

LA LOTTA ALLA CONTRAFFAZIONE ONLINE –
Strumenti di difesa nell'era dell'Industria 4.0:

NOTICE AND TAKE DOWN

Vicenza, 10 ottobre 2019

(Avv. Francesco Fontana)

Traffic diversion

- **Definizione**

Deviazione della *naturale* navigazione degli utenti

- **Modalità**

Search engine optimization (SEO) - programmazione delle pagine internet che dirotta i visitatori su determinati siti web sfruttando la popolarità acquisita da nomi, marchi, immagini altrui, mediante l'adozione di espedienti inseriti nel codice html sottostante le pagine web che, in ragione dell'elevato contenuto tecnico, risultano visibili dai *crawler* (programmi di scansione automatica) e la cui individuazione richiede elevate competenze informatiche ovvero l'intervento di operatori specializzati

- **Principali illeciti**

Contraffazione di TM (art. 20 c.p.i.) o di industrial design (art. 41 c.p.i. e art. 2, co. 1, n.10 L.d.A.), appropriazione di pregi (art. 2598 co. 2 c.c.), *unfair competition* (art. 2598 co. 3 c.c.), violazione dei diritti connessi alle fotografie *semplici* (art. 87 co. 1 L.d.A.), usurpazione del nome o dello pseudonimo (art. 7 e 9 c.c.), abuso dell'immagine altrui (art. 10 c.c.)

NOTICE AND TAKE DOWN

«*Notice and Take Down*», letteralmente traducibile in “Notifica e rimozione”

--- E' la procedura di notifica ad un soggetto, fornitore di un servizio di comunicazione, che un determinato contenuto viola i diritti di un altro soggetto, o che un contenuto è illecito. Alla ricezione della notifica il soggetto fornitore di un servizio di comunicazione sarà tenuto ad attivarsi per rimuovere quel contenuto

Il NTD ha trovato il suo primo riconoscimento normativo nella legge federale statunitense «*Digital Millennium Copyright Act*» del 1998

Caratteristiche del NTD

Natura del rimedio

- Procedura atipica di contraddittorio con l'ISP e/o con il terzo contraffattore, per segnalare una presunta violazione e chiedere all'ISP di cessarne la prosecuzione

Riferimenti normativi

- In Italia alla procedura del *Notice and Take Down* fa testuale riferimento l'articolo 5 del Regolamento AGCOM del 680/13/CONS del 12 dicembre 2013
- Il riferimento a tale procedura è implicitamente contenuto negli articoli 14, 15 e 16 del decreto legislativo n. 70/2003, allorquando prevedono che l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, possono esigere, anche in via d'urgenza, che il *provider* impedisca o ponga fine alle violazioni commesse

Strumento utilizzato

- Diffida stragiudiziale, specifica e circostanziata, a cura del soggetto leso (cfr. Tribunale Torino, 7/04/2017)

Conseguenze

- Porta l'ISP a conoscenza della presunta violazione
- Comporta per l'ISP l'obbligo di segnalazione all'autorità (e di rimozione)
- Se circostanziata (**URL, impronta HASH, ContentID**), la diffida (può) costituire elemento di prova a carico dell'ISP circa la manifesta illiceità della violazione, con conseguente responsabilità colposa omissiva
- In ipotesi di applicazione diretta della Direttiva Europea, comporta l'obbligo di rimozione immediata anche in assenza di comunicazione dell'autorità competente

Limiti della procedura NTD

- Necessità di inviare una segnalazione per ogni violazione rilevata
- Ampia attività di monitoraggio e di contenzioso con gli ISP con elevati costi gestionali aziendali
- Esercizio di molti abusi
- Impossibilità di combattere il fenomeno della contraffazione per il numero eccessivo di transazioni commerciali

"Digital Millennium Copyright Act"

La normativa americana in tema di copyright (DMCA del 1998) prevede il criterio della **conoscenza effettiva** ("*actual knowledge*") da parte degli ISP, quando il provider riceve una notificazione dal soggetto che lamenta una lesione del proprio diritto (IPR o copyright). In caso di inottemperanza l'ISP è responsabile, a titolo di concorso, dell'illecito.

