# Luci ed ombre: il *file sharing* tra diritto d'autore e diritto alla privacy.

## Note sull'ordinanza n. 26121/2008 del Tribunale di Roma – Sezione proprietà industriale ed intellettuale

Monica Suerz

ABSTRACT

*Da anni, ormai, tanto negli ordinamenti di* civil law *quanto in quelli di* common law, *si dibatte in dottrina, in giurisprudenza ed anche nella società civile, sull'annosa questione della fruizione sulla rete Internet dei contenuti digitali protetti dal diritto d'autore*[1]. *Le possibilità offerte dalle reti telematiche hanno determinato, negli ultimi anni, un crescente interesse alla loro utilizzazione per il trasferimento di materiali protetti dal diritto d'autore, da diritti cioè connessi al (o propri del) costitutore. Internet, infatti, ha reso possibile diminuire sia i tempi di* distribuzione[2], *sia i costi relativi all'intermediazione della rete commerciale. Sotto il profilo strettamente giuridico, peraltro, la rete telematica ha indotto non poche perplessità, mettendo in crisi un sistema di protezione del diritto d'autore e di proprietà intellettuale tradizionalmente basato sul controllo degli esemplari materiali delle opere (quali l'apposizione della firma dell'autore o dei contrassegni di cui agli artt. 123 e 181 bis, l. n. 633 del 1941). Questa contrapposizione evidente tra il "vecchio" ed il "nuovo" investe trasversalmente la materia della proprietà intellettuale, quella della* privacy *e della trasparenza nonché, più in generale, il tema dei meccanismi e delle dinamiche di imputazione delle condotte nello spazio globale. La responsabilità degli intermediari della comunicazione, l'*enforcement *dei diritti di proprietà intellettuale, il difficile e conflittuale rapporto tra* privacy *e* copyright *nella società dell'informazione sono solo alcuni dei profili sui quali si è dibattuto nel 2008 il Tribunale di Roma.*

PAROLE CHIAVE
ORDINANZA 26121/2008;
DIRITTO D'AUTORE; PROVIDER;
FILE-SHARING; DIRITTO ALLA RISERVATEZZA

*«More than ever, intellectual property is going through a crisis of legitimacy»*
C. Geiger[3]

SOMMARIO



1 Diverso però è l'approccio alla concezione di base dell'esclusiva sulle opere artistiche, essendo stato diverso il percorso storico che ha caratterizzato il *copyright* in Gran Bretagna ed il diritto d'autore in Europa. Negli ordinamenti di *civil law*, sulla scorta del diritto di proprietà sui beni materiali, il diritto d'autore viene concepito come un diritto della persona che protegge il legame tra l'uomo e la sua creazione, fondato sullo *ius excludendi alios*. Negli ordinamenti di *common law*, invece, il *copyright* è uno strumento di mercato che crea isole di monopolio nel mare della concorrenza. I diritti esclusivi vengono interpretati in maniera restrittiva, per non sacrificare eccessivamente la libera utilizzabilità dell'opera.

2 In senso lato, nella sua accezione economica e di mercato, quale risultato della trasmissione e del successivo *downloading* del materiale protetto a prescindere dalla qualificazione dei sottostanti diritti esercitati ai sensi della normativa sulle opere dell'ingegno.

3 C. Geiger, Copyright and Free Access to Information. For a Fair Balance of Interests in a Globalised World, in "European Intellectual Property Review", 2006, vo. 28, n. 7, p. 366.

