uno sforzo aggiuntivo sul fronte della responsabilità e del ruolo dei provider e delle piattaforme, specie quelle che gestiscono contenuti protetti.

Dato che il DSA non richiede nessuna misura proattiva contro i contenuti illegali, un suggerimento che ci sentiamo di sostenere è quello di passare a una procedura c.d. di *Notice and Stay Down* (dal precedente *Notice and Take Down*): "*La procedura di Notice and Stay Down fa seguire alla singola segnalazione da parte dei titolari di diritti IPR, che si reputano lesi da contenuti pubblicati sul web, la rimozione dei contenuti da parte dell'ISP di tutte le fattispecie di quell'illecito, prevenendo ed impedendo la reiterazione dello stesso*". Nel *Notice and Stay Down* gli intermediari sono tenuti, in presenza di una segnalazione su una determinata opera dell'ingegno oggetto di pirateria, a realizzare sostanziali azioni positive, attraverso adeguati sistemi tecnologici, per eliminare situazioni di illegalità seriali, quali:

- ✓ rimuovere tutte le copie dell'opera dell'ingegno scaricabile o gli accessi on line, da tutte le URL alle quali le offerte di download o di streaming, anche se non analiticamente indicate nella segnalazione dell'illecito da parte dei titolari di IPR;
- ✓ impedire che ulteriori copie della stessa opera siano caricate in futuro, utilizzando sistemi tecnologici di blocco, anche verso gli IP usati per violare diritti di IPR.

Il provider - con riferimento agli obblighi di *stay down* - è quindi tenuto ad agire velocemente, in forza di un *duty of care* che consegue proprio al fatto di essere stato informato dell'esistenza di un'attività illecita, in forza di una segnalazione. Diversamente, il proposto Articolo 14 del DSA appare limitato da una parte, in quanto mira solo ad una armonizzazione dei meccanismi di notifica e di azione senza migliorane l'efficacia, mentre per certi versi la proposta si spinge troppo oltre. Al fine di garantire una sostanziale protezione online, la disposizione dovrebbe almeno:

- ✓ Stabilire un chiaro obbligo di rimuovere o disabilitare rapidamente l'accesso alle informazioni notificate, unitamente ad un sistema di *Stay Down*, come proposte di cui sopra;

- ✓ Essere una normativa "a prova di futuro". Difatti, l'idea che gli avvisi debbano contenere "l'URL esatto" per identificare informazioni illegali è già obsoleta oggi, dato che le informazioni illegali non sono disponibili solo sui siti Web ma anche su app e altri servizi che non dipendono dagli URL. È necessario un approccio tecnologicamente più neutro, poiché ciò che conta è che vengano fornite informazioni sufficienti per consentire all'hosting provider di agire.

Più in generale, invece, dovrebbe essere meglio specificato dal Regolamento che la regola generale in tema di responsabilità (anche risarcitoria) è quella della responsabilità diretta del "servizio intermediario" e che il regime di limitazione della responsabilità dei "prestatori di servizi intermediari" ha natura eccezionale (conformemente a quanto attualmente previsto dal considerando 42 della Direttiva 2000/31/CE) è a condizione che questi servizi intermediari rispettino gli obblighi di dovuta diligenza (*due diligence obligations*) previsti dal Regolamento DSA. Deve tuttavia essere affermato con maggiore chiarezza che "sono fatte salve e prevalgono sul Regolamento" le previsioni della Direttiva 790/2019 sul Diritto d'Autore e sui diritti connessi nel mercato unico digitale.

La giurisprudenza italiana, avendo già dei precedenti importanti in materia di responsabilità degli intermediari e degli operatori, deve rappresentare una bussola in tal senso.

Si ricordano, in un'evoluzione interpretativa delle norme vigenti che ha sviluppato le proprie radici già nell'anno 2015 (Ord. Trib. Torino del 3 giugno 2015 nel caso Delta TV/Dailymotion), le recenti indicazioni che promanano dalla Sezione Specializzata in materia di impresa del Tribunale di Roma, il quale è intervenuto sull'argomento con due recenti sentenze, rese rispettivamente nel caso RTI SpA/Dailymotion (Dep. 21/01/2021) e RTI SpA/QLIPSO (Dep. 20/01/2021). Tali provvedimenti hanno stabilito che l'hosting provider "attivo" deve vigilare per impedire la reiterazione degli illeciti ove sia consapevole che il proprio portale ponga a disposizione del pubblico contenuti tutelati dal Diritto d'Autore, anche ove tali contenuti non gli siano stati specificamente indicati.