→ CONOSCENZA SPECIFICA DEL CONTENUTO LESIVO IL QUALE DEVE ESSERE PARTICOLARE ED IDENTIFICABILE

- Affinché la *notification* dell'illecito sia efficace ai fini del DMCA per l'attivazione della procedura di notice and take down, questa deve consistere in un atto scritto con cui il «*copyright holder*» richiede in via formale la rimozione del contenuto.

La segnalazione deve contenere:

- la firma manuale o digitale del notificante;
- l'indicazione del diritto di cui si lamenta la violazione;
- l'individuazione del materiale lesivo, unitamente ad informazioni sufficienti all'individuazione dello stesso da parte del provider e l'indirizzo URL di provenienza;
- numero di telefono ed eventuale indirizzo e-mail dell'istante.

--- Qualora la notifica non ottemperi sostanzialmente ai requisiti indicati, allora questa non rileverà ai fini della determinazione della "effettiva conoscenza" dell'illecito.

Notice and Take Down in Cina

Secondo la Legge sulla Concorrenza Sleale Cinese, le piattaforme online sono responsabili della violazione di diritti della proprietà intellettuale se, pur essendo stata loro notificata una violazione in questo senso, non oscurano le pagine in questione eliminando i link che vi rimandano.

La pagina web può consistere sia in un sito internet vero e proprio oppure in una semplice *company page* all'interno delle diverse piattaforme e-commerce diffuse in Cina (per es. Alibaba, Taobao, T-Mall, Made-in-China).

Le maggiori piattaforme e-commerce in Cina adottano tutte una policy speciale per questo tipo di azioni le quali per essere attivate richiedono:

- la prova che il soggetto richiedente sia il titolare di quel diritto della proprietà intellettuale;
- i link che riportano alle pagine dove sono collocati i prodotti incriminati;
- la *business license* del richiedente.

Questa protezione contro violazioni o atti di concorrenza sleale che si verificano nel web è stata sancita in base alle interpretazioni rese dalla Corte Suprema del Popolo di Pechino.

Ad esempio, per quanto riguarda il «caso DuPont», la Corte ha condannato la società cinese Beijing Guo Wang Information LTD., CiNET, al risarcimento dei danni e alla cancellazione del dominio (dupont.com.cn), per aver violato il diritto all'uso esclusivo del marchio notorio (sentenza del 15/11/2001)

Internet Service Provider

- tipologie e ruoli -

ISP: organizzazione o infrastruttura che fornisce agli utenti servizi internet, il «*provider*» è essenzialmente un intermediario tra chi intende comunicare una informazione ed i destinatari della stessa

- **Access (Mere conduit): semplice trasporto**
internet access, email da server locale
- **Caching: memorizzazione temporanea**
search engine (gratuito e senza filtraggio)
- **Hosting: memorizzazione di informazione**
web space, email, domain name, AdWords, social media, mondi virtuali (my space), cloud computing

Direttiva Europea sul Commercio Elettronico

L'Unione Europea ha approntato una dettagliata normativa al fine di regolamentare l'attività degli intermediari della comunicazione

→ **Direttiva Europea 31/2000/CE** sul commercio elettronico

In Italia la Direttiva E-commerce è stata recepita con il **D. Lgs. 70/2003** che disciplina l'attività dei prestatori di servizi in rete ed, in tale ottica, esenta alcuni di essi (*mere conduit, caching e hosting*) dalla responsabilità per gli illeciti commessi dagli utenti tramite i loro servizi

Access (Mere Conduit)

Art. 14 D.Lgs 70/2003: Responsabilità nell'attività di semplice trasporto

1. Nella prestazione di un servizio della società dell'informazione consistente nel **trasmettere**, su una rete di comunicazione, **informazioni fornite da** un destinatario del servizio, o nel **fornire un accesso alla rete** di comunicazione, il prestatore ***non è responsabile delle informazioni trasmesse*** a condizione che:

- a) non dia origine alla trasmissione;
- b) **non selezioni** il destinatario [**terzo rispetto al destinatario del servizio**] della trasmissione;
- c) **non selezioni** né modifichi **le informazioni** trasmesse.

2. Le attività di trasmissione e di fornitura di accesso di cui al comma 1 includono la **memorizzazione automatica, intermedia e transitoria** delle informazioni trasmesse, a condizione che questa serva solo alla trasmissione sulla rete di comunicazione e che la sua durata non ecceda il tempo ragionevolmente necessario a tale scopo.