## 1. La fattispecie

La controversia vede contrapposte, da una parte, le società Peppermint Jam Records GmbH (di seguito Peppermint), casa discografica con sede in Germania, e Techland Sp. Zoo (di seguito Techland), società che elabora e commercializza giochi elettronici con sede in Ostrow Wlkp (Polonia) e, dall'altra, il soggetto *provider* Tiscali Italia S.p.a (di seguito Tiscali) per l'accesso a Internet. Le due società intendono ottenere da Tiscali, fornitore del servizio necessario per la connessione ai sistemi informatici, la comunicazione delle generalità dei soggetti ritenuti responsabili di aver scambiato *file* protetti dal diritto d'autore tramite reti *peer-to-peer*, ossia tramite un sistema di collegamento reciproco incrociato, al fine di promuovere contro di essi un'azione giudiziaria. Va rilevato che il ricorso da parte di Peppermint e Techland si basa sull'attività svolta per conto e su autorizzazione delle predette società da Logistep AG (di seguito Logistep), società svizzera specializzata nell'antipirateria che, attraverso un'attività di monitoraggio delle reti *peer-to-peer* effettuata tramite un *software* proprietario, aveva individuato numerosi indirizzi IP i cui titolari erano stati considerati responsabili della predetta condotta illecita. Il *software*, messo a punto da Logistep, è stato capace infatti di individuare i *file* protetti tramite l'analisi dei relativi codici *hash*[1] e di memorizzare gli indirizzi IP degli utenti che possedevano tali *file*. Hanno successivamente legato l'indirizzo IP della singola connessione ai codici GUID[2], ossia agli identificativi che i sistemi di *file sharing* collegano al singolo utente così da poter individuare univocamente lo stesso utente anche ove avesse utilizzato, per una successiva connessione, un diverso indirizzo IP[3]. In sostanza, il *software* permette di tenere traccia della disponibilità in rete di un certo *contenuto*; di verificarne l'effettiva possibilità

1 *Hash* (da "*to hash*" ossia sminuzzare, pasticciare). Nel linguaggio scientifico l'*hash* è una funzione univoca operante in un solo senso e, dunque, non idonea ad essere invertita e atta alla trasformazione di un testo di lunghezza arbitraria in una stringa di lunghezza fissa e limitata che rappresenta un'impronta digitale del testo originario. In informatica, invece, la funzione di trasformazione che genera l'*hash* opera sui bit di un file restituendo una stringa di bit di lunghezza predefinita. Più precisamente è una funzione matematica applicata al documento informatico. La caratteristica della procedura consiste nel fatto che mentre il documento informatico cui si applica la funzione è costituito da una sequenza di simboli binari (bit) di lunghezza variabile per ciascun documento e che può assumere notevoli dimensioni, la funzione di *hash* genera invece una sequenza di simboli binari (bit) di lunghezza sempre fissa, breve e predefinita. La "brevità" dell'impronta (normalmente 160 bit) fa comprendere perché la crittografia della firma digitale si applichi all'impronta e non al documento il quale,potendo assumere dimensioni ben maggiori, richiederebbe tempi eccessivamente lunghi per completare il processo di firma.

2 Il GUID (*Global Unique Identifier*: identificatore unico globale) è, tecnicamente un numero pseudo casuale usato nella programmazione dei *software* al fine di distinguere vari oggetti. In tal modo è possibile identificare:
- Gli utenti grazie all'*username/nickname* a cui corrisponde un codice GUID;
- I *file* mediante il valore *hash*;
- Il pc da cui è partita l'azione di *file-sharing* tramite l'indirizzo IP.

3 L'indirizzo IP è un indirizzo in formato numerico corrispondente ad un numero telefonico necessario per far comunicare tra loro i dispositivi in rete (*webserver, e-mail server, computer*). Ogni volta che si accede ad una pagina l'indirizzo IP del computer che la consulta viene comunicato al computer sul quale tale pagina è stata salvata. Il *provider*, fornitore di accesso ad Internet assegna, altresì, gli indirizzi IP di Rete, ossia i parametri numerici che individuano univocamente le singole macchine reciprocamente collegate online, permettendo, in tal guisa l'identificazione dei diversi utenti contemporaneamente presenti sulla Rete. Un indirizzo Internet è dunque, costituito da un numero di cinque cifre, assegnato dall'*authority* a ciò preposta (ICANN ed altri organismi ad esso affiliati), funzionale proprio allo scopo di identificare online l'elaboratore utilizzato da ogni singolo *cybernauta*. L'assegnazione dell'indirizzo IP agli utenti finali è, di norma, posta in essere nella forma cd. dinamica. L'utente finale, cioè, verrà fornito del numero identificativo IP per il solo periodo di effettiva interconnessione alla Rete. Ad ogni successivo accesso alla Rete, al medesimo cliente sarà, verosimilmente, attribuito dal *provider* un indirizzo IP differente rispetto a quello utilizzato nel precedente periodo di collegamento. I fornitori di connettività (i *service provider* come Tiscali) sono, dunque, gli unici soggetti che posseggono informazioni capaci di collegare un'utenza ad un indirizzo IP e dunque a conoscere a quale utente faccia riferimento un certo indirizzo IP in un dato istante.

