7 *Internet, media, e Intelligenza Artificiale*

Riccardo Traina Chiarini, Maurizio Santoro,
Domenico Anacleto, in collaborazione con Claudia Giorgetti

SOMMARIO

1. La violazione dei diritti IP *online*

1.1. Violazioni ricorrenti del diritto d'autore e diritti connessi

Introduzione La continua evoluzione delle tecnologie informatiche e la conseguente dematerializzazione del patrimonio culturale hanno determinato una notevole facilità di riproduzione e trasmissione online delle opere dell'ingegno, con la conseguente possibilità di condividere agevolmente in rete i contenuti protetti da proprietà intellettuale, e dal diritto d'autore in particolare, attraverso i nuovi canali digitali. Tutto ciò ha aumentato il rischio che la circolazione di tali contenuti avvenga senza che i legittimi titolari possano esercitare un effettivo controllo, con conseguente difficoltà di assicurare una tutela effettiva ai titolari stessi.

Le fonti normative La regolamentazione sostanziale della materia è affidata in primo luogo alla L. n. 633/1941 ("Legge sul Diritto d'Autore" - l.d.a.), con le successive modifiche intercorse. Ci si riferisce, per citare le più recenti, alle modifiche apportare dal D.Lgs. n. 68/2003, emanato il 09/04/2003 in attuazione della Dir. 2001/29 (c.d. "Direttiva InfoSoc") sull'armonizzazione di alcuni aspetti del diritto d'autore e diritti connessi nella società dell'informazione, dal D.Lgs. n. 70/2003, emanato il 09/04/2003 in attuazione della Dir. 2000/31 (c.d. "Direttiva e-commerce") su alcuni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, cui è succeduto in materia il Regolamento 2022/2065 (c.d. "Digital Services Act"), e dal D.Lgs. n. 177/2021, emanato il 09/11/2021 in attuazione della Dir. 2019/790 (c.d. "Direttiva Copyright") sul diritto d'autore e diritti connessi nel mercato unico digitale. Per l'analisi più approfondita di tale ultima direttiva si rinvia al Capitolo 5.

Repressione e prevenzione delle violazioni *online* Dal punto di vista pratico, le violazioni online del diritto d'autore e diritti connessi presentano delle peculiarità, dovute alle caratteristiche intrinseche della rete internet, che rendono estremamente complicata l'individuazione degli autori materiali delle violazioni e la repressione delle stesse. Tali difficoltà impongono ai titolari di contenuti protetti di muoversi in una duplice direzione:

- rintracciare tutte le violazioni dei propri diritti ed i relativi autori;
- mettere in campo un'adeguata strategia di prevenzione.

Nel primo caso rientra la costante e capillare attività di monitoraggio della rete (c.d. *monitoring*), con l'obiettivo di individuare i contenuti illecitamente caricati online. Tale attività è sempre più affidata a *software* in grado di scandagliare a fondo la rete per rinvenire le violazioni e provvedere, spesso sempre in modo automatizzato, all'avvio delle procedure di rimozione dei contenuti illeciti riscontrati (le c.d. procedure di "*notice and take down*", per la

cui analisi si rinvia al successivo par. 1.3.4.). Con l'ausilio di altri strumenti ad hoc è poi possibile ricavare informazioni ulteriori in merito alle violazioni individuate (si pensi, ad esempio, ai dati del soggetto titolare del nome di dominio del sito *web* su cui sono caricati i contenuti illegittimi ed ai dati del titolare dell'indirizzo IP e del fornitore del servizio di condivisione su cui tali contenuti sono ospitati), nonché salvare ed archiviare tutte le informazioni raccolte per poterle utilizzare quali prove delle violazioni rilevate in eventuali futuri giudizi.
Le attività appena descritte, per quanto fondamentali, si inseriscono in un'ottica di accertamento di violazioni già compiute, e dunque mirano alla rimozione di contenuti protetti che sono già stati pubblicati *online*. Per cercare, invece, di prevenire l'illecito caricamento in rete di opere protette, i relativi titolari non possono contare solo sulle proprie forze, ma devono necessariamente rivolgersi ai fornitori dei servizi di caricamento e condivisione in rete di contenuti, richiedendo la loro collaborazione. In particolare a tali soggetti è richiesto, ad esempio nel caso delle piattaforme di condivisione *online*, di effettuare un controllo dei contenuti caricati sul server della piattaforma da parte degli utenti prima dell'effettiva pubblicazione e conseguente fruizione da parte del pubblico. Soltanto in questo modo, infatti, è possibile impedire che i contenuti protetti siano abusivamente pubblicati e condivisi in rete. Uno degli strumenti disponibili in tal senso è il c.d. *fingerprinting*, che consente di scansionare i file caricati dagli utenti e di confrontarli con quelli archiviati su un database gestito dai titolari della piattaforma, in modo da separare i contenuti protetti da quelli che invece costituiscono contenuti originali e sono, perciò, liberamente condivisibili. I gestori delle principali piattaforme di condivisione e pubblicazione di contenuti *online* si sono mossi, già da qualche tempo, nella direzione di operare questo controllo sui contenuti che gli utenti richiedono di caricare. In questo modo, pur non essendo obbligati per legge ad un controllo generalizzato su tutti i contenuti che gli utenti pubblicano, intendono evitare di sopportare i costi, legali ed eventualmente risarcitori, che potrebbero conseguire dall'ospitare sulle proprie piattaforme contenuti protetti senza il consenso dei relativi titolari.