Sulla scia di queste Pronunce, si inseriscono due importanti provvedimenti resi da un'altra Autorità Giudiziaria, il Tribunale di Milano, sezione specializzata Diritto d'Impresa che, recentemente, ha chiarito ancora una volta alcuni punti essenziali sul tema.

I provvedimenti in questione sono l'ordinanza n. 42163 del 5 ottobre 2020 e la pronuncia emessa a margine di un reclamo del giugno 2020, relativo ad un altro procedimento su Cloudflare.

Nel quadro generale che si va delineando sullo sfondo della Direttiva Europea 2000/31, recepita nel nostro ordinamento con il D.Lgs 70/03, la Giurisprudenza italiana, con questi ultimi provvedimenti, sembra muoversi sempre più verso una maggiore responsabilizzazione degli ISP e delle società che offrono servizi di hosting o di semplice memorizzazione e archiviazione dati.

Gli Organi Giudicanti devono infatti valutare il concreto apporto reso da queste società superando, di fatto, la mera qualificazione giuridica delle stesse (hosting provider, caching, mere conduit), laddove come statuito nei provvedimenti in questione, il fatto stesso di cooperare alla funzionalità del sito, migliorandone ad esempio la qualità e la facilità nella fruizione, o archiviando i rispettivi dati favorendone il flusso e la condivisione sul web, equivale ad una partecipazione attiva alla "vita stessa" del sito incriminato.
Contribuire al supporto e ottimizzazione di questi siti, favorendone o facilitandone la valorizzazione e pubblicizzazione o adottare comportamenti di tolleranza che si traducono in omissioni che consentono a questi siti di "sopravvivere" nonostante ordini di blocco, comporta una violazione al pari di quella messa in atto dal sito medesimo.
Si tratta di provvedimenti il cui orientamento si è consolidato anche a seguito del vaglio di casi analoghi da parte della Corte di Cassazione (Sentenza 7708/2019) la quale, dato atto che i gestori delle piattaforme digitali possono assumere il ruolo di hosting provider "attivo", secondo i dettami delle più recenti decisioni della Corte di Giustizia, e che gli stessi qualora non rimuovessero i contenuti abusivi di cui hanno avuto conoscenza dai titolari dei diritti, sarebbero responsabili di un illecito commissivo a mezzo di omissione in concorso con l'autore della violazione, cioè con colui il quale immette abusivamente in rete il contenuto protetto.

In questo stesso contesto, si rendono opportuni interventi correttivi sull'attuale testo del Digital Services Act, volti ad evitare che le cause di esclusione della responsabilità degli intermediari non siano applicabili nei casi in cui essi, anche qualora non sia provato che "sono attivi o collaborano deliberatamente con gli utenti", risultino essere coinvolti nelle violazioni o facilitino attività illegali, così come accade nella maggiore parte dei casi con i siti web c.d. "cyberlockers", per fare un esempio. È necessario quindi evitare che gli intermediari possano reclamare il *safe harbor* e la propria "neutralità" quando, di fatto, il loro intento sia quello di promuovere o di ottimizzare servizi illeciti, non rispettando gli obblighi di diligenza e di trasparenza imposti dalla legge per essere esenti da responsabilità aquiliana.
Nel senso anzidetto, non potranno essere accolti emendamenti al testo del Digital Services Act volti a conferire un'esenzione di responsabilità per gli intermediari che intraprendano "azioni volontarie" nei confronti delle attività illegali commesse in rete. L'introduzione di un principio di tal fatta, si configurerebbe come uno strumento di incoraggiamento nei confronti di taluni intermediari, i quali, ponendo in essere un minimo di azioni di contrasto nei confronti dei soggetti che mettono a disposizione del pubblico contenuti illegali, solo per questa ragione potrebbero rivendicare per sé un'esenzione di responsabilità in termini generali, così da godere di immunità per eventuali ulteriori azioni illegali da essi stessi commesse o in cui siano coinvolti.