di acquisizione, effettuandone lo scaricamento (*download*), ovvero la copia in rete dalle aree di condivisione degli utenti che ospitano quel contenuto verso i propri computer; di verificarne la segnatura digitale con algoritmo SHA1 o MD5 (in dipendenza dal protocollo *peer-to-peer* utilizzato); di controllarne la diffusione, verificando l'esistenza di altre condivisioni presuntivamente riferibili a una pregressa attività di *download* (sul presupposto che la quasi totalità degli utenti che condividono uno specifico contenuto lo abbiano a loro volta acquisito da un'altra fonte nella rete, tranne eventualmente il soggetto che originariamente lo abbia messo per la prima volta in condivisione, con una specifica segnatura digitale). Sulla base di questi elementi di fatto (gli indirizzi IP, quindi di protocollo, forniti dalla Logistep), le società ricorrenti chiedevano all'Autorità giudiziaria che venisse ordinato a Tiscali di fornire ad esse le generalità dei soggetti titolari di tali indirizzi.

Ecco dunque stabilito il *proprium* del presente ricorso, ossia se il titolare del diritto di sfruttamento di opere dell'ingegno possa pretendere da un terzo (l'*Internet Service Provider*) l'ostensione di dati personali relativi ai violatori, tramite il *file sharing*, del diritto di privativa.

Le richieste rivolte all'Autorità giudiziaria dalle società ricorrenti si basano tendenzialmente su una interpretazione estensiva del combinato disposto degli artt. 156, 156*bis* e 156*ter* della legge 22 aprile 1941, n. 633 (concernente la protezione del diritto d'autore), che consente al titolare di un diritto di utilizzazione economica di opere dell'ingegno di ottenere dal giudice l'ordine, nei confronti di chi si possa ragionevolmente presumere che abbia violato la legge citata, di fornire gli elementi necessari per l'identificazione dei soggetti implicati nella produzione e distribuzione dei prodotti o dei servizi in violazione degli stessi diritti di utilizzazione economica. L'esibizione di tali elementi atti ad identificare i soggetti dell'illecito, consentita dall'art. 156*bis*, L. 633/41, non è peraltro inibita da alcuna norma del d.lgs. 196/2003: stabilisce infatti l'art. 24, comma1, lettera f) che il trattamento dei dati personali è consentito anche senza il consenso dell'interessato, quando sia necessario «per far valere o difendere un diritto in sede giudiziaria».

Tiscali invece eccepisce:

- Sul piano pregiudiziale di rito, l'ineseguibilità della domanda chiesta dalle parti ricorrenti, poiché l'ordine di esibizione dei dati relativi al traffico telefonico può essere impartito solo dall'autorità giudiziaria penale, non da quella civile (ai sensi degli artt. 23 e 132, d.lgs. 30.6.2003), e che pertanto, qualora attuasse l'azione da esse sollecitata, incorrerebbe nel reato di violazione del diritto alla *privacy* (degli utenti). Ineseguibilità che, se confermata e dichiarata dal Tribunale di Roma, non farebbe proseguire d'ufficio il ricorso di Peppermint e Techland.