Violazioni più ricorrenti Tra le modalità tipiche più ricorrenti e rilevanti di violazioni online del diritto d'autore e diritti connessi vi sono:
- le piattaforme di condivisione di contenuti (c.d. "*content sharing platforms*");
- i servizi di archiviazione (c.d. "*cyberlockers*");
- le condivisioni tramite *streaming*;
- le condivisioni tramite IPTV ("*Internet Protocol Television*");
- le condivisioni tramite protocollo *peer-to-peer*;
- le applicazioni per dispositivi mobili;
- i *social network*.

1.2. Violazioni ricorrenti dei diritti di proprietà industriale

Introduzione Se, da un lato, la rete internet e i *social network* permettono alle imprese di ottenere un'ampia visibilità con investimenti contenuti, inclusa la possibilità di raggiungere un numero indefinito di potenziali acquirenti, dall'altro, espongono le stesse al rischio di poter difficilmente controllare ed isolare il fenomeno contraffattivo.
Molte delle violazioni dei diritti di proprietà industriale che si verificano attraverso la rete avvengo tramite alcuni dei mezzi già elencati in precedenza. In particolare, attraverso siti della stessa tipologia delle cc.dd. *content sharing platform*, sotto forma di *marketplace* virtuali in questo caso, possono essere venduti al pubblico prodotti contraffattori riportanti marchi o altri diritti di privativa di titolarità altrui. Il che può avvenire, naturalmente, anche sulle corrispondenti applicazioni per dispositivi mobili o sui *social network* (ad esempio, tanto *Facebook* quanto *Instagram* offrono ad oggi la possibilità di acquistare prodotti direttamente sulle rispettive piattaforme).
A questo tipo di violazione, consistente per l'appunto nella vendita di prodotti contraffatti tramite le varie declinazioni della rete internet, si aggiungono ulteriori fattispecie che riguardano variamente l'illecito utilizzo del marchio d'impresa in relazione ai nomi a dominio ed alle ulteriori utilizzazioni commerciali delle parole. A questo proposito vengono in rilievo le pratiche di ***Cybersquatting/domain name grabbing, Typosquatting*, registrazione di nome a dominio confondibile con altro dominio o marchio anteriore, e l'uso del marchio come *metatag* o come *keyword***.
Se di questi temi si è già trattato proprio in relazione alla disciplina dei segni distintivi (per cui si rimanda al precedente Capitolo 2, par. 15.4.1 e ss.), occorre qui invece prendere in considerazione una ulteriore forma di usurpazione di diritti della proprietà industriale in un ambito totalmente digitale, che si verifica laddove ad essere oggetto di copiatura sia la complessiva impostazione grafica di un sito internet.

1.2.1. Pubblicazione di un sito web interamente confondibile

Nozione e caratteristiche Le violazioni sopra richiamate, che coinvolgono esclusivamente il nome a dominio, non esauriscono il novero degli illeciti commessi a mezzo internet che si ripercuotono più in generale sul sito web. In alcuni casi, infatti, l'usurpazione del nome a dominio è solo un aspetto (preliminare) di una più complessa condotta illecita a cui si aggiunge la pubblicazione di un sito web interamente confondibile con quello contraddistinto dal nome a dominio oggetto di violazione.
Questa pratica consiste nella pubblicazione di una interfaccia grafica del sito web (c.d. "*look and feel*") - risultante da una particolare interazione di *layout*, immagini, *sound*, etc. - molto simile a quella del sito web di un *brand* più noto, al

