

# ASPETTI LEGALI DEL FILE SHARING

Un'introduzione ai problemi legali ed alle tecniche di controllo delle reti P2P

A cura di: Bozzano Michele – Ghio Stefano

Università degli studi di Genova – Dipartimento di informatica e scienze dell'informazione

## Indice generale

ASPETTI LEGALI DEL FILE SHARING.....	1
Problematiche principali.....	2
Leggi in vigore.....	4
Che succede in Italia.....	6
Che succede in America.....	8
Che succede in Francia.....	10
La Dottrina Sarkozy.....	10
HADOPI.....	10
Controllo della rete ed IP framing.....	12
Battaglie legali ed escamotage di fuga.....	16
It must be user error.....	18
Multimedia.....	20

## Problematiche principali

Fonte [[http://it.wikipedia.org/wiki/File\\_sharing](http://it.wikipedia.org/wiki/File_sharing)]

Il file sharing anonimo è cresciuto in popolarità e si è diffuso rapidamente grazie alle connessioni di Internet sempre più veloci e al formato, relativamente piccolo ma di alta qualità, dei file audio MP3. Il nuovo modello di condivisione peer to peer si è rivelato, però, destabilizzante per il sistema del copyright, proprio perché ha provocato una massiccia diffusione di materiale coperto da copyright, spingendo le major discografiche e mediali ad attacchi legali per tutelare i propri diritti. La condivisione di materiali coperti da copyright è ritenuta in genere illegale ma ha acceso diverse discussioni anche a causa delle diverse legislazioni in vigore nei vari paesi.

I problemi di fondo che gli ordinamenti giuridici hanno incontrato nel tentativo di regolamentare questo fenomeno si possono riassumere nelle seguenti tre categorie:

1) Il conflitto con le libertà fondamentali: Il File sharing rientra nella sfera dei diritti fondamentali previsti dalle convenzioni internazionali e dalle carte costituzionali di tutti gli stati democratici, dal momento che si basa sulla comunicazione tra privati. In Italia, ad esempio, l'articolo 15 della Costituzione sostiene la libertà di espressione e accesso alla cultura e all'informazione, mentre l'articolo 21 sancisce l'inviolabilità della corrispondenza e di ogni altra forma di comunicazione tra privati. Questi diritti fondamentali, essendo in posizione preminente rispetto a tutti gli altri, possono essere limitati solo se vi è pericolo di violazione di diritti di pari rilevanza, tra i quali non possono essere annoverati i diritti d'autore.

2) La non percezione di illiceità: Lo scambio di file è oggi molto semplice da effettuare e molto vantaggioso economicamente. Insieme alle moderne tecnologie informatiche, che hanno portato gli individui a non potersi più privare di oggetti e servizi fino a poco tempo fa sconosciuti, ha rivoluzionato le consuete abitudini di vita e risulta essere in costante ampliamento, nonostante sia una pratica riconosciuta come illecita e quindi sanzionabile. Ciò succede perché, a causa della sua capillare diffusione, si registra nel tessuto sociale una mancata percezione dell'illiceità di questo comportamento.

3) L'inesistenza di sistemi centralizzati da colpire: Il modello peer-to-peer rende difficile sanzionare la violazione del diritto poiché la rete è composta da un'infinità di soggetti, difficilmente individuabili e con diverse gradazioni di responsabilità: la posizione dell'utente che si connette saltuariamente e scambia qualche file è diversa da quella di chi viola il diritto di autore condividendo e scambiando migliaia di file, criptando dati e rendendosi non immediatamente identificabile. Il fenomeno ebbe inizio con Napster, uno dei primi software di file-sharing presto bloccato dalla giustizia americana a causa della sua natura: non si trattava ancora di un vero e proprio peer to peer, in quanto gli utenti caricavano i file su una piattaforma comune alla quale si appoggiava il software. Per questo motivo le autorità giudiziarie non ebbero alcuna difficoltà nel trovare un capro espiatorio, ingiungendo ai responsabili del server di cessare la loro attività.

La decentralizzazione è stata una risposta rapida agli attacchi delle major verso le reti centralizzate, al fine di evitare dispute legali ma anche utenti ostili. Questo implica che le reti decentralizzate non possono essere attaccate legalmente, in quanto non fanno riferimento ad un singolo individuo. Anche se il protocollo fondamentale di Internet TCP/IP era stato progettato per essere resistente ad attacchi concertati, i sistemi di file-sharing e di peer-to-peer hanno dimostrato una maggiore resistenza. Per tutto il 2001 e il 2002 tutta la comunità di file-sharing fu in fibrillazione a causa dell'azione di contrasto delle major discografiche e della RIAA. Il server di Napster fu chiuso con

l'accusa di violazione del copyright, ma la comunità reagì unita e compatta, producendo nuovi e differenti client. Da quel momento in poi si sono diffusi programmi di file-sharing grazie ai quali gli utenti possono condividere file senza necessariamente interfacciarsi con una piattaforma centrale, il che ha reso difficile agli ordinamenti giuridici risalire ad un unico responsabile per regolamentare il fenomeno; di conseguenza anche le azioni legali delle major discografiche sono state inefficaci.

Questa evoluzione ha prodotto una serie di client aventi una funzionalità ben definita che rendono la condivisione un fatto effettivo e definito in tutti i sensi consentendo il download e l'upload libero e immune da qualsiasi attacco legale, soprattutto grazie all'anonimato e alla decentralizzazione.

## Leggi in vigore

Fonte [[http://www.governo.it/Governo/Costituzione/1\\_titolo1.html](http://www.governo.it/Governo/Costituzione/1_titolo1.html)]

### Articolo 15 della Costituzione

La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili.