- Sul piano preliminare di merito:

i. l'inammissibilità del ricorso sia perché alla base vi è l'esistenza del diritto alla *privacy* meritevole di tutela, sia perché il modo in cui i dati sono stati recuperati dalla società incaricata dalle ricorrenti non appare lecito, in quanto formati in violazione delle leggi sulla stessa *privacy*;

ii. il difetto della titolarità propria dell'ISP (Tiscali) rispetto alla domanda richiesta dai soggetti attivi nel fornire i dati personali, in quanto tale parte - fornendo meramente un servizio – è da ritenersi del tutto estranea ad eventuali *download* e condotte illegali da parte degli utenti (cd. *netizens*);

iii la mancanza del requisito del *periculum in mora* (pericolo/danno grave e al contempo irreparabile causato dal ritardo)[4]. Questo si

4 Con la locuzione "danno grave" ci si riferisce all'entità del pregiudizio, calcolata in rapporto al valore del bene oggetto della controversia (opere coperte dal diritto d'autore). L'irreparabilità del danno invece riguarda la possibilità di rimediare in futuro ai danni che Peppermint e Techland subiranno. Il *periculum in mora* è uno dei requisiti fondamentali per la domanda e l'ottenimento di *discovery* in via cautelare nonché dell'ottenimento di tale provvedimento L'azione cautelare, per essere autorizzata, è condizionata sia dalla sussistenza di un pericolo al quale il ritardo può esporre il diritto (*periculum in mora*) e sia da una approssimativa

traduce per le società ricorrenti nella possibilità che il *file sharing* si ripercuoti sulle stesse causando uno sviamento di clientela, in quanto condotta reiterabile ad *ibitum*.

Qualora il processo non si chiuda in punto di rito, Tiscali indurrebbe al fatto che:

i i *videogames* non sono "in rapporto" con il diritto d'autore e quindi non rientrano nella sua sfera di protezione. Ciò è dovuto alla poca chiarezza sia della *ratio* della norma a tutela del diritto d'autore[5], che dell'estensione della stessa, nonché alle interpretazioni di *videogames* fornite nella giurisprudenza[6].

ii La prova - *l'actio ad exhibendum* (elemento fondamentale del processo civile) -delle parti ricorrenti non risulta ammissibile, poiché effettuata in modo massivo e capillare per un periodo di tempo prolungato nei confronti di utenti ignari, violando palesemente le regole sulla *privacy*;

iii Sussiste un concorso di colpa da parte delle società ricorrenti, in quanto non hanno agito anche contro i produttori e fornitori stessi dei servizi di *file sharing*.

Merita sottolineare tuttavia come Tiscali non neghi il possesso (materiale e di fatto) della *res* (la generalità degli utenti), ma contesti squisitamente il fatto di utilizzare in senso giuridico, tramite l'esibizione, la *res* stessa, in quanto lesiva della *privacy*.

Nel corso del procedimento civile, respingendo la domanda delle ricorrenti, sono pure intervenuti autonomamente e si sono costituiti:

- L'autorità amministrativa indipendente del Garante per la protezione dei dati personali[7];

verosomiglianza circa l'esistenza del diritto stesso (*fumus boni iuris*). I procedimenti cautelari nascono per ovviare alla circostanza che, durante il tempo occorrente per ottenere la tutela giurisdizionale, le condizioni patrimoniali o di fatto della parte debitrice mutino e, a seguito di tale mutamento, venga compromessa la fruttuosità della tutela giudiziaria invocata. La sua funzione è dunque sia quella di anticipazione degli effetti della sentenza che quella cautelare conservativa (come nella fattispecie, proposto nel corso di un giudizio di denuncia di nuova opera o danno temuto).

5 In Italia, così come in altri paesi di *civil law*, ciò che può essere oggetto del diritto d'autore è definito dalla legge con un catalogo aperto. Essendo infinite le forme d'arte, è illimitata la materia proteggibile. Si vede infatti l'art. 2 l.d.a., secondo cui «sono comprese nella protezione:
1 -Le opere letterarie, drammatiche, scientifiche, didattiche, religiose tanto se in forma scritta quanto se orale;
2 Le opere e le composizioni musicali, con o senza parole, le opere drammatico-musicali e le variazioni musicali costituenti di per sé opera originali;
3 Le opere coreografiche o pantomimiche;
4 Le opere della scultura, della pittura, dell'arte del disegno, della incisione e delle arti figurative similari, compresa la scenografia;
5 I disegni e le opere dell'architettura;
6 Le opere dell'arte cinematografica;
7 Le opere fotografiche;
8 I programmi per elaboratore [ndr. Software];
9 Le banche dati;
10 Le opere del disegno industriale che presentino di per sé carattere creativo e valore artistico.»