fine di confondere i consumatori in merito all'origine imprenditoriale dei prodotti e/o servizi pubblicizzati e/o offerti in vendita sul sito web 'mascherato'.
In giurisprudenza è stato riconosciuto che la veste grafica del sito o della pagina web possa ricevere tutela ai sensi del diritto d'autore quando sia ravvisabile il requisito dell'originalità (**Corte UE 22/12/2010**, causa C-393/09 in *www.curia.europa.eu*, anche richiamata in **Trib. Bologna 27/07/2012**, in *OneLegale*).
Inoltre, l'imitazione delle caratteristiche del sito internet di un concorrente può integrare altresì la concorrenza sleale confusoria *ex* art. 2598, n. 1, c.c.

> Questa valutazione di confondibilità conduce ad esiti opposti (nel senso di ritenerla sussistente) se si confrontano le modalità con cui i servizi di IEM sono pubblicizzati in Internet [...]. Basti allo scopo considerare le modalità di descrizione dei singoli servizi resi (due colonne affiancate di caselle contenenti ciascuna una breve descrizione del servizio che in entrambi i casi termina con l'espressione "per saperne di più..."; ogni casella ha poi il proprio titoletto racchiuso in un riquadro che nel sito di Index ha forma ovale ed in quello IEM rettangolare); ancora del tutto simile lo sfondo blu delle singole pagine web nonché l'immagine delle singole finestre che si aprono per fornire approfondite informazioni in ordine a ciascun servizio, finestre, peraltro, anch'esse di colore blu all'interno di una cornice bianca. Né vale a scongiurare l'evidente similitudine nelle strutture dei rispettivi siti web la dichiarazione di chi affermi di avere autonomamente elaborato la struttura del sito (**Trib. Venezia 08/03/2006**, in *GADI*, 2006, 669).

1.3. Strumenti alternativi di tutela dei diritti IP *online*

Introduzione In ambiente digitale, tanto per le opere protette dal diritto d'autore quanto per i segni distintivi e le privative industriali in genere e, conseguentemente, per i prodotti sui quali insistano una o più privative industriali o diritti d'autore, l'accertamento e la repressione delle violazioni possono essere particolarmente complessi. In considerazione delle caratteristiche della rete Internet e della vasta tipologia di canali e modalità attraverso cui possono verificarsi gli illeciti, infatti, può rivelarsi da un lato estremamente complicato (se non impossibile, in molti casi) individuare l'autore materiale dell'attività illegittima, dall'altro inutile (o quantomeno sconveniente) il ricorso a metodi "tradizionali" di accertamento e di repressione della stessa.
I titolari dei diritti, per ovviare a questo tipo di problematiche, dovranno dunque innanzitutto provare quanto più ad "anticipare" le violazioni dei propri *asset*, nonché ad individuare soggetti differenti da quelli che materialmente pongono in essere le condotte illecite; soggetti che potrebbero anche essere totalmente estranei all'attività in questione ma che, poiché perpetrata tramite i loro sistemi, possono essere tenuti a collaborare nella individuazione e rimozione delle stesse violazioni.
Rimandando al paragrafo successivo l'analisi della disciplina che regola i doveri (e le relative responsabilità) degli operatori intermediari della rete, vediamo dunque innanzitutto quali sono i principali strumenti e *best practices*

che i titolari dei diritti possono implementare per prevenire, individuare e tenere sotto controllo le violazioni dei propri diritti di proprietà intellettuale ed i rimedi di carattere stragiudiziale che possono essere utilizzati per rimuovere contenuti illegittimi dalla rete.

1.3.1. Strumenti di riconoscimento dei contenuti

Si può parlare di "prevenzione" degli illeciti sulla rete Internet quando il controllo operato, tipicamente in collaborazione tra il titolare dei diritti ed il gestore di una piattaforma a "*user generated content*", avviene in un momento intermedio tra il caricamento di un contenuto sul *server* della piattaforma da parte di un utente e l'effettiva pubblicazione dello stesso per la sua fruizione.
A tal fine è possibile utilizzare strumenti tecnologici che permettono il riconoscimento automatico dei contenuti digitali che vengono caricati o riprodotti su una piattaforma web, tra cui in particolare i *digital watermark*, i codici *hash* e le cc.dd. *fingerprint*; strumenti - che possono essere anche utilizzati congiuntamente tra loro - che incorporano, calcolano e generano informazioni relative a specifici contenuti digitali, che possono così essere identificati, esaminati e, quindi, rimossi nel caso in cui siano stati utilizzati illegittimamente.