La loro limitazione può avvenire soltanto per atto motivato dell'Autorità giudiziaria con le garanzie stabilite dalla legge.

Fonte [[http://www.interlex.it/testi/l41\\_633.htm](http://www.interlex.it/testi/l41_633.htm)]

### Legge 22 aprile 1941 n. 633

Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (testo consolidato il 9 febbraio 2008)

*Art. 171*

Salvo quanto disposto dall'art. 171-bis e dall'articolo 171-ter è punito con la multa da euro 51 a euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma:

a) riproduce, trascrive, recita in pubblico, diffonde, vende o mette in vendita o pone altrimenti in commercio un'opera altrui o ne rivela il contenuto prima che sia reso pubblico, o introduce e mette in circolazione nello Stato esemplari prodotti all'estero contrariamente alla legge italiana; a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa;

b) rappresenta, esegue o recita in pubblico o diffonde, con o senza variazioni od aggiunte, un'opera altrui adatta a pubblico spettacolo od una composizione musicale. La rappresentazione o esecuzione comprende la proiezione pubblica dell'opera cinematografica, l'esecuzione in pubblico delle composizioni musicali inserite nelle opere cinematografiche e la radiodiffusione mediante altoparlante azionato in pubblico;

c) compie i fatti indicati nelle precedenti lettere mediante una delle forme di elaborazione previste da questa legge;

d) riproduce un numero di esemplari o esegue o rappresenta un numero di esecuzioni o di rappresentazioni maggiore di quello che aveva il diritto rispettivamente di riprodurre o di rappresentare;

e) *(soppresso)*

f) in violazione dell'art. 79 ritrasmette su filo o per radio o registra in dischi fonografici o altri apparecchi analoghi le trasmissioni o ritrasmissioni radiofoniche o smercia i dischi fonografici o altri apparecchi indebitamente registrati.

*1-bis.* Chiunque commette la violazione di cui al primo comma, lettera a-bis), è ammesso a pagare, prima dell'apertura del dibattimento, ovvero prima dell'emissione del decreto penale di condanna, una somma corrispondente alla metà del massimo della pena stabilita dal primo comma per il reato commesso, oltre le spese del procedimento. Il pagamento estingue il reato.

La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 se i reati di cui sopra sono commessi sopra una opera altrui non destinata alla pubblicità, ovvero con usurpazione

della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

La violazione delle disposizioni di cui al terzo ed al quarto comma dell'articolo 68 comporta la sospensione della attività di fotocopia, xerocopia o analogo sistema di riproduzione da sei mesi ad un anno nonché la sanzione amministrativa pecuniaria da da euro 1.032 a euro 5.164.

# Che succede in Italia..

## Il caso Peppermint

fonte [[http://www.google.it/url?sa=t&source=web&ct=res&cd=1&ved=0CAcQFjAA&url=http%3A%2F%2Fwww.massimofarina.it%2Fdocs%2FPEPPERMINT%2520PRIVACY\\_G\\_SATTA.pdf&rct=j&q=peppermint+fatti&ei=wwoS73dloaQsAbYnZimDQ&usg=AFQjCNHZNLRzqUPaSiUc1ypam9DiRvh0xQ](http://www.google.it/url?sa=t&source=web&ct=res&cd=1&ved=0CAcQFjAA&url=http%3A%2F%2Fwww.massimofarina.it%2Fdocs%2FPEPPERMINT%2520PRIVACY_G_SATTA.pdf&rct=j&q=peppermint+fatti&ei=wwoS73dloaQsAbYnZimDQ&usg=AFQjCNHZNLRzqUPaSiUc1ypam9DiRvh0xQ)]

I protagonisti:

### La casa discografica Peppermint GmbH

Titolare dei diritti di sfruttamento del diritto d'autore di alcuni brani musicali condivisi in rete da alcuni utenti.

### La società svizzera Logistep AG

Incaricata di ricercare, con un software apposito, gli indirizzi IP degli utenti che condividevano illecitamente i file musicali.

### Lo studio legale M.&R. di Bolzano

Ha inviato una raccomandata agli utenti "intercettati" con richiesta di pagamento di 330€ per risarcimento danni.

Fonte [<http://punto-informatico.it/2221923/PI/News/peppermint-garante- protegge-utenti-p2p.aspx>]

Una decisione considerata di enorme rilievo quella assunta dal Garante della Privacy a conclusione dell'istruttoria sul caso Peppermint: ha affermato che è "illecito spiare gli utenti che scambiano file musicali e giochi" sulle reti del file sharing. Una decisione che toglie terreno sotto ai piedi di quelle case dell'intrattenimento che fanno e han fatto ricorso al P2P per poter analizzare le attività degli utenti e incastrarli proprio sulla base di quelle attività.

Il software utilizzato per l'operazione sulle reti Gnutella e eDonkey consente di condividere file, di archiviare tutte le informazioni altrimenti volatili, ossia non necessarie una volta concluso il trasferimento dei file nonché di correlare le attività sulle reti P2P di un determinato utente al variare dell'indirizzo IP assunto, nonché del provider utilizzato.

In altre parole "il sistema fsm consente la raccolta dei seguenti dati: indirizzi Ip dell'offerente, il nome e il valore Hash del file, la misure del file, l'user name, il Guid, la data e l'ora del download".

