RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0027

I profili informatici nella valutazione della responsabilità dell'Hosting Provider

Ciro D'Urso

Il presente contributo ha lo scopo di analizzare i profili tecnico-informatici che emergono, come principali argomenti di indagine, nella valutazione della responsabilità civile dei prestatori di servizi di condivisione online di contenuti forniti dagli utenti (*user-generated contents*). Le riflessioni sono sviluppate con particolare riferimento alla condivisione di contenuti multimediali effettuata senza preventiva autorizzazione del titolare dei diritti di proprietà intellettuale. Si trae spunto dall'osservare che, in ambito nazionale e indipendentemente dalla peculiarità delle singole controversie civili, le questioni tecnico-informatiche che andremo ad esaminare sono state oggetto di approfondimento istruttorio nelle valutazioni del giudice per mezzo di apposite indagini peritali disposte con l'obiettivo di rispondere a quesiti che si riscontrano, con una certa frequenza, sostanzialmente invariati dinanzi a giudici diversi.

Responsabilità civile – Diritto d'autore – ISP - Internet Service Provider – Hosting Provider – Commercio elettronico – Contenuti multimediali

1. Introduzione

La disponibilità sulla rete Internet di piattaforme di condivisione di contenuti audiovisivi fruibili online ha attirato l'interesse, a livello mondiale, di centinaia di milioni di utenti, determinando l'affermazione di grandi *player* specializzati (solo per citarne i principali, *YouTube*, *Vimeo*, *Dailymotion*) e di decine di altri siti che, pur erogando in via principale una diversa tipologia di servizio, hanno altresì ampliato l'offerta per consentire ai propri utenti il caricamento e la condivisione di filmati.

Un aspetto fondamentale connesso alla condivisione sui siti specializzati di contenuti caricati da terzi (c.d. utenti) è rappresentato dalla responsabilità civile dei proprietari delle piattaforme tecnologiche tramite le quali avviene l'attività degli utenti. Su questo tema si è assistito negli ultimi anni alla proliferazione di azioni legali, sia in ambito nazionale che europeo, promosse dai titolari dei diritti di proprietà intellettuale delle opere o dei prodotti pubblicati senza autorizzazione nelle suddette piattaforme[1].

Questo contributo analizza i profili tecnico-informatici sottesi alla normativa di riferimento con particolare riguardo alla condivisione di contenuti multimediali effettuata senza autorizzazione dei titolari dei diritti d'autore. Nel corso della disamina verranno anche evidenziati gli aspetti più controversi sui quali non vi è un orientamento giurisprudenziale univoco e, al riguardo, verranno proposti indirizzi di

C. D'Urso è ingegnere informatico e Senior Member dell'IEEE; ha ottenuto la specializzazione con lode in "Ricerca operativa e strategie decisionali" nonché il Master di II livello in "Valutazione delle politiche pubbliche". Docente a contratto presso l'Università LUMSA di Roma, è Consigliere parlamentare del Senato della Repubblica. Le opinioni espresse sono personali e non impegnano in alcun modo le Istituzioni di appartenenza.

indagine tecnico-informatica applicabili ai casi specifici. La sezione conclusiva fornirà l'opportunità di riflettere sulle prospettive future alla luce delle recenti proposte della Commissione europea.

2. Dietro le quinte della normativa: i principali profili informatici

Rinviando ai numerosi e autorevoli contributi della dottrina che analizzano diffusamente la normativa applicabile[2], occorre richiamare per gli scopi del presente lavoro, la direttiva n. 31/2000 ed il corrispondente decreto legislativo di attuazione n. 70/2003. Si farà riferimento, altresì, all'articolo 17 della nuova direttiva sul copyright del Parlamento europeo n. 790/2019 del 17 aprile 2019, ancorché non ancora recepita nell'ordinamento nazionale.

Come noto, la direttiva n. 31/2000, e conseguentemente il decreto legislativo 70/2003 (nel seguito anche rispettivamente "direttiva" e "decreto"), classificano i prestatori[3] di servizi della società dell'informazione[4] (anche detti ISP - Internet Service Provider o Hosting Provider) in tre diverse categorie in base alla tipologia di servizio erogato. In estrema sintesi sono individuati servizi di[5]: semplice trasporto su una rete di comunicazione di informazioni fornite da un destinatario del servizio e fornitura dell'accesso alla rete di comunicazione (*mere conduit*); memorizzazione temporanea di informazioni fornite da un destinatario del servizio allo scopo di rendere più efficace l'inoltro ad altri destinatari (*caching*), memorizzazione non temporanea di informazioni condivise da un destinatario del servizio (*hosting*). Allo stesso tempo, il legislatore configura una disciplina sulla responsabilità dei prestatori per i contenuti illecitamente pubblicati dagli utenti pur escludendo un obbligo di sorveglianza preventivo e generalizzato.

Procediamo, quindi, per gradi e identifichiamo i più rilevanti profili informatici coinvolti nella valutazione della responsabilità dell'Hosting Provider facendoci guidare dalla normativa richiamata.

In particolare, i considerando dal 42 al 48 e gli articoli dal 12 al 15 della direttiva, nonché gli articoli dal 14 al 17 del decreto, delineano i principi in base ai quali valutare la responsabilità dell'ISP, unitamente alla previsione dell'assenza di un obbligo generale di sorveglianza. Nella giurisprudenza nazionale, tuttavia, si è venuta a formare una distinzione che non si rinviene nella citata normativa. Infatti, nelle decisioni dei giudici di merito indicate nella nota 1 si osserva l'evolversi di una ulteriore classificazione introdotta dal giudice tra Hosting Provider attivo (ovvero non neutrale) e passivo (ovvero neutrale) sulla base delle caratteristiche del servizio erogato[6]. Sul punto occorre peraltro evidenziare che l'esenzione della responsabilità di cui all'articolo 16 del decreto non è comunque automaticamente riconosciuta all'ISP cosiddetto passivo[7]. Dunque il primo aspetto che il giudice affronta nelle controversie legali analoghe a quelle citate concerne senz'altro la natura dell'ISP in relazione ai fatti contestati.