Digital watermark Si tratta sicuramente della tecnologia utilizzata da più tempo, e consiste sostanzialmente in un elemento informativo che può essere inserito permanentemente in un contenuto digitale, attraverso il quale se ne può certificare l'autenticità.
Tale elemento può essere percettibile - come il logo del canale televisivo inserito in sovrimpressione su un video - o impercettibile - come una minima variazione di *pixel* in un certo *frame* di un video.
Anche da ciò dipende, naturalmente, la "forza" del *digital watermark*, il cui uso sarà tanto più efficace quanto è minore la possibilità di percepire lo stesso e conseguentemente la semplicità con cui possa essere alterato o rimosso dal contraffattore.

Hash L'inserimento di un codice *hash* all'interno di un file digitale avviene tramite l'uso di un algoritmo - come MD5, SHA-1 o SHA-2 - che crea, per l'appunto, un codice identificatore univoco (una stringa di caratteri alfanumerici) per il file in questione, sulla base dei metadati dello stesso. In questo modo, due file perfettamente identici non solo a livello "visivo" ma, per l'appunto, anche nei rispettivi metadati, avranno lo stesso codice *hash*, mentre due file differenti, anche se la differenza fosse minima o impercettibile, avranno codici *hash* differenti.
La loro utilità risiede nel fatto che i codici *hash* relativi a file che infrangono diritti di proprietà intellettuale possono, ad esempio, essere inseriti in *black list* appositamente mantenute da parte dei gestori delle piattaforme online al fine di individuare e bloccare il caricamento di file illeciti, o rimuoverli se l'accertamento avviene solamente *ex post*.

Lo svantaggio dell'utilizzo del codice *hash* per riconoscimento dei file è che, per l'appunto, tale strumento permette solamente l'identificazione di un file, e non del contenuto portato dallo stesso; una minima variazione del contenuto comporterà quindi una variazione dell'*hash*, impedendo il riconoscimento di quel contenuto come contraffattorio.

Fingerprinting Il c.d. *fingerprinting* digitale è un mezzo di cattura ed identificazione delle caratteristiche uniche di un contenuto digitale specifico, come possono essere le onde sonore dallo stesso generate, o parti di testo in esso contenute o, ancora, alcuni frammenti di un'immagine o di un video.
Viene utilizzato in particolare dalle piattaforme di *video sharing* per permettere ai titolari dei diritti d'autore di "marchiare" con una "impronta digitale" i propri contenuti, così che possano in seguito essere archiviati in un database di riferimento per ogni confronto successivo. Al momento di ogni caricamento da parte degli utenti della piattaforma il contenuto sarà sottoposto ad un'analisi automatica e ad un rilievo delle *fingerprint* dello stesso; il confronto tra queste e quelle inserite all'interno del database determinerà se il contenuto è legittimo, e potrà quindi essere caricato, o meno.

> Il D.Lgs. 08/11/2021, n. 177, di recepimento della Dir. UE n. 790/2019 ha introdotto alla legge sul diritto d'autore (L. 22/04/1941, n. 633) alcuni articoli dettati espressamente per i prestatori di servizi di condivisione di contenuti online, ove viene previsto un onere, a carico degli stessi, di impedire il caricamento non autorizzato di opere protette. In particolare, in recepimento dell'art. 17 della Direttiva, il nuovo art. 102-*septies* prevede che i prestatori di servizi di condivisione di contenuti online, laddove non abbiano ottenuto l'autorizzazione alla trasmissione del contenuto, "sono responsabili per gli atti non autorizzati di comunicazione al pubblico e di messa a disposizione del pubblico di opere e di altri materiali protetti dal diritto d'autore, salvo che dimostrino di avere soddisfatto cumulativamente le seguenti condizioni:
> a) aver compiuto i massimi sforzi per ottenere un'autorizzazione secondo elevati standard di diligenza professionale di settore;
> b) aver compiuto, secondo elevati standard di diligenza professionale di settore i **massimi sforzi per assicurarsi che non sono rese disponibili opere e altri materiali specifici** per i quali hanno ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti;
> c) avere, dopo la ricezione di una segnalazione sufficientemente motivata da parte dei titolari dei diritti, tempestivamente disabilitato l'accesso o rimosso dai propri siti web le opere o gli altri materiali oggetto di segnalazione e aver compiuto, secondo il livello di diligenza richiesto alla lettera b), i massimi sforzi per impedirne il caricamento in futuro".
> Sulla legittimità dell'art. 17 della c.d. Direttiva *Copyright* si è recentemente espressa la **Corte di Giustizia dell'Unione Europea**, che ha innanzitutto ricordato come, in effetti, "al fine di beneficiare dell'esonero da responsabilità (...) i fornitori di servizi di condivisione di contenuti online non solo sono tenuti ad agire immediatamente per far cessare, sulle loro piattaforme, violazioni concrete del diritto d'autore dopo che queste ultime si sono verificate e sono state segnalate loro in modo sufficientemente motivato dai titolari, ma altresì devono, dopo aver ricevuto una tale segnalazione o