Il software di per sè non viene demonizzato, in quanto non risulta essere intrusivo; cio' nonostante tale attività è stata ritenuta illecita dalle autorità per i seguenti motivi:

- la direttiva europea sulle comunicazioni elettroniche vieta ai privati di poter effettuare monitoraggi, ossia trattamenti di dati massivi, capillari e prolungati nei riguardi di un numero elevato di soggetti;
- viene leso il **principio di finalità**, secondo il quale le reti P2P hanno come scopo il solo scambio di dati tra utenti e nessuna altra attività è lecita;
- vengono violati anche i principi di **trasparenza e correttezza** in quanto i dati venivano raccolti all'insaputa degli interessati;
- viene violato anche il **principio di proporzionalità**, in quanto si è leso il diritto alla segretezza delle comunicazioni laddove non era consentito.

Come risultato della sentenza tutti i dati personali raccolti furono dovuti essere distrutti.

## Spunti riflessivi

fonte [<http://punto-informatico.it/2224659/PI/Commenti/se-privato-intercetta-p2p.aspx>]

Questa sentenza offre uno spunto riflessivo in merito alla registrazione e documentazione del file-sharing altrui **da parte di privati**, anziché dalla polizia giudiziaria.

L'unico movente che può portare a fare indagini di questo tipo è la raccolta di elementi che documentino la possibilità che un reato sia stato commesso, per poi sottoporre il materiale alla Autorità giudiziaria, la quale si occuperà di stabilire se tale reato sia stato compiuto e da chi. Tale attività precede quindi il procedimento e non può mai essere utilizzata come prova, ma solamente come kick-off per il procedimento penale.

Diverso è il caso in cui l'attività svolta può essere considerata come "**documento**", nel qual caso il giudice ha la facoltà di prederlo in considerazione per la decisione.

Per "documento" (o, più correttamente, prova documentale nel processo penale) si intende la rappresentazione/memorizzazione (in qualsiasi forma: manoscritto, registrazione visiva, digitale etc.) di un fatto, che sia formata "al di fuori" del procedimento penale, nel senso cioè che non trovi la sua causa genetica nella necessità di accertare il reato.

Difficile che si verifichi questa ipotesi, soprattutto se a monitorare è la futura parte lesa del processo.

C'è da considerare inoltre che le operazioni suddette comportano da parte dell'investigatore il download dei file compromettenti sul proprio hard disk; azione che non può essere definita come **intercettazione** in quanto parte attiva della comunicazione.

Questi sono i requisiti che deve soddisfare un'intercettazione:

1. oggetto della captazione deve essere una comunicazione riservata
2. chi percepisce la comunicazione altrui deve essere terzo rispetto agli (ignari) interlocutori
3. per "registrare" la comunicazione devono essere impiegati strumenti tecnici

Sul primo punto si trovano in contrasto le opinioni della Corte di Cassazione e del Garante. Non è infatti chiaro se la comunicazione sulle reti p2p sia **privata o pubblica**. Secondo quest'ultimo infatti vengono a mancare, tra l'altro, la simultaneità e l'unicità della trasmissione che sono caratteristiche qualificanti di una comunicazione al pubblico. Per la Corte di Cassazione, al contrario, l'utente pone in essere una sorta di gratuita offerta al pubblico, mettendo a disposizione di chiunque i files e non meritando di conseguenza la tutela prevista dall'articolo 15.

## Che succede in America..

### Verdetti riguardo pagamenti dovuti a violazioni di copyright contrari alla Costituzione

fonte [\[http://www.bittorrentdir.com/verdicts-over-copyright-infringement-charges-violate-us-constitution\]](http://www.bittorrentdir.com/verdicts-over-copyright-infringement-charges-violate-us-constitution)

Dopo i casi delle major e le pesanti sanzioni inflitte a persone trovate "colpevoli" di utilizzare siti web di peer-to-peer file-sharing, il Tribunale federale è ora in acque bollenti per aver violato le sue stesse regole. In molti criticarono e fecero sentire la propria voce a proposito delle "eccessive" multe schiaffate ai "trasgressori", aggiungendo che la corte violò anche i diritti di tali persone ad essere sottoposte a un giusto processo in base al Costituzione degli Stati Uniti.

Va ricordato che diverse persone sono già state accusate dal giudice con sanzioni elevate. Un caso fu quello della ragazza madre, Jammie Thomas-Rasset del Minnesota, a cui fu ordinato dalla giuria di pagare circa 1,9 milioni dollari di danni alle etichette discografiche dopo la condivisione e il download illegale di 24 file musicali tramite Kazaa lo scorso giugno.

Un altro caso che è stato molto apprezzato dalla critica come un grande esempio di violazione costituzionale è quello dello studente universitario Joel Tenenbaum, dove una giuria federale di Boston gli impose il pagamento di 675.000 dollari a favore delle major, dopo la condivisione di circa 30 canzoni su sei differenti reti P2P.

La giuria si è schierata dalla parte delle case discografiche dopo aver "scoperto" che lo studente ha violato gli avvertimenti più e più volte nell'ultimo decennio.

Ma, nonostante l'imposizione di forza del giudice, gli imputati hanno trattato con sprezzo la deliberazione della corte dicendo che avrebbero contestato il verdetto e che sarebbero ricorsi ad un tribunale superiore.

Con questi sviluppi, la Corte si sta ora mordendo la coda da sola, proprio per via di sentenze già imposte in passato, è ora chiamata a rispondere a domande irrisolte sulle presunte violazioni concernenti la violazione del copyright.

Numerosi critici hanno puntato il dito contro la giuria federale e il giudice sostenendo che potrebbero avere difficoltà a giustificare le rigide sanzioni nei confronti dei trasgressori in quanto le decisioni prese risulterebbero illegali perchè in contrasto con la Costituzione degli Stati Uniti.

E' stato inoltre detto che la giuria potrebbe dover dimostrare ancora una volta l'entità del danno arrecato dai trasgressori, dicendo che i danni effettivi in un file musicale per quanto riguarda il diritto d'autore sarebbero impossibili da dimostrare.