6 Dapprima assimilati – dalla Pretura di Torino – al *software*. La prospettiva muta quando lo stesso Tribunale di Torino (15 luglio 1983) pose l'accento sull'elemento delle immagini in movimento che contraddistingue qualsiasi videogioco, attirandolo in questo modo nel campo delle opere audiovisive e lasciando l'alveo della nozione *software*. I videogiochi costituiscono un tipo particolare di opera cinematografica, possibile oggetto della tutela prevista per tali opere dalle norme sul diritto d'autore. L'opera cinematografica, disciplinata dalla norma sul diritto d'autore, è un *genus* al quale appartengono non sono i film, ma anche altre forme di rappresentazione, qualunque ne sia la tecnica di realizzazione e la forma di espressione. Oggetto della tutela prevista dalla l.d.a. non è solo l'opera d'arte, bensì l'opera dell'intelletto o della mente (opera dell'ingegno), che abbia il requisito oggettivo dell'originalità e non banalità (carattere creativo). Si ricordi che il nostro legislatore peraltro ha previsto per il *software* una disciplina specifica contenuta negli artt. 64*bis* e ss. della legge sul diritto d'autore, che differisce notevolmente rispetto a quella dettata per le opere audiovisive. Tant'è vero che uno dei risultati della qualifica di gioco come opera multimediale complessa è proprio quello di ammettere il prestito e la libera riproduzione da parte delle biblioteche e delle discoteche appartenenti allo Stato o ad altri enti pubblici, secondo quanto previsto dall'art. 69 della legge sul diritto d'autore. Per ogni riferimento al Codice si veda: www.studiocataldi.it/codicionline.asp.

7 Ciò al fine di verificare che nella vicenda vengano rispettati tutti i diritti di protezione dei dati stessi degli utenti, evidenziando come non sia possibile limitare il diritto alla segretezza delle comunicazioni in virtù dell'esercizio di una ragione civile. Si osservi

- Il Coordinamento delle Associazioni per la difesa dell'Ambiente e dei diritti degli utenti e dei Consumatori (cd. Codacons[8];

- L'Associazione Italiana Difesa Consumatori ed Ambiente (cd. Adiconsum)[9].

L'intervento di tali soggetti, in merito alla questione fondamentale della fattispecie ivi analizzata sull'utilizzo della *discovery* per la comunicazione di informazioni personali circa gli utenti, è da ricercarsi nel netto conflitto con l'interesse delle società resistenti. Perché, nel caso di specie, l'esecuzione dell'ordine di *discovery* si risolverebbe in una comunicazione dei dati personali degli utenti (dei loro nominativi e dei loro indirizzi fisici) senza alcun consenso dei medesimi, che operano sulla rete in presunzione di anonimato andando così a ledere il diritto alla riservatezza degli stessi. Le informazioni richieste dall'istante infatti non sono informazioni da poco. Si tratta di una questione che ha tenuto e tiene inchiodato l'intero mondo Internet circa la questione della cd. "neutralità della Rete".

## 2. Sulle questioni: principi ed istituti giuridici

Le ricorrenti qualificano la domanda di *discovery*[10] da loro proposta come istanza di *di-*