3. L'autorità giudiziaria o quella amministrativa, avente funzioni di vigilanza, può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 2, impedisca o ponga fine alle violazioni commesse.

Le lettere a), b) e c) non costituiscono una fattispecie complessa, ma fonti alternative di responsabilità aquiliana.

Caching

Art. 15 D.Lgs 70/2003: Responsabilità nell'attività di memorizzazione temporanea

1. Nella prestazione di un servizio della società dell'informazione, consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, il prestatore **non è responsabile della memorizzazione automatica, intermedia e temporanea** di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltra ad altri destinatari a loro richiesta, a condizione che:

- a) non modifichi le informazioni;
- b) si conformi alle condizioni di accesso alle informazioni;
- c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore;
- d) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni;
- e) **agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione dell'accesso.**

2. L'autorità giudiziaria o quella amministrativa aventi funzioni di vigilanza può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse

Hosting

Art. 16 D. Lgs 70/2003: Responsabilità nell'attività di memorizzazione di informazioni

1. Nella prestazione di un servizio della società dell'informazione, consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore **non è responsabile delle informazioni memorizzate a richiesta di un destinatario** del servizio, a condizione che detto prestatore:

a) **non sia effettivamente a conoscenza** del fatto che **l'attività o l'informazione è illecita** e, per quanto attiene ad azioni risarcitorie, **non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità** dell'attività o dell'informazione;

b) non appena a conoscenza di tali fatti, **su comunicazione delle autorità competenti, agisca immediatamente per rimuovere** le informazioni o per disabilitarne l'accesso.

2. Le disposizioni di cui al comma 1 non si applicano se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore.

3. L'autorità giudiziaria o quella amministrativa competente può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse.

Safe Harbors

17. D. Lgs 70/2003: Assenza dell'obbligo generale di sorveglianza

1. Nella prestazione dei servizi di cui agli articoli 14, 15 e 16, il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.

2. Fatte salve le disposizioni di cui agli articoli 14, 15 e 16, il prestatore è comunque tenuto:

a) ad **informare senza indugio** l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione; (cfr. art. 6 D.Lgs. 231/2001)

b) a **fornire senza indugio, a richiesta delle autorità competenti, le informazioni** in suo possesso che consentano l'**identificazione del destinatario** dei suoi servizi con cui ha accordi di memorizzazione dei dati, **al fine di individuare e prevenire attività illecite** (cfr. art. 6 D.Lgs. 231/2001)

3. *[Se ed in quanto rientri nel campo di applicazione del comma 1, n.d.r.]* Il prestatore è **civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non ha provveduto ad informarne l'autorità competente.**

Evoluzione normativa

- Ante Direttiva E-Commerce (2000/31/CE)

Fonte della responsabilità: contatto sociale (art. 1173 c.c.), esercizio di attività pericolose e/o responsabilità del padrone (art. 2049 e 2050 c.c.), danno da cose in custodia (art. 2051 c.c.), illecito aquiliano (art. 2043 c.c.)

- Post Direttiva E-Commerce (2000/31/CE)

Esclusione obbligo generale di vigilanza; fonte di responsabilità connessa ad un ruolo attivo dell'ISP nella gestione delle informazioni, ovvero per omessa o tardiva esecuzione dell'ordine dell'autorità competente (colpa omissiva o commissiva, cfr. art. 40 c.p.)

Differenze testuali

Art. 16 co.1 b) D. Lgs. 70/2003

1. Nella prestazione di un servizio della società dell'informazione, consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore **non è responsabile delle informazioni memorizzate a richiesta di un destinatario** del servizio, a condizione che detto prestatore:

a) **non sia effettivamente a conoscenza** del fatto che **l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità** dell'attività o dell'informazione;

b) **non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere** le informazioni o per disabilitarne l'accesso.

2.

3. L'autorità giudiziaria o quella amministrativa competente **può esigere**, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse.

Art. 14 co.1 b) Direttiva 2000/31/CE

1. Gli Stati membri provvedono affinché, nella prestazione di un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non sia responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore:

a) non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione, o

b) **non appena al corrente di tali fatti, agisca immediatamente** per rimuovere le informazioni o per disabilitarne l'accesso.

2.