Successivamente, chiarito il regime giuridico applicabile in relazione alla determinazione della natura del fornitore, occorre avere riguardo al comportamento tenuto dal medesimo con particolare riferimento al principio del considerando 46 della direttiva: «per godere di una limitazione della responsabilità, il prestatore di un servizio della società dell'informazione consistente nella memorizzazione di informazioni deve agire immediatamente per rimuovere le informazioni o per disabilitare l'accesso alle medesime non appena sia informato o si renda conto delle attività illecite». È interessante notare che analoga previsione si rinviene nella direttiva n. 790/2019 all'articolo 17: «... sono responsabili ... a meno che non dimostrino di ... aver compiuto ... i massimi sforzi per assicurare che non siano disponibili opere e altri materiali specifici per i quali abbiano ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti ... e in ogni caso aver agito tempestivamente, dopo aver ricevuto una segnalazione sufficientemente motivata dai titolari dei diritti, per disabilitare l'accesso o rimuovere dai loro siti web le opere o altri materiali oggetto di segnalazione e aver compiuto i massimi sforzi per impedirne il caricamento ...». Ecco che emerge l'ulteriore aspetto tecnico recato dagli aggettivi "pertinenti e necessarie" e "sufficientemente motivata": anche in questo caso la giurisprudenza non è univoca. Infatti, alcune sentenze identificano come informazione indispensabile l'indicazione "qualificata, puntuale e circoscritta" dei contenuti contestati per mezzo degli indirizzi URL (vedi *infra*)[8], al contrario, in altre decisioni, il giudice ha ritenuto sufficiente un'indicazione "specifica dei file illeciti con ogni mezzo" (e.g., il nome della trasmissione televisiva o il titolo del film)[9]. Anche in questo caso le argomentazioni tecnico-informatiche possono chiarire al giudice l'eventuale fattibilità ed efficacia della ricerca ed estrapolazione dei contenuti illeciti sulla base di informazioni generiche.

Il prestatore, ricevuta la segnalazione, ha agito tempestivamente? Ovvero, per usare le parole della direttiva n. 790/2019[10]: ha disabilitato l'accesso o rimosso le opere o altri materiali oggetto di segnalazione e ha compiuto i massimi sforzi per impedirne il caricamento in futuro? Dal quesito discendono alcuni aspetti tecnici non privi di complessità anche correlati alle modalità tipiche della segnalazione. Essa

infatti può consistere, come accennato, in una lista di titoli (per esempio, di programmi o film) corrispondenti a file pubblicati illecitamente sul sito contenenti cospicue parti o singole scene dell'opera originaria. Su questa base si dovrebbe ritenere che il provider a partire da questo momento è "informato", ai sensi del considerando 46 della direttiva, delle attività illecite, e che quindi dovrebbe agire con una rimozione *ex-post*[11] dei contenuti esistenti sulla propria piattaforma. Ma, per lo stesso principio di diligenza e tempestività, dovrebbe anche impedire *ex-ante*[12] il caricamento di brani analoghi estratti dall'insieme di opere segnalate. A questo scopo vengono in soccorso due tipologie di strumenti informatici, la prima agisce sia *ex-ante* sia *ex-post*, la seconda invece unicamente *ex-post*.

Il percorso logico fin qui seguito ci conduce infine alla quantificazione del danno, la cui elaborazione necessita di analisi molto approfondite sulle caratteristiche (più propriamente metadati) dei singoli file pubblicati illecitamente nel tempo. L'esame può richiedere il controllo, come avvenuto nel coso di taluni giudizi, di evidenze informatiche risalenti anche a un decennio prima.

2.1. La natura attiva o passiva dell'Internet Service Provider

La sentenza della Suprema Corte di Cassazione del 19 marzo 2019, n. 7708, è intervenuta sul tema della responsabilità dei prestatori di servizi della società dell'informazione (caso RTI v. Yahoo!). La parte convenuta in questo caso non è stata riconosciuta quale provider "attivo", ma la Cassazione ha colto l'occasione per chiarire la distinzione tra Hosting Provider attivo e passivo[13] introducendo tre elementi che influenzerebbero tale classificazione. Ad avviso della Corte, il prestatore di servizi di hosting svolge un ruolo attivo, allorché esso compia una o più delle seguenti operazioni sui contenuti: filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione, promozione (primo elemento: c.d. "indici di interferenza"), se effettuate nel contesto di una gestione imprenditoriale del servizio (secondo elemento). La Corte ha aggiunto, altresì, che anche le tecniche di valutazione comportamentale degli utenti possono avere rilievo nel riconoscimento in capo all'ISP di un ruolo attivo, allorché esse siano impiegate per aumentare la fidelizzazione degli utenti con lo scopo di completare e arricchire, in modo non passivo, la fruizione di contenuti da parte di un pubblico indeterminato (terzo elemento). Conseguentemente, i citati tre elementi sottoposti alla valutazione del giudice dovrebbero essere accertati in corso di causa e, trattandosi di profili molto tecnici, appare indispensabile l'ausilio del consulente d'ufficio che approfondirà gli aspetti che nel seguito andiamo a descrivere.

Gli elementi citati primo e terzo devono essere controllati analizzando il comportamento del sito web rispetto all'interazione con le diverse tipologie di utenti, considerando quantomeno da un lato l'azione di un utente anonimo fruitore di contenuti e dall'altro di un utente produttore dei medesimi e registrato sulla piattaforma. Si applica, in tal caso, un metodo sperimentale avendo riguardo alle funzionalità del sito attivate durante la navigazione anonima e a quelle utilizzate nel corso del processo di caricamento dei file, nonché all'effetto di queste ultime sulla catalogazione e ricerca dei contenuti, considerando, peraltro, anche l'eventuale indicizzazione da parte di motori di ricerca esterni al sito stesso. Un ulteriore aspetto da apprezzare ai fini della valutazione del giudice, che si pone a metà strada tra il secondo e il terzo elemento sopra elencati, è costituito dall'analisi degli eventuali annunci pubblicitari visualizzati durante la navigazione dell'utente, i quali presuppongono una monetizzazione degli accessi al sito stesso e, eventualmente, una profilazione del comportamento[14]. Inoltre, particolare cautela deve essere esercitata nella compilazione delle conclusioni tecniche valutando i risultati ottenuti anche alla luce delle motivazioni del considerando 42 della direttiva, spesso richiamato dalle parti convenute, allorquando stabilisce la sussistenza della deroga alla responsabilità per l'attività di "ordine puramente 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". Infatti, con le attuali tecniche di intelligenza artificiale (*machine learning*), i processi automatici che è possibile "programmare", affinché il contenuto degli utenti sia opportunamente elaborato dai calcolatori, sono divenuti particolarmente sofisticati. Basti pensare per esempio ai metodi di riconoscimento e classificazione delle immagini. In altre parole, è vero che operazioni di questo tipo possono essere automatiche (eseguite dal calcolatore), ma è altrettanto vero che gli algoritmi per eseguirle sono predisposti da tecnici informatici che li personalizzano per essere utilizzati nella piattaforma in esame.