tuttavia come Agcom sia ora titolata a sostituirsi all'autorità giudiziaria. Infatti, in vigore dal 31 marzo 2014, il Regolamento in materia di tutela del diritto d'autore promuove lo sviluppo dell'offerta legale di opere digitali e la loro corretta fruizione e definisce le procedure per l'accertamento da parte dell'Autorità delle violazioni commesse sulle reti di comunicazione elettronica. I titolari dei diritti, le associazioni di settore e le società di gestione collettiva possono inviare un'istanza all'Autorità, compilando un apposito modulo, per chiedere la rimozione delle opere digitali diffuse in violazione dei diritti d'autore o dei diritti connessi, sia *online* che sui mezzi radiotelevisivi. A questo punto le possibilità per il Garante, nel caso in cui la richiesta venga accolta, sono due: procedere in maniera ordinaria, con 35 giorni di tempo, o con un rito abbreviato, 12 giorni. Questa seconda opzione scatta automaticamente nel caso in cui la segnalazione arrivi da una delle associazioni che detengono i diritti come Anica (Associazione nazionale industrie cinematografiche audiovisive e multimediali) o Siae (Società italiana degli autori e degli editori) o se si è al cospetto di una violazione a scopo di lucro. L'intero regolamento non quindi è relativo solo alla pirateria in senso stretto, ma alla tutela generale delle opere digitali, termine che indica "un'opera, o parti di essa, di carattere sonoro, audiovisivo, fotografico, videoludico, editoriale e letterario, inclusi i programmi applicativi e i sistemi operativi per elaboratore, tutelata dalla Legge sul diritto d'autore e diffusa su reti di comunicazione elettronica". La morsa si stringe, non a caso, nel momento in cui l'offerta legale sta aumentando: si pensi allo streaming musicale di Spotify o Deezer o ai servizi di contenuti video su abbonamento *online* lanciati da Mediaset e Sky, Infinity e River, che non sono più interessate solo a proteggere i propri contenuti ma anche a incoraggiare l'utilizzo delle loro piattaforme a pagamento. Da lunedì 31 marzo, quindi, per i titolari del diritto d'autore di qualsiasi opera digitale, da un articolo a una canzone passando per un video o una foto, e per le associazioni che li rappresentano sarà molto più semplice far sentire la propria voce. Sono del parere tuttavia che serva un d.d.l. che depenalizzi il *file sharing* senza scopo di lucro, affinché vengano puniti solo i delinquenti veri, quelli che si arricchiscono alle spalle di chi la cultura la produce. Per ulteriori approfondimenti si veda www.agcom.it/.

8 Ciò al fine di tutelare con ogni mezzo legittimo i diritti e gli interessi degli utenti-consumatori.

9 Ciò per concertare che le condizioni di difesa - individuale e/o collettiva - degli utenti-consumatori vengano rispettate. Per tale soggetto, inoltre, la norma contenuta nell'art. 156*bis* della legge 633/1941 (in materia di diritto d'autore) risulterebbe essere in contrasto con il principio sancito nella Costituzione all'art. 15 Cost. (in materia di diritti sulla comunicazione interpersonale), in quanto non possono essere richieste e comunicate informazioni personali per la repressione o l'accertamento di illeciti civili. L'Adiconsum è infatti un'associazione di tutela dei consumatori istituita su iniziativa della CISL ed iscritta nell'elenco delle associazioni dei consumatori e utenti rappresentative a livello nazionale, di cui all'art. 5 della legge 281/98 (ora art. 137 del Codice del Consumo). È presente sul territorio nazionale dal 1987 con oltre 149.375 associati. Per ulteriori approfondimenti si veda www.adiconsum.it. Pertanto, qualora il giudice ammettesse la domanda di Peppermint e Techland, convaliderebbe un atto illecito. L'Adiconsum va a contestare altresì l'interpretazione delle disposizioni del diritto comunitario avanzate dalla parte ricorrente, poiché risultano difformi dall'applicazione locale nonché nazionale del diritto comunitario stesso.

10 La possibilità di disporre di celeri ed efficaci misure provvisorie per salvaguardare le condizioni relative alle violazioni dei diritti di proprietà intellettuale è, del resto, espressamente garantita dall'art. 8, 9 e 11 della direttiva *Enforcemen*t 2004/48/CE di cui il d.lgs. 16 marzo 2006, n. 140 costituisce attuazione. In armonia con quanto chiarito, la direttiva 2004/48/CE precisa:
- art. 8 rubricato nella Sezione 3 "*Diritto d'informazione*":
1. Gli Stati membri assicurano che, nel contesto dei procedimenti riguardanti la violazione di un diritto di proprietà intellettuale e in risposta a una