Nemmeno gli economisti più pagati potrebbero provare con le loro testimonianze che questi trasgressori stavano effettivamente arrecando un danno o quanto possa essere costato alle etichette.

### RIAA

fonte [\[http://it.wikipedia.org/wiki/RIAA\]](http://it.wikipedia.org/wiki/RIAA)

La sigla **R.I.A.A.** è l'acronimo dell'inglese **Recording Industry Association of America**, *Associazione americana dei produttori discografici*, fondata nel 1952, rappresenta l'industria discografica

americana, il gruppo autorizzato per la certificazione dei dischi d'oro e di platino.

La RIAA è stata recentemente al centro delle controversie sullo sviluppo del peer-to-peer, l'MP3 e la condivisione di file. I suoi tentativi di difendere gli interessi delle major sono stati visti da alcuni come un comportamento lesivo sia nei confronti dei consumatori che degli artisti.

Gli avversari della RIAA affermano che questo gruppo forma un cartello che gonfia artificialmente e fissa i prezzi dei CD. Questa affermazione sarebbe dimostrata dal fatto che le Big Five (BMG, EMI, Sony Music, Universal Music e Warner) distribuiscono almeno il 95% di tutti i CD a livello mondiale.

Dal 1988 al 2003, presidente e chief executive officer della RIAA è stata Hilary Rosen che ha chiaramente criticato l'uso del peer-to-peer. Sotto la sua direzione, la RIAA ha intrapreso un'aggressiva campagna legale per fermarne la diffusione.

La digitalizzazione della musica e la disponibilità di mezzi di comunicazione digitale piuttosto economici, unite alle tecnologie di file-swapping, ha messo in crisi le major discografiche. Molti credono che queste tecnologie siano in grado di eliminare completamente la distribuzione fisica dei CD musicali, minacciando di fatto l'esistenza di molte aziende che attualmente dominano il marketing e la distribuzione nel settore.

La RIAA cerca di proteggere i suoi interessi sensibilizzando i politici e formando delle lobby al fine di modificare le leggi sul copyright. Come risultato i membri della RIAA negli U.S.A. hanno ora a disposizione una legislazione speciale che protegge e rinforza il loro modello industriale. Queste leggi le aiutano a citare in giudizio molti provider e utenti che utilizzano il peer-to-peer.

## Che succede in Francia..

### La Dottrina Sarkozy

Fonte [<http://www.webmasterpoint.org/news/>]



Denis Olivennes, ideatore della legge delle tre disconnessioni, nota come Dottrina Sarkozy, può ritenersi soddisfatto. L'Assemblea Nazionale francese, con 296 voti contro 233, ha approvato la legge HADOPI, stoppata a sorpresa in una precedente votazione. Ora manca solo un passaggio al Senato, che appare scontato, e il parere del Consiglio Costituzionale, al quale l'opposizione ha già annunciato di voler presentare ricorso.

Un altro scoglio da affrontare potrebbe presentarsi in sede europea, visto che il Parlamento UE ha stabilito che la disconnessione da Internet può avvenire solo su pronunciamento dell'autorità giudiziaria. L'HADOPI, invece, è un'autorità amministrativa. Ma Christine Albanel, Ministro della Cultura francese, è sicura che non ci saranno problemi, perché l'emendamento UE non riconosce l'accesso a Internet come una libertà fondamentale, mentre afferma che le decisioni delle autorità giudiziarie sono necessarie solo quando a essere minacciati sono i diritti e le libertà fondamentali dei netizen.

Se tutto procederà come previsto da Albanel, gli internauti francesi colti per tre volte a scaricare materiale protetto da copyright saranno disconnessi da Internet e dovranno anche continuare a pagare l'abbonamento per l'accesso per tutta la durata del contratto.

### HADOPI

Fonte [<http://nexa.polito.it/battaglia-hadopi-htm>]

Il termine HADOPI è l'acronimo francese che sta per "Haute Autorité pour la Diffusion des Oeuvres et la Protection des droits sur Internet", letteralmente "Alta Autorità per la diffusione delle opere e la protezione dei diritti su Internet".

Esso contrassegna sia la legge n°2009-669 del 12 giugno 2009, che l'autorità amministrativa incaricata di adempiere a tale compito.

Inoltre Hadopi designa anche il nome del corpo legislativo promesso la sera delle sue elezioni dal presidente francese Nicolas Sarkozy, artefice dell'omonima Dottrina.

La motivazione di questa legge nasce dal fatto che il pirata è visto come il nemico da abbattere, colui che condivide opere su Internet senza autorizzazione sarebbe il responsabile della crisi dell'industria dell'intrattenimento.

La promulgazione della legge non avviene certo senza intoppi, ma il 22 settembre 2009 il testo viene quasi interamente approvato dal Consiglio Costituzionale .

La presenza di una legge che condanni la condivisione di opere protette dal diritto d'autore non implica però che l'attuazione della stessa sia pratica ordinaria.

Già lungo il suo iter burocratico la legge perse molto in efficacia; il 10 giugno 2009 il Consiglio impose che le sanzioni dovevano essere pronunciate da un giudice e non potevano essere di massa.

La sospensione dell'accesso a internet nei confronti di un cittadino diventava così competenza esclusiva del giudice, il quale godeva inoltre di discrezionalità; la legge stabilisce che egli ha il dovere di tenere conto delle circostanze in cui l'atto era compiuto e della situazione socio-economica in cui versava l'autore.

La risposta graduata perdeva così la possibilità di rispondere a un fenomeno di massa con sanzioni di massa.

Il Ministro della Cultura incaricato del disegno di legge ha tenuto a specificare la presenza che questa è stata fondamentale una battaglia ideologica.