3. Il presente articolo lascia impregiudicata **la possibilità**, secondo gli ordinamenti degli Stati membri, che **un organo giurisdizionale o un'autorità amministrativa esiga** che il prestatore impedisca una violazione o vi ponga fine nonché la possibilità, per gli Stati membri, di definire procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime.

Conseguenze applicative

art. 14 co.1 b) Direttiva 2000/31/CE

-> rimozione immediata

art. 16 co.1 b) D. Lgs. 70/2003

-> rimozione su comunicazione dell'Autorità

In entrambi i casi vi è **l'obbligo giuridico della rimozione** che genera una responsabilità in capo all'ISP che non vi provveda (cfr. Trib. Napoli Nord, 03.11.2016, Trib. Torino, 07.04.2017)

Neutralità dell'ISP

Esenzioni e compiti:

- Non ha un obbligo generale di vigilanza
(cfr. art. 2049, 2050 e 2051 c.c.)
- Non è responsabile degli illeciti di terze parti
- Segnala potenziali illeciti di cui ha conoscenza
- Collabora all'individuazione dell'autore dell'illecito
- Rimuove i contenuti e disabilita l'accesso, su comunicazione delle autorità competenti

--- Principio del «*Network Neutrality*»

L'ISP si deve limitare alla fornitura "neutra" del servizio, mediante un **trattamento puramente tecnico, automatico e passivo dei dati ad esso forniti dai suoi clienti**, sempreché tale trattamento non sia atto a conferirgli (anche per previsione contrattuale) una conoscenza o un controllo dei dati in questione.

Il ruolo “attivo” dell’ISP

Indicizzazione dei siti (SEO) e tracciamento dei contenuti:

- il *domain name* (indirizzo della pagina)
- il titolo della pagina (*tag title*)
- i metatag *description* e *keywords*
- il testo e le immagini della pagina
- frequenza e posizionamento delle parole chiave nel testo della pagina
- i link (collegamenti ad altri siti web)
- la “*link popularity*” (*link presenti nella pagina e link ricevuti dalla pagina, c.d. “google bombing”*)

Indicizzazione e tracciamento per contenuti, risonanza, notorietà, etc., di un sito web costituiscono **comportamenti qualificati** dell’ISP, tali da escludere lo scarico di responsabilità prevista dall’art. 17 D.Lgs. 70/2003 (cfr. Cassazione penale 23/12/2009, n. 49437 in riferimento alla violazione dell’art. 171ter L.d.A. e conseguente sequestro preventivo del sito web ex art. 321 c.p.p.)

(segue) «Indici di interferenza»

L'ISP svolge un ruolo «attivo», andando oltre il mero servizio tecnico, automatico e passivo, allorché compia una o più delle seguenti operazioni sui contenuti:

- filtro
- selezione
- indicizzazione
- organizzazione
- catalogazione
- aggregazione
- valutazione
- uso
- modifica
- estrazione

Responsabilità civile del provider

Il prestatore (**in regime di Safe Harbor**) è civilmente responsabile del contenuto dei servizi nel caso in cui, a seguito della richiesta dell'Autorità giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, **non ha provveduto ad informarne l'Autorità competente. (Art. 17, 3 co. D.Lgs 70/2003)**

→ risarcimento del danno e possibile applicazione di penali per le future violazioni in spregio ad un comando giudiziale

Il prestatore (**non / non più in regime di Safe Harbor per effetto del NTD**) ha un obbligo attivo di vigilanza e monitoraggio specifico delle attività illecite segnalate

→ risarcimento del danno e possibile applicazione di penali, con decorrenza dal NTD

(segue): filtro preventivo ?

NO ad un filtro preventivo delle informazioni memorizzate da hosting

L'ingiunzione rivolta al prestatore di servizi di hosting di predisporre il sistema di filtraggio controverso lo obbligherebbe a procedere ad una sorveglianza attiva della quasi totalità dei dati relativi a ciascuno degli utenti dei suoi servizi, onde prevenire qualsiasi futura violazione di diritti di proprietà intellettuale.