richiesta giustificata e proporzionata del richiedente, l'autorità giudiziaria competente possa ordinare che le informazioni sull'origine e sulle reti di distribuzione di merci o di prestazione di servizi che violano un diritto di proprietà intellettuale siano fornite dall'autore della violazione e/o da ogni altra persona che:
a) sia stata trovata in possesso di merci oggetto di violazione di un diritto, su scala commerciale;
b)sia stata sorpresa a utilizzare servizi oggetto di violazione di un diritto, su scala commerciale;
c) sia stata sorpresa a fornire su scala commerciale servizi utilizzati in attività di violazione di un diritto; oppure
d) sia stata indicata dai soggetti di cui alle lettere a), b) o c) come persona implicata nella produzione, fabbricazione o distribuzione di tali prodotti o nella fornitura di tali servizi.
2. Le informazioni di cui al paragrafo 1 comprendono, ove opportuno, quanto segue:
a) nome e indirizzo dei produttori, dei fabbricanti, dei distributori, dei fornitori e degli altri precedenti detentori dei prodotti o dei servizi, nonché dei grossisti e dei dettaglianti;
b) informazioni sulle quantità prodotte, fabbricate, consegnate, ricevute o ordinate, nonché sul prezzo spuntato per i prodotti o i servizi in questione
3. I paragrafi 1 e 2 si applicano fatte salve le altre disposizioni regolamentari che:
a) accordano al titolare diritti d'informazione più ampi;
b) disciplinano l'uso in sede civile o penale delle informazioni comunicate in virtù del presente articolo;
c) disciplinano la responsabilità per abuso del diritto d'informazione;
d) accordano la possibilità di rifiutarsi di fornire informazioni che costringerebbero i soggetti di cui al paragrafo 1 ad ammettere la sua partecipazione personale o quella di parenti stretti ad una violazione di un diritto di proprietà intellettuale, oppure
e) disciplinano la protezione o la riservatezza delle fonti informative o il trattamento di dati personali
art. 9 rubricato nella sezione 4 "*Misure provvisorie e cautelari*":
1. Gli Stati membri assicurano che le competenti autorità giudiziarie possano, su richiesta dell'attore,
a) emettere nei confronti del presunto autore della violazione un'ingiunzione interlocutoria volta a prevenire qualsiasi violazione imminente di un diritto di proprietà intellettuale, o a vietare, a titolo
provvisorio e, imponendo se del caso il pagamento di una pena pecuniaria suscettibile di essere reiterata, ove sia previsto dalla legislazione nazionale, il proseguimento di asserite violazioni di tale diritto, o a subordinare l'azione alla costituzione di garanzie finalizzate ad assicurare il risarcimento del titolare; un'ingiunzione interlocutoria può inoltre essere emessa, alle stesse condizioni, contro un intermediario, i cui servizi sono utilizzati da terzi per violare un diritto di proprietà intellettuale; ingiunzioni contro intermediari i cui servizi sono utilizzati da terzi per violare un diritto d'autore o un diritto connesso sono contemplate dalla direttiva 2001/29/CE *Information Society Directive;*
b) disporre il sequestro o la consegna dei prodotti sospettati di pregiudicare un diritto di proprietà intellettuale per impedirne l'ingresso o la circolazione nei circuiti commerciali.
2. Nei casi di violazioni commesse su scala commerciale gli Stati membri assicurano che, quando la parte lesa faccia valere l'esistenza di circostanze atte a pregiudicare il pagamento del risarcimento, l'autorità giudiziaria competente possa disporre il sequestro conservativo di beni mobili e immobili del presunto autore della violazione, compreso il blocco dei suoi conti bancari e di altri averi. A tal fine la competente autorità può disporre la comunicazione delle documentazioni bancarie, finanziarie o commerciali, o l'appropriato accesso alle pertinenti informazioni.
3. L'autorità giudiziaria ha facoltà, con riguardo alle misure di cui ai paragrafi 1 e 2, di richiedere all'attore di fornire qualsiasi elemento di prova ragionevolmente accessibile al fine di accertare con un sufficiente grado di certezza che il medesimo è il titolare del diritto e che una violazione di tale diritto è in atto o imminente.
4. Gli Stati membri assicurano che le misure di cui ai paragrafi 1 e 2 possano, ove opportuno, essere adottate inaudita altera parte, in particolare quando un ritardo potrebbe arrecare un danno irreparabile al titolare del diritto. In tal caso le parti ne vengono informate, senza indugio, al più tardi dopo l'esecuzione delle misure.
Su richiesta del convenuto si procede a un riesame, nel corso del quale il medesimo ha diritto ad essere inteso, allo scopo di decidere, entro un termine ragionevole dopo la notificazione delle misure, se queste vadano modificate, revocate o confermate.
5. Gli Stati membri assicurano che le misure provvisorie di cui ai paragrafi 1 e 2 siano revocate o cessino comunque di essere efficaci, su richiesta del convenuto, se l'attore non promuove un'azione di merito dinanzi all'autorità giudiziaria competente entro un periodo ragionevole che sarà determinato dall'autorità giudiziaria che ordina tali misure quando la legislazione dello Stato membro lo consente oppure, in assenza di tale determinazione, entro un periodo che non deve superare 20 giorni lavorativi o 31 giorni di calendario, qualora questi rappresentino un periodo più lungo.
6. Le competenti autorità giudiziarie possono subordinare le misure di cui ai paragrafi 1 e 2 alla costituzione da parte del richiedente di una cauzione adeguata o di una garanzia equivalente destinata ad assicurare l'eventuale risarcimento del danno subito dal convenuto, quale previsto al paragrafo 7.
7. Qualora le misure provvisorie siano revocate o decadano in seguito ad un'azione o omissione dell'attore, o qualora successivamente si constati che non vi è stata violazione o minaccia di violazione di un diritto di proprietà intellettuale, l'autorità giudiziaria ha la facoltà di ordinare all'attore, su richiesta del