Per quanto riguarda il secondo elemento sopra richiamato, risulta sufficiente approfondire il modello di business del fornitore di servizi, segnatamente soffermandosi sulla descrizione del funzionamento dell'organizzazione dal punto di vista dei clienti, dell'offerta, delle infrastrutture e della solidità finanziaria, facendo riferimento agli schemi (*patterns*) rappresen-

tativi dei modelli più diffusi nell'ambito dei servizi della società dell'informazione[15]. In particolare, nel caso delle piattaforme leader di mercato, il carattere *multi-sided* del business è rappresentato quantomeno dal *pattern Freemium*: il servizio di base è gratuito, si paga per avere qualcosa in più.

2.2. Le segnalazioni

I brani audiovisivi pubblicati nelle piattaforme citate sono fisicamente dei file memorizzati in apparati tecnologici controllati dal prestatore di servizi. Essi sono identificati per mezzo di una stringa alfanumerica chiamata URL[16]. Il contenuto di una segnalazione[17] effettuata dal titolare dei diritti e indirizzata al provider può essere così dettagliato da contenere tutte le URL dei file contestati, ovvero un elenco esaustivo dei titoli dei film e delle trasmissioni rivendicate unitamente ad un campione esemplificativo di URL. L'idoneità del contenuto della predetta segnalazione a costituire informazione "pertinente e necessaria" tale da rendere effettivamente edotto il prestatore circa l'illegittimità del contenuto pubblicato è valutata dal giudice in relazione alle risultanze peritali concernenti gli strumenti utilizzabili dal prestatore di cui si dirà nel successivo paragrafo. La Comunicazione della Commissione europea COM(2017)555, del 28 settembre 2017, in merito alle segnalazioni (sezione 3.2.3), consiglia di predisporre «meccanismi efficaci volti a facilitare la presentazione di segnalazioni sufficientemente precise e adeguatamente giustificate al fine di consentire alle piattaforme di prendere decisioni rapide e informate sui provvedimenti da adottare», aggiungendo, rispetto alla forma delle stesse segnalazioni, che esse dovrebbero contenere «una chiara indicazione dell'ubicazione del contenuto potenzialmente illegale (ad esempio l'indirizzo URL)».

L'indirizzo giurisprudenziale, anche in questo caso, non è univoco nell'affermare la necessità di comunicare l'elenco completo degli indirizzi URL. Infatti è possibile citare, ad esempio, le decisioni: Corte d'appello di Milano, n. 29/2015 (RTI/Yahoo!) e Tribunale di Torino n. 1928/17 (cit.), nelle quali è stabilito che si debba «... escludere che una generica diffida, contenente i soli titoli commerciali dei prodotti audiovisivi, sia idonea a far venire meno la neutralità del gestore, e quindi attivare la sua responsabilità»[18]. Di segno opposto, invece, le decisioni: Corte d'appello di Roma, sentenza del 29 aprile 2017 (RTI – Break Media); Tribunale di Roma, ordinanza collegiale del 14 febbraio 2014 (RTI c. Google) e sentenza del 15 luglio 2016 (cit.) e, da ultimo, sentenza del 10 gennaio 2021 (RTI c. Dailymotion) (cit.), nelle quali è stabilito che le informazioni necessarie e sufficienti che il titolare dei diritti deve fornire al gestore di una piattaforma possono consistere in un elenco dei titoli commerciali dei programmi e non necessariamente dei singoli indirizzi URL per la localizzazione dei video contestati[19].

Tra l'altro, è la stessa sentenza della Corte di Cassazione n. 7708 (cit.), a fornire una *ratio* della non univocità delle decisioni di merito, nonché della necessità di esaminare caso per caso la questione in parola, allorquando stabilisce che «l'idoneità della comunicazione al prestatore del servizio a consentire al destinatario la comprensione e l'identificazione dei contenuti illeciti va valutata caso per caso, a tal fine deve allora aversi riguardo ai profili tecnico-informatici per valutare se, nell'ipotesi di trasmissione di prodotti video in violazione dell'altrui diritto di autore, questi siano identificabili mediante la mera indicazione del nome della trasmissione da cui sono tratti e simili elementi descrittivi, oppure occorra anche la precisa indicazione del cd. indirizzo URL». La stessa Corte, tuttavia, con sentenza n. 7709/2019, trattando il caso di un prestatore di servizi della società dell'informazione che esercita la mera attività neutrale di *caching*, stabilendo che la responsabilità prevista dall'articolo 15 del d.lgs. n. 70 sussiste in capo al prestatore dei servizi che non abbia provveduto alla immediata rimozione dei contenuti illeciti – pur essendogli ciò stato intimato dall'ordine proveniente da un'autorità amministrativa o giurisdizionale – ha inoltre aggiunto che, nel caso di specie, la notizia contenuta nella diffida extragiudiziale era generica, in quanto priva delle specifiche indicazioni dei singoli filmati contestati e del loro posizionamento tramite URL. Osserviamo, quindi, che anche in questo contesto l'intervento del consulente tecnico del Giudice risulta dirimente. In particolare esso sarà finalizzato a certificare la natura del prestatore di servizi, sulla base di opportune indagini peritali aventi ad oggetto l'analisi della piattaforma informatica e degli algoritmi utilizzati per erogare il servizio.

Sul punto, inoltre, è utile osservare che una funzionalità, resa disponibile dai siti dei principali prestatori, consiste nella possibilità di inviare puntuali segnalazioni di violazioni, utilizzando una modulistica online per sottomettere la richiesta del cosiddetto *take down*, in linea, tra l'altro, con quanto previsto dal paragrafo 9 dell'articolo 17 della già richiamata direttiva n. 790/2019: «gli Stati membri dispongono che i prestatori di servizi di condivisione di contenuti online istituiscano un meccanismo di reclamo e ricorso celere ed efficace che sia disponibile agli utenti dei loro servizi in caso di controversie in merito alla disabilitazione dell'accesso a – o alla rimozione di – specifiche opere o altri materiali da essi caricati».