Si è voluto fare passare il messaggio che creatori, artisti, registi, musicisti hanno il diritto di essere remunerati per quello che fanno, e consapevolizzare i cittadini che il comportamento tenuto è illegale e provoca oltremodo dei disastri nel mondo dell'industria.

Il fatto che questo messaggio sia o non sia passato è quantomeno dubbio; ogni critica alla HADOPI ha goduto di ampi spazi sui mezzi di comunicazione di massa, che non hanno certo contribuito a far vedere la legge di buon occhio, mentre i pochi sondaggi in materia non hanno ottenuto le percentuali sperate.

# Controllo della rete ed IP framing

## Controllo della rete

fonte [[http://dmca.cs.washington.edu/uwcse\\_dmca\\_tr.pdf](http://dmca.cs.washington.edu/uwcse_dmca_tr.pdf)]

Una rete P2P “di successo” deve garantire ai propri utenti stabilità anche in caso di downtime di alcuni peer o server della rete ed anonimato.

L'anonimato è molto importante dal punto di vista legale in quanto è l'unica difesa che un utente ha dalle minacce di disconnessione o multa viste in precedenza.

Siccome chi tenta di far valere il proprio copyright adotta metodi del tipo “caccia alle mosche col bazooka”, si rende necessario, quantomeno per quei pochi utenti corretti, fornire meccanismi di protezione da metodi di controllo non proprio democratici ed a volte nemmeno costituzionali.

L'idea è difatti quella di punire gli utenti che si riescono a cogliere sul fatto in maniera esemplare – ed a volte eccessivamente esemplare, scadendo quasi nel ridicolo – per dare un avvertimento agli altri, così facendo non ci sofferma nemmeno troppo sull'andare a verificare effettivamente la reale colpevolezza dell'utente in questione e si applica giustizia sommaria. A tutto questo va aggiunto che spesso gli organismi legislativi cui spetta di decidere della questione non hanno una chiara visione della materia finendo addirittura con l'emettere sentenze del tutto contraddittorie.

Solitamente le case cinema-discografiche affidano il controllo del traffico di materiale illegale a società terze che monitorano la rete internet, in particolare le reti P2P, alla ricerca di violazioni del copyright per procedere successivamente con misure deterrenti (ad esempio con l'avvertimento DMCA di cui parleremo a breve) o più drastiche come nel caso delle multe e delle “tre disconnessioni”.

Uno studio dell'università di Washington legato alla rete bittorrent, mostra come funzionino i moderni “crawler” per reti P2P e come si siano evoluti nel periodo di tempo di un anno (2007-2008).

## DMCA ed EUCD

Prima di analizzare il loro lavoro, andiamo a vedere cosa sia l'avvertimento DMCA citato in precedenza. Il DMCA (Digital Millennium Copyright Act) è una legge USA del 1998 che sanziona coloro che non rispettano il copyright, soffermandosi con attenzione sulle infrazioni via internet. L'equivalente europeo è l'EUCD (European Union Copyright Directive) del 2001 assieme all'ECD (Electronic Commerce Directive). Sia il DMCA che l'EUCD attestano l'esenzione diretta ed indiretta di responsabilità per gli OSP (Online Service Provider, ISP (Internet Service Provider) inclusi) ed eventuali altri intermediari – sotto determinate condizioni- , puntando quindi direttamente all'utente finale.

Agli OSP viene infatti garantita l'esenzione dalle accuse solo se accettano di seguire linee guida particolari ed implementano sistemi di bloccaggio e/o rimozione dei contenuti ritenuti violazione di copyright, da attuarsi nel momento in cui tali organizzazioni ricevano una lettera di notifica di violazione da parte di un detentore di copyright od un suo agente. L'OCILLA (Online Copyright Infringement Liability Limitation Act), questo il nome della sezione 2 del DMCA, non nega però la

possibilità di dimostrare che il materiale per cui si è ricevuta la notifica non costituisca effettiva violazione. L'OCILLA sancisce inoltre la possibilità di inviare mandati di comparizione agli OSP per testimoniare riguardo l'identità dell'utente incriminato.

Il modo con cui si "convincono" gli ISP ad implementare tali controlli non sempre è completamente legale, come nel caso dell'ISP Irlandese Eircom [<http://www.eircom.net/>], che ha ricevuto un misterioso aiuto finanziario [<http://torrentfreak.com/why-the-ifpieircom-anti-piracy-deal-sucks-090131/>] proprio prima di iniziare una collaborazione [<http://torrentfreak.com/irelands-largest-isp-starts-throttling-and-disconnections-090725/>] con l'IFPI [<http://www.ifpi.org/>], che "rappresenta l'industria discografica su scala mondiale".

### Why my printer received a DMCA takedown notice

In precedenza, Napster su tutti, i contenuti della rete passavano attraverso uno o più server centrali, che mantenevano indici puntanti agli utenti presso i quali tali contenuti erano disponibili. In questo caso si parla di *indexer*, organizzazioni cui peraltro erano rivolte le varie cause legali. Con le moderne reti di tipo bittorrent o gnutella, non esistono più server centrali presso cui reperire informazioni sui file cercati, ma si ha una rete decentralizzata. Nel caso bittorrent la ricerca di file avviene in metodo analogo a Napster, sebbene le informazioni recuperate non siano riconducibili effettivamente al file stesso (è il caso dei "fake") e nemmeno agli utenti che ne dispongono, si parla perciò di *tracker*.

Non avendo più un'organizzazione fisica contro cui accanirsi si cerca di attaccare la pirateria in vari modi spaziando dalle accuse ai siti di tracker fino ad arrivare all'utente della rete.