→ La suddetta ingiunzione imporrebbe al prestatore di servizi di hosting una sorveglianza generalizzata, **vietata dall'articolo 15, paragrafo 1, della direttiva 2000/31/CE (Direttiva E-Commerce), contraria alle condizioni stabilite dall'articolo 3, paragrafo 1, della direttiva 2004/48/CE (Direttiva Enforcement), il quale richiede che le misure adottate per assicurare il rispetto dei diritti di proprietà intellettuale non siano inutilmente complesse o costose.**

Tale forma di responsabilità *ex ante* è stata esclusa anche dalla giurisprudenza, cfr.:

--- Corte di Giustizia UE 16.02.2012, C-360/10 (caso Netlog)

--- Cass. Pen., Sez. III, 17.12.2013 n. 5107 (caso Google c. ViviDown)

Non è quindi ammissibile l'ingiunzione, rivolta da un giudice nazionale ad un prestatore di servizi di hosting, di predisporre un sistema di filtraggio: delle informazioni memorizzate sui server di detto prestatore dagli utenti dei suoi servizi; che si applichi indistintamente nei confronti di tutti questi utenti; a titolo preventivo; a spese esclusive del prestatore, e senza limiti nel tempo, idoneo ad identificare i file elettronici contenenti opere musicali, cinematografiche o audiovisive rispetto alle quali il richiedente il provvedimento di ingiunzione affermi di vantare diritti di proprietà intellettuale, onde bloccare la messa a disposizione del pubblico di dette opere, lesiva del diritto d'autore.

Notice and Take Down oppure Notice and Stay Down?

Vi è dibattito internazionale sull'opportunità di passaggio da un mero atteggiamento di «*Notice and Take Down*», ove **gli ISP si attivano solo su segnalazione** degli interessati, ad un approccio più coinvolgente degli ISP, definito «*Notice and Stay Down*».

Notice and Stay Down: alla singola segnalazione da parte dei titolari di diritti che si reputano lesi da contenuti pubblicati o da merci commercializzate sul web segue **la rimozione dei contenuti da parte dell'ISP di tutte le fattispecie di quell'illecito, prevenendo ed impedendo la reiterazione dello stesso.**

→ Nel NSD l'ISP pone in essere sostanziali azioni positive, attraverso adeguati sistemi tecnologici, volte ad eliminare situazioni di contraffazioni seriali (*duty of care*)

(segue): eugenetica processuale del Tribunale di Milano

--- Trib. Milano, sezione specializzata in materia di impresa, decreto 25/03/2019 - ordinanza 22 maggio 2019

Su segnalazione del titolare e del licenziatario dei diritti – nella fattispecie, trattandosi dei diritti sulla trasmissione dei contenuti audiovisivi relativi alle partite del Campionato di Serie A di calcio, rispettivamente la Lega Nazionale Professionisti Serie A e Sky Italia –, il Tribunale di Milano ha concesso, in esito a più procedimenti d'urgenza, provvedimenti cautelari che, già *inaudita altera parte*, hanno ordinato agli *Internet Service Provider* di «mere conduit» convenuti di «adottare immediatamente le più opportune misure tecniche al fine di inibire effettivamente a tutti i destinatari dei propri servizi:

- a), b) *l'accesso agli indirizzi IP ed ai nomi a dominio;*
- c) *l'accesso a qualsiasi altro eventuale indirizzo IP – **purché univoco** – che consenta l'accesso ai menzionati nomi a dominio;*
- d) *l'accesso ai menzionati nomi a dominio di secondo livello anche ove venga associato un top level domain diverso da quelli già indicati che metta a disposizione del pubblico i medesimi contenuti illeciti oggetto del presente provvedimento;*
- e) *l'accesso agli alias derivanti da modifiche al second level domain relativi a tutti gli attuali siti-vetrina e a quelli associati ai main server indicati a condizione che – oltre a rimandare ai medesimi contenuti illeciti innanzi considerati – il collegamento soggettivo con i soggetti responsabili dell'attività illecita attualmente in essere sia obbiettivamente rilevabile*

Ordina in ogni caso ai resistenti di dare esecuzione al provvedimento non oltre ... 48 ore dalla comunicazione da parte della ricorrente dell'eventuale nuovo indirizzo IP, purché univoco, ovvero del nuovo top level domain associato al nome di dominio di secondo livello grandiptv, ovvero dell'eventuale nuovo nome di dominio di secondo livello quanto agli ordini di cui ai punti sub c), d) ed e) ...»