Osserviamo che le piattaforme con sede legale negli USA (come Vimeo) nelle predette pagine web fanno riferimento al *Digital Millennium Copyright Act* (DMCA), una legge degli Stati Uniti d'America sul copyright che implementa i due trattati del 1996 dell'Organizzazione Mondiale per la Proprietà Intellettuale. Il DMCA rende illegali la produzione e la divulgazione di tecnologie, strumenti o servizi che possano essere usati per aggirare le misure di accesso ai lavori protetti dal copyright e prevede, altresì, un inasprimento delle pene per la violazione del copyright su Internet. Tipicamente, questa funzionalità è contenuta nella sezione del sito dell'Hosting Provider dedicata all'illustrazione delle linee guida per l'utilizzo corretto del servizio (*Terms of service*).

2.3. Gli strumenti

Affrontiamo in questa sezione la questione concernente le modalità tecniche idonee ad identificare i video pubblicati in violazione dei diritti d'autore. In tale contesto, è utile fare riferimento anche alla Comunicazione della Commissione europea COM(2017)555 (cit.) ove vengono prospettati alcuni orientamenti alla luce del quadro giuridico vigente. In particolare si evidenzia come le piattaforme online, ad oggi, dispongono solitamente dei mezzi tecnici per identificare e rimuovere i contenuti illeciti e che, alla luce del progresso tecnologico nell'elaborazione di informazioni e nell'intelligenza artificiale, l'uso di tecnologie di individuazione e filtraggio automatico sta diventando uno strumento ancora più importante nella lotta contro i contenuti illegali online.

A questo fine, da un punto di vista più tecnico, occorre distinguere due principali modalità: (i) una basata sulla tecnica del c.d. video *fingerprinting*; (ii) l'altra basata su una ricerca per parole chiave almeno parzialmente automatizzata.

Una generica organizzazione che produce contenuti (audio o video) ha interesse a controllare la distribuzione e l'uso degli stessi, al fine di proteggere gli investimenti effettuati. In tale contesto, negli ultimi venti anni, vi è stata una continua evoluzione della tecnologia classificata come *Digital Rights Management* (*DRM*). Si tratta di software sviluppati per aiutare a tenere sotto controllo, in maniera automatizzata, l'utilizzo di contenuti protetti da diritti di proprietà intellettuale. Questa particolare tecnologia è in grado di supportare in modo automatico le seguenti attività: (i) identificazione dei contenuti, (ii) controllo del copyright, (iii) protezione delle copie, (iv) tracciamento degli utilizzi. Le tecniche utilizzate sono varie, a titolo esemplificativo citiamo l'ormai ampiamente diffuso *watermarking*, ovvero l'introduzione nel file video di informazioni aggiuntive che "marchiano", come un tatuaggio digitale, ogni fotogramma. Per gli scopi della presente analisi è, tuttavia, di particolare rilievo la tecnica denominata "video *fingerprinting*". Essa consiste, analogamente a quanto avviene nel caso delle impronte digitali delle persone, nel rilevare alcuni elementi che caratterizzano univocamente il file (video/audio) e nel memorizzarli in una base dati, in modo che sia possibile confrontare successivamente qualsiasi video con le tracce presenti in tale archivio al fine di identificare la presenza di sequenze riconducibili al file originario.

Tale tecnica risponde all'esigenza di rendere disponibile una base dati da utilizzare per identificare una esatta porzione di un contenuto (audio/video) ogni volta che il sistema la incontra, anche in diversi e successivi file. Al contrario, invece, memorizzare l'intero contenuto, per poi utilizzarlo in futuro per il confronto, richiederebbe una quantità di spazio e di capacità elaborativa costosa ed esageratamente grande. Conseguentemente, le tecniche utilizzate sono mutuate dal campionamento statistico, per cui solo un campione del file originario è memorizzato ed utilizzato per operare il confronto. Questo campione rappresenta una sequenza univoca che identifica il file originario e, come nel caso delle impronte digitali, può essere utilizzata per identificare la presenza di quel contenuto in altri file, ma non consente di riprodurre il video o l'audio. Cosa molto importante, con tale tecnica è possibile, con determinati accorgimenti, identificare anche porzioni di audio/video, come per esempio nei video *mash up*, nei quali sono presenti spezzoni provenienti da svariati file opportunamente montati. Dotarsi di un sistema di questo tipo significa implementare innanzitutto un processo al fine di creare l'archivio delle "impronte", e successivamente utilizzare l'archivio così generato per confrontare le "impronte" memorizzate con quelle dei nuovi contenuti audiovisivi. Si osserva, sul punto, che sono disponibili diversi algoritmi di generazione del *fingerprint* dei contenuti audio-video, sia con riferimento alla letteratura scientifica, sia con riferimento a soluzioni di mercato proprietarie o disponibili in modalità "codice aperto" (i.e., *open source*). Tali algoritmi da soli non sono comunque sufficienti, infatti essi devono essere inseriti in un processo tecnico-organizzativo di livello *enterprise* al fine di realizzare i controlli nel contesto di realtà delle dimensioni delle aziende coinvolte nelle cause citate. Si ricorda, peraltro, che la semplice disponibilità di librerie software scaricabili da Internet, previo pagamento di un limitato importo o rese disponibili in modalità *open source*, non determina affatto che un processo di implementazione su vasta scala basato su tali moduli

software sia di per sé "agevole" o "economico" (in particolare la disponibilità di software distribuito in modalità "open source", ancorché non preveda alcun pagamento per la licenza, non implica affatto che il suo utilizzo sia a costo zero, in quanto occorre considerare non solo il costo iniziale ma soprattutto il c.d. TCO - *Total Cost of Ownership*[20]). Si evidenzia, tra l'altro, la presenza di ampia letteratura scientifica sul tema del video *fingerprinting* e della correlata disponibilità di algoritmi e moduli software che li implementano. Basti segnalare che l'elaborazione di tale tecnica risale addirittura al 1983, in particolare fu introdotta, come approccio teorico generale e non specificamente per applicazioni collegate a brani audiovisivi, da un noto articolo di N.R. Wagner[21]. A tale riguardo, è utile fare riferimento, tra gli altri, anche all'interessante illustrazione dell'approccio ai fini del suo utilizzo nelle applicazioni *DRM* che emerge nell'*invited paper* di D. Kundur[22].

Il funzionamento è il seguente: il sistema ispeziona i nuovi caricamenti e i video esistenti per rilevare i casi di uso non legittimo (i.e., video non caricati dal proprietario dei diritti). Il file sospetto viene quindi classificato come candidato per essere oggetto di un'operazione di *take down*. L'utente che lo ha caricato è costretto a rimuovere il video o a cambiare la colonna sonora del video stesso. In alternativa, nel caso l'utente fosse sicuro delle proprie ragioni, il sito consente di sottoporre una richiesta di appello. In relazione ai brani audiovisivi per i quali è stata accertata la violazione di copyright, è possibile utilizzare un metodo di filtro *ex ante* per impedire che brani identici a quelli soggetti a operazione di *take down* siano caricati nuovamente.