allorché tali titolari hanno fornito loro le informazioni pertinenti e necessarie prima del verificarsi di una violazione del diritto d'autore, compiere «secondo elevati standard di diligenza professionale di settore, i massimi sforzi» per evitare che tali violazioni si producano o si ripetano"; così riconoscendo che tali "obblighi impongono pertanto de facto (...) a tali fornitori di svolgere un controllo preventivo dei contenuti che gli utenti intendono caricare sulle loro piattaforme" (**Corte UE 26/04/2022, causa C-401/19**, *Rep. di Polonia c. Parlamento Europeo e Consiglio dell'UE*, in *www.curia.europa.eu*).

FOCUS

IL *CONTENT-ID* DI *YOUTUBE*

L'esempio più significativo di sistema di "prevenzione" delle violazioni di contenuti protetti da diritto d'autore è probabilmente il *Content ID* di *YouTube*.

Tale strumento opera tipicamente tramite *fingerprinting* dei contenuti: prima di ogni pubblicazione viene eseguita automaticamente un'analisi dei file audiovisivi di cui gli utenti vogliano eseguire il caricamento, attraverso la quale il sistema è in grado di confrontarli, a livello contenutistico, con quelli archiviati in un *database* conservato dallo stesso gestore della piattaforma, e quindi di filtrare quelli corrispondenti a contenuti protetti da quelli che invece costituiscono contenuti originali.

Nel funzionamento di tale sistema rimane fondamentale il ruolo attivo dei titolari dei diritti, i quali possono fornire alla piattaforma copia dei contenuti di cui sono proprietari, e di cui il software acquisisce l'impronta digitale che costituisce la base per tutti i successivi raffronti.

Il livello di precisione del *Content ID* di Google/YouTube e degli altri strumenti ad esso similari è oggi molto elevato: come descritto dalla stessa Google sul report «*How Google Fights Piracy*" (novembre 2018, su *https://blog.google/outreach-initiatives/public-policy/protecting-what-we-love-about-internet-our-efforts-stop-online-piracy/*) "*Content ID can now catch efforts to evade detection like changing a video's aspect ratio, flipping images horizontally, and speeding up or slowing down the audio. With advancements in machine learning, Content ID can now detect copyrighted melodies, video, and audio, helping identify cover performances, remixes, or reuploads they may want to claim, track, or remove from YouTube*".

Poiché, nonostante la grande precisione, sussistono incertezze circa l'efficacia di questa tipologia di strumenti, *Content-ID* consente di effettuare un controllo successivo: in caso di blocco al caricamento, l'utente che riceve notizia di rivendicazioni sui video dallo stesso caricati visualizzerà una notifica nell'apposita sezione della pagina relativa al proprio account; egli potrà accettare o meno tale notifica, in tale ultimo caso avendo la possibilità di intraprendere altre azioni, come contestare la rivendicazione, in particolare laddove detenga effettivamente i diritti di utilizzo del materiale protetto da copyright. Come ancora evidenziato dalla stessa Google nel medesimo report, del resto, "*fewer than 1% of Content ID claims are disputed*".

Si noti infine come l'efficienza dello strumento stia anche nel fatto che i titolari dei diritti vengono messi in condizione di monetizzare sugli stessi contenuti caricati da terzi (almeno inizialmente) senza autorizzazione: lo stesso *Content ID* prevede infatti che i titolari dei diritti possano scegliere se inibire il caricamento di contenuti illegittimi o se concedere la pubblicazione delle proprie opere a terzi partecipando ai guadagni da essa generati.