→ AMMISSIBILITA' DI NOTICE AND STAY DOWN CAUTELARE MEDIANTE ORDINE INIBITORIO VALIDO PRO FUTURO CHE IMPONE L'ONERE DI SORVEGLIANZA ED ATTIVAZIONE IMMEDIATA DEGLI ISP SENZA NECESSITA' DI PROMOZIONE DI UN NUOVO PROCEDIMENTO

Rimedi giudiziali

--- Nel caso in cui l'ISP osti alla rimozione del contenuto illecito, il soggetto leso potrà fare ricorso all'Autorità competente per fare valere i propri diritti tramite:

- Procedimento cautelare finalizzato alla rimozione del contenuto illecito (requisiti *fumus boni iuris* e *periculum in mora*)
- Azione civile con richiesta di risarcimento del danno patito
- Sequestro ed oscuramento dei siti web dediti alla contraffazione (in sede civile e penale)

Procedure convenzionali di notice and take down

I principali ISP si sono dotati di forme di autotutela (sistemi effettivi di notice and take down) mettendo a disposizione dei propri utenti procedure per contestare violazioni di copyright o altri illeciti.

Per esempio:

- **FACEBOOK:** l'operatore ha creato una pagina apposita ove i proprietari di diritti trovano informazioni utili su come segnalare violazioni del copyright o di altri diritti da parte degli utenti che pubblicano contenuti sul sito web Facebook. La procedura di segnalazione è piuttosto semplice ed intuitiva: è sufficiente compilare un modulo che in automatico viene inviato al personale preposto da Facebook per analizzare la questione; se la segnalazione è coerente, il personale di Facebook rimuove immediatamente il contenuto in oggetto o ne blocca l'accesso.
- **YOUTUBE:** l'ISP, attraverso le condizioni di utilizzo della propria piattaforma, rende noto ai propri utenti di riservarsi la possibilità di rimuovere dal sito contenuti che violino privative di terzi. Allo stesso modo, informa i titolari dei diritti della possibilità di denunciare tali violazioni attraverso semplici procedure di notifica.
- **YAHOO!:** anche Yahoo! si riserva il diritto, secondo le proprie condizioni di utilizzo del servizio, in determinate circostanze e a sua discrezione, di disattivare e/o sospendere senza preavviso l'account degli utenti che risultino aver violato diritti di proprietà intellettuale di terzi.

Seconda parte

Cenni a questioni trasversali



Temperamento di posizioni

Uso del lemma (nome o TM) altrui nell'ambito della indicizzazione e dei servizi di posizionamento

- nei rapporti tra operatori economici in regime di concorrenza (titolare vs contraffattore)

Sentenza CGE 22/09/2011, Prima Sezione, Causa C-323/09

Interflora / Marks & Spencer

- nei rapporti tra titolare del TM e ISP

Sentenza CGE, Cause riunite, C-236/08, C-237/08 e C-238/08

Google / Louis Vuitton Malletier

Sentenza CGE 22/09/2011

Interflora / Marks & Spencer (Causa C-323/09)

*Il titolare di un marchio ha il diritto di vietare ad un concorrente di fare pubblicità — **a partire da una parola chiave identica a detto marchio che tale concorrente**, senza il consenso del titolare del marchio, **ha scelto nell'ambito di un servizio di posizionamento su Internet** — a prodotti o servizi identici a quelli per i quali tale marchio è stato registrato, quando il predetto uso è idoneo a violare una delle **funzioni del marchio**. Siffatto uso:*

— **viola la funzione di indicazione d'origine** del marchio allorché la pubblicità che compare a partire dalla suddetta parola chiave non consente o consente solo difficilmente all'utente di Internet normalmente informato e ragionevolmente attento di sapere se i prodotti o i servizi menzionati nell'annuncio provengano dal titolare del marchio o da un'impresa economicamente collegata a quest'ultimo oppure, al contrario, da un terzo;

— **non viola**, nell'ambito di un servizio di posizionamento avente le caratteristiche di quello di cui trattasi nella causa principale, **la funzione di pubblicità** del marchio, e

— **viola la funzione di investimento** del marchio ove intralci in modo sostanziale l'utilizzo, da parte del titolare in questione, del proprio marchio per acquisire o mantenere una reputazione idonea ad attirare i consumatori e a renderli fedeli.