Si cita quale esperienza rilevante il caso di Google che ha creato un sofisticato meccanismo per controllare l'uso illegittimo di contenuti audio/video nella piattaforma YouTube. Infatti, la predetta piattaforma consente ai proprietari di contenuti di sottomettere i propri file per elaborarne il relativo *fingerprint* e memorizzarlo nell'archivio appositamente predisposto dalla stessa YouTube. Ogni video aggiunto alla piattaforma è dapprima confrontato con l'archivio centrale delle impronte e solo dopo l'esito negativo della comparazione viene messo a disposizione degli utenti. Tale sistema è noto con il nome di "Content ID". È interessante citare, in questa sede, la collaborazione tra Google e alcuni fornitori di piattaforme software per la gestione automatizzata dei processi relativi al DRM, come per esempio Harmonic Inc. (produttore della tecnologia Rhozet), che prevede la generazione del *fingerprint* compatibile con la piattaforma "Content ID" già in sede di produzione del file audio/video.

Google dichiara[23] che la piattaforma Content ID, usata per la ricerca automatica dei video clip caricati violando il copyright su YouTube, è efficace nel 98% dei casi, solo il 2% dei video privi di autorizzazione richiede la rimozione manuale, inoltre ha reso noto che il giro d'affari del sistema Content ID, usato da YouTube, vale 2 miliardi di dollari. Google ha rivelato anche che gli investimenti nell'antipirateria (in particolare nella piattaforma Content ID) fino al 2015 sono stati pari a 60 milioni di dollari. Per contro, alcune primarie istituzioni che detengono i diritti di importanti opere audio/video non concordano sull'efficacia del sistema di YouTube, dichiarando che esso fallisce nel 40% dei casi, e che, da un certo punto di vista, rischia di legittimare la pirateria[24].

Va osservato che un sistema di questo tipo, se sviluppato in casa, richiede la disponibilità di un'elevata capacità di memorizzazione e di una significativa potenza elaborativa. La realizzazione di una soluzione di questo tipo ha, quindi, costi non trascurabili, sia una tantum (e.g., acquisizione/sviluppo e configurazione/personalizzazione del sistema software), sia ricorrenti (e.g., costi fissi come canoni di manutenzione, retribuzione del personale). Nell'ipotesi alternativa di acquisizione di un servizio da un operatore specializzato[25] i costi sono senz'altro minori rispetto ad una soluzione sviluppata in casa, atteso che l'operatore che offre tali servizi realizza economie di scala in relazione al numero dei clienti posseduti e può spalmare il costo di realizzazione e di manutenzione sul portafoglio clienti. D'altra parte, un servizio di questa specializzazione e con i volumi associati alle piattaforme più diffuse richiede comunque un investimento non trascurabile, che presuppone accordi specifici tra cliente e fornitore, stimabile tra alcune centinaia di migliaia di dollari all'anno e qualche milione (i listini pubblicati dalle aziende specializzate in genere elencano i costi fino ad un numero di video di poche migliaia, per volumi superiori rimandano a specifici accordi presi caso per caso).

Gli strumenti che rientrano nella tipologia fin qui descritta costituiscono, quindi, la tecnica più efficace ed efficiente per il controllo sia preventivo (*ex-ante*, cioè effettuato prima della pubblicazione dei video)[26] sia successivo (*ex-post*, cioè effettuabile anche dopo la pubblicazione dei video) dei contenuti da pubblicare o pubblicati, ed alle cui risultanze subordinare la stessa pubblicazione e/o la permanenza online del contenuto audiovisivo considerato. D'altra parte, se si volesse valutare una modalità tecnica diversa dal video *fingerprinting* utilizzabile *ex-post* (ovvero dopo la pubblicazione del video), si dovrebbe agire facendo uso delle interfacce standard messe a disposizione dalle piattaforme (i.e., interfaccia basata su API -

Application Programming Interface) per interrogare in maniera automatica l'archivio del prestatore di servizi ed ottenere un insieme di video che corrispondono ai criteri di ricerca definiti[27]. Tale modalità certamente non possiede un'efficacia paragonabile al metodo sopra descritto, per contro consente, con un intervento umano successivo all'estrapolazione automatica della lista dei video che corrispondono alla ricerca effettuata, di rilevare un insieme non trascurabile di file da sottoporre al *take down*.

2.4. Quantificazione del danno

In alcune delle sentenze esaminate (citate in nota 1), la quantificazione del danno causato al titolare dei diritti dalla pubblicazione non autorizzata delle proprie opere è avvenuta con riferimento al calcolo delle *royalties*. Con *royalty* si indica il diritto del titolare di un brevetto o di una proprietà intellettuale ad ottenere il versamento di una somma di denaro da parte di chiunque effettui lo sfruttamento dei predetti beni per fini commerciali e/o di lucro. In molti dei citati giudizi, siamo in presenza di opere audiovisive caratterizzate da alti costi di produzione (in termini di mezzi tecnologici utilizzati, risorse umane impiegate e attività organizzative poste in essere) e bassi costi marginali di sfruttamento (a valle della disponibilità del prodotto finale, è possibile replicare l'opera diffondendola mediante svariati canali con un investimento economico molto minore rispetto a quello necessario per produrla). Occorre considerare, quindi, da una parte il titolare dei diritti che, come conseguenza della diffusione non autorizzata delle proprie opere, sperimenta un mancato guadagno derivato dall'impossibilità di sfruttare (e.g., con la pubblicità ovvero con l'eventuale corrispettivo di un abbonamento) i brani audio-video divenuti disponibili su una piattaforma di *video sharing* e fruibili senza controllo da una vasta platea di spettatori. Per contro, la stessa piattaforma di *video sharing* sperimenta un effetto positivo (invero difficilmente quantificabile) in termini di popolarità, maggiori accessi, conseguente aumento di utenti e, eventualmente, maggiori abbonamenti onerosi: in altri termini, il c.d. effetto di rete, su cui però è assai complicato elaborare calcoli adeguatamente motivati.