La ricerca di cui analizziamo i risultati, mostra come le nuove tecniche impiegate non siano particolarmente efficienti, risultando approssimate ed eludibili. Nello specifico, i ricercatori sono stati in grado di ricevere qualche centinaio di lettere DMCA sebbene non abbiano mai partecipato attivamente alla rete P2P.

Trace	Complaint type						Totals	
	Movie	Music	Television	Software	Books	Mixed	Complaints	Swarms obs.
August, 2007	82	0	11	18	11	0	122	55,523
May, 2008	200	0	17	46	0	18	281	27,545

**Tabella 1: avvertimenti DMCA ricevuti durante l'esperimento. Tutti falsi positivi.**

Le società di controllo adottano due metodi principali per identificare gli utenti che commettono infrazioni:

- **indiretto**, basandosi sull'insieme di peer ottenuto durante il bootstrap con il tracker e considerando tale lista come valevole per asserire quegli IP come parte attiva nello scambio dati;
- **diretto**, connettendosi direttamente con il peer sospetto e scambiando dati con lo stesso.

L'approccio diretto è più efficace ed è quello utilizzato dalla RIAA per monitorare la rete gnutella, sebbene sia più esigente in termini di risorse e di tempo.

Per le reti di tipo bittorrent si utilizza invece l'approccio indiretto, da qui la possibilità di effettuare

spoofing ed aggirare i filtri.

Per poter essere identificati come peer attivi, i ricercatori hanno inviato richieste di aggiornamento a vari tracker continuamente ad intervalli di 15 minuti da differenti postazioni all'interno della rete universitaria finendo col ricevere così le notifiche riportate in tabella 1 senza aver (s)caricato alcun dato. Le informazioni relative al 2007 sono state collezionate in seguito ad uno studio differente, sempre su rete bittorrent ma non mirato all'analisi che si sta effettuando ora.

Con tecniche di framing e spoofing sono riusciti a ricevere avvertimenti DMCA come segue:

Host type	Number of complaints
Desktop machine (1)	5
IP Printers (3)	9
Wireless AP (1)	4

**Tabella 2: Falsi positivi ricevuti su indirizzi "framed".**

Il fatto che sul totale di 281 lettere ricevute solo 18 siano state effettivamente indirizzate a macchine "framed" deriva dal fatto che lo spoofing si può effettuare solo se il tracker supporta una particolare estensione del protocollo. Non sapendo quali tracker offrissero questa possibilità, non è stato possibile incrementare ulteriormente tale risultato.

La prima richiesta di un client bittorrent ad un tracker ha due scopi:

- sollecitare una risposta con cui fornire al client appena entrato un set di peer cui collegarsi
- notificare al tracker stesso che è disponibile un nuovo client verso cui indirizzare future richieste

### IP spoofing

Normalmente, i tracker registrano l'IP sorgente della richiesta come l'indirizzo verso cui indirizzare altri peer, alcuni tracker tuttavia supportano la possibilità per il client di indicare un indirizzo alternativo verso cui instradare richieste per poter supportare anche client con proxy od in una rete NAT. Utilizzando questa estensione è quindi possibile fare framing verso altri IP mediante una semplice richiesta HTTP.

```
wget 'tracker_URL/announce.php?info_hash=%0E%B0c%A4B%24%28%86%9F%3B%D2%CC%BD%0A%D1%A7%BE%83%10v&peer_id=-AZ2504-tUalhrpbVcq&port=55746&uploaded=0&downloaded=0&left=366039040&event=started&numwant=50&no_peer_id=1&compact=1&ip=A.B.C.D&key=NfBFoSCo'
```

In questo caso si contatta il tracker indicando A.B.C.D come IP verso cui instradare le future richieste. Oltre a quelle riportati nella tabella precedente, erano stati "accusati" anche altri IP che però non erano associati ad alcuna macchina e quindi non erano pingabili da remoto. Per tali IP non è stata ricevuta alcuna notifica DMCA.

Oltre allo spoofing IP da client, esistono molti altri metodi che consentono di effettuare framing di IP. Vediamone qualcuno.

### Via tracker framing

Siccome i file .torrent sono generati dall'utente e successivamente caricati sui vari tracker, è possibile creare file ad hoc e poi metterli in circolazione, dal punto di vista dell'utente un tracker che sia vittima di tale attacco è indistinguibile dagli altri. In questo caso, indipendentemente dalla partecipazione dell'IP "framed" alla rete, il tracker lo restituirà ad ogni richiesta, esponendolo al

crawling delle società di controllo.

### **DHCP timeout e reti aperte**

E' inoltre possibile giocare sulle riassegnazioni di indirizzi via DHCP. Consideriamo l'esempio seguente:

Bob utilizza un client bittorrent connettendosi tramite rete wireless con un IP dinamico ottenuto presso un punto d'accesso pubblico. Ad un certo punto Bob si disconnette dalla rete, senza che il tracker che stava utilizzando sia notificato dell'evento. Successivamente Alice accede alla stessa rete ed ottiene l'IP precedentemente assegnato a Bob. Se la società di controllo inviasse una notifica adesso all'ISP che gestisce la connessione usata da Bob, il timestamp di tale avvertimento legherebbe Alice all'IP incriminato creando un falso positivo. Chiaramente dipende tutto dai tempi di aggiornamento del tracker e di riassegnazione di indirizzi IP.

Un problema analogo si pone nel caso in cui qualcuno disponga di un router-access point wireless e non lo protegga adeguatamente o abbia il PC infettato con malware.