*Il titolare di un marchio che gode di notorietà ha il diritto di vietare ad un concorrente di fare pubblicità a partire da una parola chiave corrispondente a tale marchio che il suddetto concorrente, senza il consenso del titolare del marchio, ha scelto nell'ambito di un servizio di posizionamento su Internet, **qualora detto concorrente tragga così indebitamente vantaggio dal carattere distintivo o dalla notorietà del marchio (parassitismo) oppure qualora tale pubblicità arrechi pregiudizio a detto carattere distintivo (diluizione) o a detta notorietà (corrosione)**.*

Un annuncio pubblicitario a partire da una parola chiave siffatta arreca pregiudizio al carattere distintivo del marchio che gode di notorietà (diluizione), in particolare, ove contribuisca a trasformare la natura di tale marchio rendendolo un termine generico.

*Per contro, il titolare di un marchio che gode di notorietà non può vietare, in particolare, annunci pubblicitari fatti comparire dai suoi concorrenti a partire da parole chiave che corrispondono a detto marchio e propongono, senza offrire una semplice imitazione dei prodotti e dei servizi del titolare di tale marchio, senza provocare una diluizione o una corrosione e senza peraltro arrecare pregiudizio alle funzioni di detto marchio che gode di notorietà, **un'alternativa** rispetto ai prodotti o ai servizi del titolare di detto marchio.*

Corte di Giustizia - Cause riunite C-236/08, C-237/08 e C-238/08 Google / Louis Vuitton

La selezione da parte di un operatore economico, mediante un accordo di posizionamento a pagamento su Internet, di una parola chiave che, se utilizzata in una ricerca, comporta la visualizzazione di un collegamento che propone il rinvio a un sito gestito da detto operatore economico al fine di offrire in vendita prodotti o servizi, e che riproduce o imita un marchio registrato da terzi per prodotti identici o simili, senza l'autorizzazione del titolare del marchio, non costituisce di per sé una violazione del diritto esclusivo garantito a quest'ultimo dall'art. 5 della prima direttiva del Consiglio 21 dicembre 1988, 89/104/CEE, sul ravvicinamento delle legislazioni degli Stati membri **in materia di marchi d'impresa.**

... il titolare di un marchio non può vietare al prestatore di un servizio di posizionamento a pagamento di mettere a disposizione degli inserzionisti parole chiave che riproducono o imitano marchi registrati o di predisporre in base al contratto di posizionamento collegamenti pubblicitari a siti creati e visualizzati in modo favorevole, sulla base di tali parole chiave.

Si deve escludere che il prestatore del servizio di posizionamento a pagamento fornisca un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite dal destinatario del servizio ai sensi dell'art. 14 della direttiva del Parlamento europeo e del Consiglio 8 giugno 2000, 2000/31/CE, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»).

Responsabilità penale dell'ISP

--- Leading Case Google vs Vividown (Cass. Pen. Sez. III, 17/12/2013 n. 5107)

Il gestore o il proprietario di un sito web qualificabile come "*content provider*" non può essere ritenuto corresponsabile del reato di illecito trattamento dei dati personali derivante dal contenuto di materiale caricato da terzi in mancanza di una previsione normativa che imponga il controllo preventivo di tutti i dati che transitano sui siti web



- Si esclude che esista un onere di controllo in capo all'ISP.
- Nell'ipotesi di ISP "attivo" (*content provider*) sussiste l'obbligo di corretta informazione, non di filtraggio preventivo.
- Non sussiste una posizione di garanzia ex art. 40 c.p. (reato omissivo improprio)

A diverse conclusioni, si può pervenire qualora si individui nel testo ufficiale della Direttiva la fonte di attivazione immediata dell'ISP, nei casi di omessa o tardiva rimozione dei contenuti illeciti (anche senza comunicazione dell'autorità)

(segue): www.thepiratebay.org

Cassazione Penale, 23/12/2009, n. 49437 (peer-to-peer)