Ci muoviamo, in base a quanto illustrato, in uno scenario controfattuale per il quale non risulta agevole l'elaborazione di un modello: infatti siamo in presenza di parametri – che definiscono i mancati introiti di una parte e i "guadagni" dell'altra – difficilmente quantificabili. In questo contesto è usuale seguire, per il calcolo del danno, il criterio del prezzo del consenso[28]: conseguentemente, l'individuazione delle *royalties* si sostanzia nella stima dei proventi che il danneggiato avrebbe ottenuto se avesse ceduto a titolo oneroso al danneggiante i diritti di cui quest'ultimo si è invece illecitamente appropriato. A questo scopo l'analisi tecnico-informatica viene espletata avendo riguardo al numero di file contestati, alla loro durata, al tempo di permanenza sulle piattaforme degli Hosting Provider calcolato a far data dalla pubblicazione dei file stessi ovvero dalle segnalazioni del titolare fino alla loro rimozione, al numero di visualizzazioni e *download* nel periodo di disponibilità online.

Occorre, però, ribadire che lo scenario controfattuale in commento è in genere privo di talune informazioni indispensabili per il suo completo svolgimento, le quali non possono essere desunte né dagli atti di causa né da comportamenti passati delle parti. Tale lacuna è determinata principalmente dal fatto che le condizioni di mercato, in particolare la pubblicazione di contenuti multimediali su piattaforma web di condivisione di contenuti per il mercato in lingua italiana, potrebbero non essere rilevabili in precedenti accordi volontari tra le parti o con aziende di produzione televisiva e/o cinematografica per lo sfruttamento di video su una piattaforma web. Una possibilità di approfondimento consiste, in questo contesto, nel provare a sviluppare il calcolo del prezzo del consenso con diverse argomentazioni, tra le quali si citano le seguenti. Una prima argomentazione potrebbe essere basata su contratti stipulati e accordi transattivi sottoscritti in precedenti analoghi procedimenti; un secondo approccio potrebbe essere basato sull'analisi delle modalità con le quali operano quelle aziende che hanno come modello di business la cessione in licenza dei propri contenuti multimediali attraverso acquisti online[29]; la terza potrebbe essere ispirata ai servizi di *Video on demand* messi a disposizione da alcuni fornitori per talune fattispecie di utenti paganti e che consentono agli stessi di ricavare un profitto dalla pubblicazione sulle piattaforme medesime dei brani audiovisivi di propria creazione[30]. Quest'ultima argomentazione si basa sul criterio noto come condivisione del fatturato (*revenue sharing*).

3. Conclusioni

Dalle considerazioni sviluppate, emerge che l'attività del consulente d'ufficio debba proporre al giudice una narrazione che integri i vari aspetti informatici della disciplina applicabile al contesto esaminato, solo apparentemente distinti, presentandoli sotto una prospettiva unitaria e consequenziale. Sulla base dei quesiti posti dal giudice, andrebbe effettuata una disamina delle caratteristiche tecniche che governano le

modalità di erogazione e di fruizione dei servizi, nonché un'analisi delle azioni poste in essere dalle parti, condotta con riferimento alle tecnologie disponibili all'epoca dei fatti. Alcune questioni, come detto, sono ancora in divenire e non univocamente definite in un orientamento giurisprudenziale consolidato, tuttavia occorre anche considerare che ciascun caso fa storia a sé, sia per le caratteristiche dell'Hosting Provider sia per il periodo temporale in cui si collocano i fatti. Probabilmente l'aspetto più controverso delle analisi rimane quello legato alla quantificazione del danno, per il motivo a cui si accennava nel precedente paragrafo, e, cioè, per la difficoltà – che a volte diviene impossibilità – di condurre una motivata analisi controfattuale delle strategie commerciali delle parti.

Volgendo lo sguardo ai possibili scenari futuri e alla possibile evoluzione delle questioni sopra discusse, si segnala che, il 15 dicembre 2020, la Commissione europea ha presentato le proposte di due Regolamenti in ambito digitale: il *Digital Services Act* (DSA) e il *Digital Markets Act* (DMA) allo scopo di regolare, sulla base dell'attuale Direttiva sull'e-Commerce (cit.), i cosiddetti servizi digitali. Le due proposte, presentate dalla Commissione, verranno ora sottoposte al vaglio del Parlamento europeo e del Consiglio dell'Unione secondo la procedura legislativa ordinaria.

Con riferimento alla tematica del regime di responsabilità degli intermediari, si osserva, tra l'altro, che la prima delle due proposte, nel mantenere il sistema di responsabilità attualmente in vigore, introduce il principio secondo il quale i meccanismi di *notice and take down* dovranno essere standardizzati, rispettare precisi requisiti e consentire ad ogni individuo o entità di notificare la presenza di specifici contenuti che sono ritenuti illegali. Si segnala, inoltre, l'introduzione di garanzie per gli utenti i cui contenuti sono stati erroneamente cancellati dalle piattaforme e nuovi obblighi per le piattaforme di grandi dimensioni di adottare misure basate sul rischio al fine di prevenire abusi dei loro sistemi.

Parallelamente, il secondo pilastro della proposta di regolamentazione di Bruxelles è quello della concorrenza. Con la legge sui mercati digitali l'Ue interviene sul ruolo dei cosiddetti *gatekeeper*, le piattaforme che hanno una posizione di dominio tale da poter impedire l'accesso di nuove aziende sul mercato, con la previsione di una serie di nuove regole per evitare comportamenti anticompetitivi. Le piattaforme, per esempio, non potranno promuovere i propri servizi a scapito di quelli dei concorrenti e dovranno condividere parte dei loro dati con altre aziende. Sono inoltre previste una serie di sanzioni che possono arrivare fino al 10% del fatturato annuo.

Gli interventi citati, se confermati all'esito della procedura legislativa, consentiranno di proteggere in modo più efficace i diritti fondamentali degli utenti della rete Internet, rendendo i mercati digitali più equi e con minori barriere all'entrata di nuovi operatori. Essi permetteranno, altresì, di rendere più circoscritti gli approfondimenti peritali disposti dal giudice, dovendosi indagare sul rispetto di requisiti tecnici che risulterebbero, almeno in parte, più standardizzati e compiutamente definiti[31] se paragonati a quanto previsto dalla normativa vigente.