Un ulteriore aspetto che FAPAV intende sottolineare in merito al contenuto del Digital Services Act è quello che riguarda la necessità che tale provvedimento garantisca la totale salvaguardia delle norme interne attualmente esistenti in ciascuno Stato membro poste a tutela dei titolari dei diritti. Non potranno di conseguenza essere imposte condizioni o limitazioni di carattere formale per l'esercizio delle azioni legali d'urgenza nei confronti degli intermediari responsabili per le violazioni commesse in rete.

Infine, vanno valutate negativamente le disposizioni del DSA che siano rivolte a incoraggiare azioni di contrasto verso gli utenti finali autori di singole violazioni, qualora l'intermediario si trovi nella posizione migliore per fare cessare l'illecito o per rimuovere o disabilitare l'accesso ai contenuti abusivi, secondo i dettami della Direttiva 2001/29/EC (Considerando 59). In più, è necessario che gli esistenti rimedi contro i contenuti illegali siano preservati. Quindi, il DSA non deve aumentare gli adempimenti burocratici e non deve interferire senza necessità nelle leggi degli Stati Membri, ad esempio tramite la imposizione di condizioni procedurali sulle ingiunzioni a livello di singolo Stato.

L'approccio ***Know Your Business Customer*** *(KYBC)* rappresenta una soluzione semplice ed efficace per contrastare l'anonimato sul web: tale protocollo dovrebbe essere adottato da tutte quelle realtà web che forniscono servizi (*hosting*, sistemi di pagamento e di pubblicità, domini ecc) e senza, pertanto, alcuna esclusione di obbligo delle piccole e microimprese.

Chi distribuisce illegalmente contenuti audiovisivi sul web decide infatti deliberatamente di non comunicare i propri dati reali quando si trova ad acquistare qualcuno di questi servizi fondamentali per la messa in opera di un sito pirata. Quindi abbiamo da un lato chi opera illegalmente sul web non fornendo informazioni sulla propria identità, mentre dall'altro gli operatori e fornitori di servizi che non sono incentivati a verificare queste informazioni. Il Digital Services Act può e deve colmare questa lacuna a livello europeo.

Un ambiente online sicuro e trasparente per tutti deve essere la priorità anche nei confronti dei consumatori. Quando si accede a siti web o piattaforme che mettono a disposizione contenuti audiovisivi in modo illecito, non solo si violano precise regole normative, ma si mette anche a repentaglio la sicurezza e la privacy dei singoli utenti e dei loro familiari. Imbattersi in malware, phishing o peggio ancora essere derubati dei propri dati personali è una possibilità tutt'altro che remota anche se tutto sembra in termini di percezione molto conveniente e poco rischioso.

Nel ringraziare per la cortese attenzione, cogliamo l'occasione per porgere i più cordiali saluti.

FAPAV - Federazione per la Tutela dei Contenuti Audiovisivi e Multimediali

FAPAV - Federazione per la Tutela dei Contenuti Audiovisivi e Multimediali
Viale Regina Margherita 286 - 00198 Roma - Tel. 06 69 35 98 53 - Fax 06 62 27 00 28
C.F. 97056610583 - www.fapav.it - email: info@fapav.it - PEC: fapav@legalmail.it

FEDERAZIONE PER LA **TUTELA** DEI CONTENUTI AUDIOVISIVI E MULTIMEDIALI

LO SCENARIO DELLA PIRATERIA AUDIOVISIVA IN ITALIA - ALCUNI DATI IN BREVE

37%: l'incidenza complessiva della pirateria (di film, serie/fiction, programmi tv e sport live) tra gli italiani di 15 anni o più nel 2019

414 milioni: la **stima complessiva degli atti di pirateria** nel 2019. Il 50% sono film, il 27% serie/fiction, il 16% programmi tv, il 7% sport live

1,07 miliardi di euro: la **stima del fatturato perso da tutti i settori economici italiani** a causa della pirateria audiovisiva

449 milioni: il **danno stimato** sull'economia italiana i termini di **PIL**

5.900: la stima dei **posti di lavoro a rischio** a causa della pirateria

FAPAV - Federazione per la Tutela dei Contenuti Audiovisivi e Multimediali
Viale Regina Margherita 286 - 00198 Roma - Tel. 06 69 35 98 53 - Fax 06 62 27 00 28
C.F. 97056610583 - www.fapav.it - email: info@fapav.it - PEC: fapav@legalmail.it