Se il sito web si limitasse a mettere a disposizione il protocollo di comunicazione (quale quello peer-to-peer) per consentire la condivisione dei file, contenenti l'opera coperta da diritto d'autore, ed il loro trasferimento tra utenti, il titolare del sito stesso sarebbe in realtà estraneo al reato. Però **se il titolare del sito non si limita a ciò ma fa qualcosa di più – ossia indicizza le informazioni che gli vengono dagli utenti che sono tutti potenziali autori di uploading, sicché queste informazioni** (i.e. chiavi di accesso agli utenti periferici che posseggono, in tutto o in parte, l'opera), **anche se ridotte al minimo, ma pur sempre essenziali perché gli utenti possano orientarsi chiedendo il downloading di quell'opera piuttosto che un'altra, sono in tal modo elaborate e rese disponibili nel sito**, ad esempio a mezzo di un motore di ricerca o con delle liste indicizzate – **il sito cessa di essere un mero “corriere” che organizza il trasporto dei dati. C'è un *quid pluris* in quanto viene resa disponibile all'utenza del sito anche una indicizzazione costantemente aggiornata che consente di percepire il contenuto dei file suscettibili di trasferimento. A quel punto l'attività del trasporto dei file (file transfert) non è più agnostica; ma si caratterizza come trasporto di dati contenenti materiale coperto da diritto d'autore. Cassazione Penale 16/07/2010, n. 35511**

Non sono responsabili dei reati commessi in rete gli access providers, i service providers e – a fortiori – gli hosting providers, a meno che non fossero al corrente del contenuto criminoso del messaggio diramato (ma, in tal caso, essi devono rispondere a titolo di concorso nel reato doloso e non ex art. 57 c.p.)

- Riferimenti Normativi -

- Direttiva 2000/31/CE (e-commerce)
- Art. 14 Direttiva 2000/31/CE (hosting)
- D. Lgs. 70/2003 (attuazione e-commerce)
- Art. 14 D. Lgs. 70/2003 (Responsabilità nell'attività di semplice trasporto *Mere conduit*)
- Art. 15 D. Lgs. 70/2003 (Responsabilità nell'attività di memorizzazione temporanea *Caching*)
- Art. 16 D. Lgs. 70/2003 (Responsabilità nell'attività di memorizzazione temporanea *Hosting*)
- Art. 17 D. Lgs. 70/2003 (Assenza dell'obbligo generale di sorveglianza)
- Direttiva 2004/48/CE (enforcement)
- Art. 5 c.p.i. e art. 13 Reg. CE 26/2/2009 n. 207 (esaurimento nazionale e comunitario)
- Art. 87 co1 L. 633/1941 (L.d.A., diritti connessi alle fotografie *semplici*)
- Art. 156 L.d.A. (accertamento negativo vs gli intermediari di servizi)
- Art. 163 L.d.A. (inibitoria cautelare vs gli intermediari di servizi)
- Art. 12 co1 b) c.p.i. (novità e domain name)
- Art. 20 c.p.i. (diritti conferiti dalla registrazione)
- Art. 21 c.p.i. (limitazioni del diritto di marchio, uso descrittivo)
- Art. 22 c.p.i. (unitarietà dei segni distintivi, nome a dominio di un sito usato nell'attività economica)
- Art. 1173 c.c. (fonti dell'obbligazione e contatto sociale)
- Art. 2049 c.c. (responsabilità dei padroni e dei committenti)
- Art. 2050 c.c. (responsabilità per esercizio di attività pericolose)
- Art. 2051 c.c. (danno da cose in custodia)
- Art. 110 c.p. (concorso nel reato)
- Art. 40 c.p. (reato omissivo improprio - non impedire un evento che si ha l'obbligo giuridico di impedire, equivale a cagionarlo)
- Artt. 473, 474, 517, 517 *ter* c.p. (reati cd presupposto)
- D. Lgs. 231/2001 (disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica)
- Art. 6 D.Lgs. 231/2001 (contenuto del modello organizzativo e specificità del protocollo)
- Art. 9 D.Lgs. 231/2001 (interdizione dall'esercizio dell'attività, divieto di pubblicizzare beni o servizi)
- Art. 25-bis. D.Lgs. 231/2001 (Falsità in ... segni di riconoscimento)
- Art. 25-bis.1. D.Lgs. 231/2001 (Delitti contro l'industria e il commercio)
- Art. 25-novies. D.Lgs. 231/2001 (Delitti in materia di violazione del diritto d'autore)
- Art. 45 D.Lgs. 231/2001 (applicazione delle misure cautelari interdittive)

Avv. Francesco Fontana

fontana@afpc.it

0444 526690



**Centro Produttività
Veneto**
Formazione & Innovazione



Camera di Commercio
Vicenza



Alberti Fontana Peron Cera
società tra avvocati