Note

[1]Si considerino *ex multis*, in tema di responsabilità dell'Hosting Provider rispetto a contenuti generici forniti dagli utenti: Corte di Giustizia Europea: sentenza 23 marzo 2010, cause riunite da C-236/08 a C-238/08 (Google France c. Louis Vuitton); sentenza 12 luglio 2011, C-324/09, (L'Oréal SA c. eBay International AG); sentenza 16 febbraio 2012, C-360/10 (Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) c. Netlog NV); sentenza 11 settembre 2014, C-291/13 (Papasavvas c. Fileleftheros); sentenza 14 giugno 2017, C-610/15 (Stichting Brein c. Ziggo BV); Tribunale di Milano: sentenza 7 giugno 2011, n. 7680, RTI c. Italia On Line; sentenza n. 29/2015, RTI c. Yahoo! Italia s.r.l. / Yahoo! Inc; ordinanza 8 maggio 2017, Mediaset c. Live TV; Tribunale di Roma: sentenza n. 17279/2011, RTI c. VBB-COM. Limited/Choopa LLC; sentenza 7 luglio 2016, RTI c. Megavideo LTD; sentenza n. 2883/2017, RTI c. Break Media; sentenza 15 luglio 2016, n. 14279, RTI c. Megavideo (2016); sentenze n. 693/2019, n. 14760/2019, RTI c. Vimeo; sentenza n. 3512/2019, Mediaset c. Facebook; sentenze del 12 luglio 2019, n. 14757, e del 22/01/2021 nella causa RG 62326/2015, RTI c. Dailymotion; Tribunale di Torino: sentenza 1928/17, Delta TV Programs S.r.l c. Google, Inc. / YouTube LLC / Google Ireland Holdings; sentenza n. 342/2018, Dailymotion S.A c. Delta TV Programs srl.

[2]Sulla responsabilità civile degli ISP la letteratura è molto vasta. Si vedano ad esempio: M.R. Allegri, *Alcune considerazioni sulla responsabilità degli intermediari digitali, e particolarmente dei social network provider, per i contenuti prodotti dagli utenti*, in "Informatica e diritto, 2017, n. 1-2, pp. 69-112; E. Tosi, *Contrasti giurisprudenziali in materia di responsabilità civile degli hosting provider – passivi e attivi – tra tipizzazione normativa e interpretazione evolutiva applicata alle nuove figure soggettive dei motori di ricerca, social network e aggregatori di contenuti*, in "Rivista di diritto industriale", 2017, n. 1, pp. 75-122; M. Cocuccio, *La responsabilità civile per fatto illecito dell'Internet Service Provider*, in "Responsabilità civile e previdenza", 2015, n. 4, p. 1312 ss.; G. Sartor, E. Rosati, *Social networks e responsabilità del provider*, Working paper n. 5-Dept. of Law, EUI 2012; M. De Cata, *La responsabilità civile dell'Internet service provider*, Giuffrè, 2010; L. Albertini, *Sulla responsabilità civile degli internet service provider per i materiali caricati dagli utenti (con qualche considerazione generale sul loro ruolo di gatekeepers della comunicazione)*, in "Law and Media Working Paper Series 2020", October 7, 2020.

[3]Ai sensi dell'art. 2, c. 1, lett. b), del d.lgs. 70/2003 per "prestatore" si intende: "la persona fisica o giuridica che presta un servizio della società dell'informazione".

[4]Ai sensi dell'art. 2, c. 1, lett. a), del d.lgs. 70/2003 per "servizi della società dell'informazione" si intendono: "le

attività economiche svolte on line, nonché i servizi definiti dall'articolo 1, comma 1, lettera b), della legge 21 giugno 1986, n. 317, e successive modificazioni".

[5]Artt. 13, 14 e 15 della direttiva citata.

[6]Secondo il Tribunale di Roma, tra l'altro, il provider attivo non costituisce una sub-categoria di quello passivo, ma è figura del tutto autonoma che si sottrae dalla disciplina comunitaria e nazionale prevista per l'hosting neutro (sentenza 14757/2019 cit.).

[7]Si veda la recente sentenza del Tribunale di Roma nella causa R.G. 33124/2012, RTI c. Facebook Inc. e Facebook Ireland Limited, nonché il commento: C. Novelli, *Il social giudizioso. La giurisprudenza italiana sulla responsabilità civile degli ISP*, in "Rivista Italiana di Informatica e Diritto", 2019, n. 1, pp. 97-106.

[8]Così Tribunale di Milano, Sentenza n. 29/2015 del 7 gennaio 2015 cit.

[9]In tema di irrilevanza della comunicazione delle URL si vedano le sentenze 14757/2019 e 3512/2019 cit.

[10]Si veda l'articolo 17, sezione 4, lettera c).

[11]Operazione di *take down*: disabilitazione di contenuti pubblicati da un terzo che il titolare consideri in violazione dei propri diritti d'autore.

[12]Operazione di *stay down*: prevenire la ricomparsa di contenuti illeciti analoghi a quelli già oggetto di *take down*.

[13]Si ricorda che la definizione di Hosting Provider attivo" è stata coniata da Trib. Milano, 7 giugno 2011, n. 7680 (cit.): «una diversa figura di prestatore di servizi, non completamente passivo e neutro rispetto all'organizzazione della gestione dei contenuti immessi dagli utenti (c.d. hosting attivo), organizzazione da cui trae anche sostegno finanziario in ragione dello sfruttamento pubblicitario connesso alla presentazione (organizzata) di tali contenuti».

[14]La pubblicità presente sui portali in discorso assume tipicamente tre forme: i) annunci pubblicitari (c.d. "display advertisement"), sotto forma, ad esempio, di banner direttamente visibili sulle pagine; ii) clip pubblicitarie (annunci veri e propri), che l'utente, per fruire del video selezionato, è obbligato a vedere in parte (per es. fino a 15-20 secondi) o per intero (per es. fino a 50 secondi); tali annunci sono riprodotti prima che inizi il video selezionato e/o nel corso della visione dello stesso; iii) banner trasparenti che si giustappongono al video visualizzato, in particolare occupando la porzione inferiore (tali annunci sono simili a banner e possono essere eliminati dall'utente cliccando sull'estremo superiore destro). I predetti annunci pubblicitari generano introiti in due modalità diverse: *pay-per-click* per il primo ed il terzo tipo di pubblicità, *pay-per-view* per la seconda tipologia.

[15]Una pubblicazione di taglio divulgativo, ma non per questo priva di rigore scientifico: A. Osterwalder, Y. Pigneur, *Business Model Generation*, John Wiley & Sons, 2010.