### **Man-in-the-middle**

Le risposte dei tracker non sono cifrate per cui si prestano facilmente ad attacchi di tipo man-in-the-middle, chiunque si posizioni tra il tracker e la società di monitoraggio è in grado di modificare la risposta del tracker stesso. Attacchi dello stesso tipo possono essere messi in piedi a livello overlay, sfruttando la rete DHT ed il peer gossip ritornando falsi IP alle richieste.

### **Blacklist**

Un metodo diffuso per evitare i filtri di controllo è quello delle blacklist, elenchi mantenuti a mano di IP malevoli con cui è preferibile non instaurare connessioni. Il problema di queste liste è che non esiste un metodo automatizzato per effettuare l'aggiornamento, sebbene sia possibile distinguere il comportamento di un peer che partecipa alla rete da quello di uno che la scansiona.

# Battaglie legali ed escamotage di fuga

## Battaglie legali

Le continue pressioni da parte dei detentori di copyright per far valere il proprio diritto alle royalties hanno prodotto una lunga serie di battaglie legali con esiti altalenanti. Essendo incapaci di attuare politiche mirate a debellare il problema e non avendo una reale conoscenza dello stesso, si è finiti a minacciare e/o corrompere direttamente gli ISP ed i siti di tracker.

Nel primo caso si riesce a far sì che gli ISP applichino filtri al traffico di rete per limitare il consumo di banda da parte degli utenti coinvolti negli scambi P2P, arrivando fino alla legge delle tre disconnessioni. Questo metodo si rivela efficace solo per quelle reti che si appoggiano a server centralizzati per la ricerca di file.

Per ovviare a tale problema, i moderni client P2P offrono funzionalità di cifratura delle connessioni e reti di tipo serverless (DHT per bittorrent e KAD per gnutella ad esempio).

Per i tracker invece, essendo presenti in quantità molto maggiori rispetto agli ISP (che solitamente sono 2-3 per paese), ed avendo i server localizzati geograficamente in luoghi dove le leggi contro la pirateria informatica sono deboli e/o permissive, non si riesce ad agire direttamente e si può solo tentare di instillare terrore nei gestori del server/sito.

In questo caso i risultati variano dalle burle in risposta alla chiusura del sito in questione.

## Le burle

Spesso le richieste di rimozione dei contenuti, chiusura del sito e pagamento di multe, arrivano dall'America (USA in particolare), ed a causa delle differenti legislazioni vigenti nei paesi in cui risiedono i server che ospitano il sito finiscono col risultare legalmente errate e/o inattuabili. Per questo motivo sovente i siti di tracker che le ricevono si fanno gioco dei richiedenti. The Pirate Bay su tutti è un esempio lampante della cosa, avendo addirittura aperto una sezione apposita [<http://thepiratebay.org/legal>] all'interno del sito in cui raccolgono tutte le minacce legali ricevute con le relative risposte.

Alcuni possono scegliere di continuare a fornire il servizio, magari proseguendo la battaglia legale iniziata, è l'esempio di IsoHunt [<http://torrentfreak.com/images/isohunt-statement.pdf>].

## La modifica nel metodo di fornitura del servizio

Non tutti preferiscono farsi gioco degli altri quando ci sono di mezzo richieste legali, ma non volendo interrompere il servizio, lo modificano in modo che appaia il più legale possibile. Le accuse mosse agli indexer erano quelle di fornire hosting a materiale coperto da copyright e non eliminarlo, nel caso dei tracker questo non è più vero in quanto il materiale in questione non risiede sul server, che si limita solamente a fornire un elenco di nodi da contattare per cercare il file desiderato. Si cerca quindi di mostrare che mantenere un elenco di contatti presso cui ricercare il

file sia analogo all'avere il file stesso.

Chiaramente l'accusa non corrisponde alla realtà, ma le forti pressioni legali possono portare a decidere di modificare il servizio in modo da essere al sicuro da future minacce dello stesso tipo. Si passa quindi dall'offrire un servizio di hosting di file .torrent, al fornire un magnet link, che non viene scaricato dal browser ma aperto direttamente dal proprio client P2P.

Si ha uno schema URI (Uniform Resource Identifier) che definisce la struttura dei link magnet. Tali link identificano un file non mediante locazione o nome, ma contenuto, più precisamente, mediante un hash del contenuto. Essendo che i file sono identificati mediante contenuto e/o metadati, si può pensare al magnet link come una specie di URN (Uniform Resource Name), piuttosto che un URL (Uniform Resource Locator). Impiegarlo in una rete di tipo P2P può essere molto utile in quanto permette di referenziare le risorse senza la necessità di avere un particolare host sempre disponibile.

Oltre ad essere un modo per evitare le accuse rivolte esplicitamente al meccanismo di tracking, i magnet link sono anche considerati essere il futuro della condivisione e sempre più tracker stanno affiancando i due servizi, per passare in futuro definitivamente al secondo. I magnet link fanno ampio uso della rete DHT, che garantisce maggiore anonimato.

### **La modifica dell'entità del sito**

Quando la paura diviene troppo elevata, è possibile che il sito decida di cambiare interamente la sua natura "convertendosi" al lato chiaro della forza. In questo caso si cessa di fornire tracking per qualsiasi tipo di file e si accettano solamente contenuti verificati oppure si consente l'upload di tali contenuti solamente agli utenti la cui identità sia stata verificata. E' questo il caso recente di Mininova [<http://mnstat.com/images/blog/index.html>], che ha abbandonato la veste di tracker torrent restando sito di Content Distribution per uniformarsi alla sentenza della corte di Utrecht.

Nei casi più spinti si può decidere di chiudere definitivamente il sito.