[16]Il World Wide Web (WWW) è uno dei servizi più utilizzati della rete Internet. Esso è realizzato come sistema distribuito client-server, in cui il client è un browser e il server è un server web. Nella comunicazione tra client e server non è sufficiente che richiesta e risposta giungano correttamente al destinatario, occorre che i due programmi comunicanti siano in grado di comprendere le rispettive comunicazioni, cioè "parlino la stessa lingua": devono perciò condividere uno stesso protocollo applicativo. Nel caso del WWW, il protocollo applicativo che specifica il formato della richiesta del browser e della risposta del server web, è denominato "HyperText Transfer Protocol (HTTP)". Per poter accedere ai servizi applicativi messi a disposizione dai server sulla rete è necessario che ognuno di tali servizi risulti univocamente identificabile da parte dei client. Nel caso di Internet è stato definito uno schema uniforme di identificazione applicativa, che consente di assegnare un metodo di accesso e un indirizzo a ogni risorsa presente sulla rete in base ad uno standard chiamato "Uniform Resource Locator (URL)". In generale, una URL ha la seguente forma: protocollo://host:portaTCP/risorsa. Per esempio, nel caso di un video pubblicato su Vimeo.com o su Dailymotion.com: - "https://": rappresenta il protocollo adottato; - "vimeo.com", "dailymotion.com": rappresentano gli indirizzi dei server web a cui è inviata la richiesta; - "367584952", "x7ov2sf": rappresentano il nome del file richiesto, in questo caso l'identificativo numerico univoco di un video pubblicato sui siti corrispondenti.

[17]Tipicamente, con riferimento ai giudizi citati, si tratta di una formale diffida.

[18]Così anche Trib. Roma, ordinanze 22 marzo e 11 luglio 2011, PFA Film s.r.l. c. Google Italia s.r.l. e Yahoo! Italia Inc. (Caso About Elly).

[19]È interessante osservare come nelle decisioni citate questo principio assuma diverse forme: «...la società convenuta poteva facilmente ed autonomamente prendere conoscenza delle violazioni sia per la notorietà dei programmi in questione [...] che, in particolare, per la presenza [...] dei marchi distintivi di RTI»; «...deve disattendersi l'ulteriore censura della necessità dell'indirizzo URL per poter intervenire in modo da rimuovere o impedire in futuro il caricamento dei contenuti lesivi contestati [...] posto che [...] tale dato tecnico non coincide con i contenuti lesivi presenti nella piattaforma»; «...non assume rilievo l'argomentazione difensiva [...] in ordine all'erronea imposizione di un obbligo di controllo preventivo dei contenuti immessi nella piattaforma digitale, in quanto tale obbligo sussiste [...] con riguardo a specifici contenuti [...] una volta avuta conoscenza della natura illecita della diffusione degli stessi»; «... [le diffide] sono idonee a consentire al destinatario di individuare con sufficiente puntualità i singoli contenuti multimediali [...] La responsabilità del provider non può essere esclusa per la circostanza se gli URL [...] gli siano stati indicati o meno».

[20]Si veda, al riguardo, tra l'altro, il breve ma esplicativo intervento di Alfonso Fuggetta.

[21]N. R. Wagner, Fingerprinting, in "Proceedings of the 1983 IEEE Symposium on Security and Privacy", 1983, pp. 18-22.

[22]D. Kundur, K. Karthik, *Video Fingerprinting and Encryption Principles for Digital Rights Management*, in "Proceedings of the IEEE", Vol. 92, No. 6, June 2004.

[23]Cfr. *How Google Fights Piracy 2016 Update*.

[24]BPI-British Phonographic Industry; FIMI-Federazione Industria Musicale Italiana.

[25]Si vedano, a titolo esemplificativo, l'italiana SIAE (siae.it), le statunitensi Nagra-Gudelski Group ex Civolution, Audible Magic, la francese INA.

[26] Al riguardo, M.R. Allegri, *op cit.*, p. 99: «il Tribunale di Torino, nelle ordinanze cautelari relative al caso Delta TV, ha sostenuto non solo l'obbligo per il gestore della piattaforma di rimuovere i contenuti audiovisivi illecitamente diffusi, i cui url erano stati indicati specificamente, ma anche quello di impedire l'ulteriore caricamento sulla piattaforma YouTube dei medesimi materiali, impiegando a tal fine, a propria cura e spese, il software Content ID».

[27]Si pensi a quanto precedentemente detto circa la validità delle segnalazioni di *copyright infringement* prive dell'elenco delle URL ma effettuate con l'indicazione di alcune informazioni relative ai file video, come il titolo, la descrizione, l'autore, i protagonisti, ecc.

[28]Il "prezzo del consenso" corrisponde a uno dei criteri previsti dalla normativa per determinare l'entità del risarcimento dovuto al titolare del diritto da parte dell'utilizzatore responsabile di un illecito sfruttamento dell'opera. Tale criterio è definito dall'art. 158, comma 2, della legge del diritto d'autore che così recita: «Il risarcimento dovuto al danneggiato è liquidato secondo le disposizioni degli articoli 1223, 1226 e 1227 del codice civile. Il lucro cessante è valutato dal giudice

ai sensi dell'articolo 2056, secondo comma, del codice civile, anche tenuto conto degli utili realizzati in violazione del diritto. Il giudice può altresì liquidare il danno in via forfettaria sulla base quanto meno dell'importo dei diritti che avrebbero dovuto essere riconosciuti, qualora l'autore della violazione avesse chiesto al titolare l'autorizzazione per l'utilizzazione del diritto».

[29]Si veda ad esempio: il "Footage Rate Card" della ABC (Australian Broadcasting Corporation); il catalogo della CBC (Canadian Broadcasting Corporation - Archive Sales); il catalogo di Vimeo Stock.

[30]Netflix, Amazon Prime Video, Vimeo On Demand (VOD).

[31]Si veda ad esempio l'articolo 8 del DSA che, con riferimento al contenuto degli ordini emessi dalle autorità giudiziarie o amministrative di contrastare specifici contenuti illegali, menziona tra gli elementi caratterizzanti «[...] uno o più indirizzi URL esatti [...]».

* * *

Digital forensic analysis on the liability of Hosting Providers

Abstract: This paper investigates digital forensic methods related to the assessment of the liability of service providers with respect to user-generated contents. The analysis is developed with particular reference to the sharing of digital video carried out without the prior authorization of the owner. It is inspired by the observation that, at national level and regardless of the peculiarity of the single case, the technical investigation have been the subject of in-depth analysis in the judges' assessments by means of specific forensic analysis concerning some questions that are encountered, with a certain frequency, substantially invariant, in the different judgments.

Keywords: ISP – Hosting Provider – Copyright – Liability – E-commerce – Digital video content