Va notato che la natura pubblica o privata del sito stesso è un fattore importante da considerare per scegliere dove colpire. Solitamente in tracker privati hanno un numero di iscritti ridotto a causa delle politiche di "user share ratio" adottate. Tali politiche garantiscono all'utente una serie di bonus, tra cui anche una maggiore priorità nella connessione ad altri peer per scaricare quanto voluto. Utenti *leecher* o *free rider* saranno perciò maggiormente rivolti verso tracker pubblici, facendone il bersaglio ideale per la caccia da parte delle società di controllo.

Impostare un tracker come privato è un'operazione semplice, basta difatti settare il bit relativo all'interno del file .torrent. Se non lo fa l'utente, molti tracker privati lo inseriscono in automatico. Questo significa che utilizzando un tracker privato non è possibile sfruttare la rete DHT, ma non è vero che è necessario che quest'ultima sia disabilitata.

## It must be user error

### Il problema è del P2P o dell'utente?

Se le reti P2P sono nate con lo scopo di permettere la facile collaborazione tra diversi host per raggiungere uno scopo comune, il problema dell'utilizzo illegale è da imputare alla rete stessa o agli utenti che ne usufruiscono?

Una ridottissima percentuale del traffico P2P per file sharing è legata alla diffusione di programmi opensource ma è davvero una goccia nell'oceano rispetto al resto dei file che circolano. Riguardo gli aspetti di controllo e censura dei contenuti, la rete ed i client da soli non forniscono strumento alcuno per impedire lo scambio di materiale coperto da copyright, anzi mettono a disposizione strumenti che realizzano esattamente l'idea oposta come i protocolli di offuscamento o le blacklist, sono allora da incolpare del problema?

La risposta è palesemente no. Sebbene sia più facile cercare di colpire la rete che gli utenti come nel caso di WinMX [<http://www.azpoint.net/software/download/11686/WinMX-chiude-i-battenti-Per-sempre.asp>].

Casi di mal utilizzo di client di file sharing non si limitano solamente all'infrazione di qualche legge sul diritto d'autore - diritto ampiamente questionabile sia per come è formalizzato sia per i prezzi del materiale che protegge - ma possono anche sfociare in operazioni dannose per sè stessi o per per gli altri.

Ogni client prevede difatti la possibilità di condividere all'interno della rete file che risiedono sull'host in questione. Un utente poco accorto potrebbe finire con il condividere informazioni personali e/o private e vederle circolare velocemente oppure rilasciarle di proposito, come nel caso delle dichiarazioni dei redditi 2005 [<http://termometropolitico.wordpress.com/2008/05/02/i-redditi-online-sui-peer-to-peer-si-trova-di-tutto/>], rese pubbliche senza un valido motivo direttamente dall'agenzia delle entrate, poi frettolosamente rimosse. Ma non abbastanza velocemente, ancora oggi è difatti possibile reperire tali informazioni (evitando fake e malware vari) sulla rete eMule.

Un caso di "beata ignoranza" arriva invece direttamente dall'America [[http://news.cnet.com/8301-10787\\_3-10184785-60.html](http://news.cnet.com/8301-10787_3-10184785-60.html)] dove un client P2P installato all'interno di una rete sicura ha fatto fuoriuscire i piani dell'intera flotta degli elicotteri presidenziali, modifiche e migliorie in corso compresi. Sam Hopkins, della compagnia Tiversa, che per prima ha identificato il fatto, commenta:

*It was on the Gnutella network. Someone installed it and it may have been a buggy client. All it takes is for someone to say, "Hey, do you have anything on this client?" and it gets downloaded. We see 50 of those a day. There was a large publicly traded company which accidentally just disclosed all their forecasts and M&A plans throughout 2009. A person leaked all his files and all his internal e-mail conversations as well as his calendar and all his contact information.*

D'altronde per sparare con un fucile serve qualcuno che preme il grilletto.

Le reti P2P inoltre possono essere impiegate per molti altri scopi non necessariamente legati al file sharing. Abbiamo la possibilità di:

- creare connessioni per il cloud computing, un esempio è [Folding@home](http://folding.stanford.edu/) [<http://folding.stanford.edu/>], lanciato dall'università di Stanford. In questo caso l'utente

installa un piccolo software e decide di mettere a disposizione una certa quantità di risorse che verrà impiegata per effettuare un calcolo distribuito per studiare proprietà legate alle proteine;

- oltrepassare blocchi di censura, come nel caso della rete Freenet [<http://informatica.aulaweb.unige.it/mod/wiki/view.php?id=10175&page=Freenet>];
- fornire distribuzione digitale di materiale protetto da copyright, come nel caso della piattaforma Steam [<http://store.steampowered.com/>], un progetto Valve [<http://www.valvesoftware.com/>], che ha ultimamente aumentato di molto la sua fama proprio perchè fornisce la possibilità all'utente di ricevere un determinato contenuto direttamente sulla propria macchina, pagando un prezzo inferiore rispetto al negozio fisico;
- distribuire materiale di vario tipo utilizzando canali di comunicazione molto rapidi, la Blizzard ad esempio distribuisce patch e client del suo gioco più noto tramite la rete bittorrent e non è l'unica [<http://www.techdirt.com/articles/20090721/0354125606.shtml>].

Anche con nomi del livello di Asus, Blizzard, Valve e molti altri, dalla parte del P2P per la distribuzione di contenuti, questa pratica è ancora molto osteggiata ma non siamo riusciti a trovare una motivazione valida.

## **Multimedia**

Un video youtube che fa il paragone tra le pene per la pirateria ed altri reati non informatici ma più gravi: [http://www.youtube.com/watch?v=io1c\\_B6fL08](http://www.youtube.com/watch?v=io1c_B6fL08)

Una vignetta xkcd sui metodi di controllo adottati per combattere la pirateria: <http://xkcd.com/86/>