*scovery*[11] in via cautelare, dove il *petitum* (*ergo*, l'oggetto della domanda) è da rinvenirsi nella richiesta delle generalità degli utenti-consumatori e dove la *causa petendi* (*ergo*, il motivo per cui Techland e Peppermint ricorrono) è da ritrovarsi nella lesione dei diritti di proprietà intellettuale di cui le ricorrenti sono titolari[12].

Altre norme all'uopo impugnate, dinnanzi al Tribunale di Roma, dalle società Peppermint e Techland, sono gli art.156 *ter* l.d.a. 633/1941, ovvero *ex* art. 700 c.p.c.[13], e l'art. 8.3 della direttiva CE 2001/29[14]. La parte ricorrente, rifacendosi a tale ordito normativo, ha dunque voluto sostenere l'idea che il legislatore comunitario, con tale direttiva, abbia rafforzato la possibilità di difesa giudiziaria in sede civile di chi ha subito una lesione dei diritti di utilizzazione economica prevedendo, per l'appunto, la possibilità

convenuto, di corrispondere a quest'ultimo un adeguato risarcimento del danno eventualmente arrecato dalle misure in questione.

Art. 11 *Ingiunzioni* rubricato nella sezione 5 "*Misure adottate a seguito di decisione sul merito*": Gli Stati membri assicurano che, in presenza di una decisione giudiziaria che ha accertato una violazione di un diritto di proprietà intellettuale, le autorità giudiziarie possano emettere nei confronti dell'autore della violazione un'ingiunzione diretta a vietare il proseguimento della violazione. Se previsto dalla legislazione nazionale, il mancato rispetto di un'ingiunzione è oggetto , ove opportuno, del pagamento di una pena pecuniaria suscettibile di essere reiterata, al fine di assicurarne l'esecuzione. Gli Stati membri assicurano che i titolari possano chiedere un provvedimento ingiuntivo nei confronti di intermediari i cui servizi sono utilizzati da terzi per violare un diritto di proprietà intellettuale, senza pregiudizio dell'articolo 8, paragrafo 3 della direttiva 2001/29/CE.

11 La giurisprudenza, peraltro, di solito parla di *discovery* solo con riguardo alle misure previste dall'art. 156 *bis* l.d.a. e del corrispondente art. 121 c.p.i., mentre utilizza l'espressione "diritto di informazione" per le misure previste dall'art. 156 *ter* l.d.a. e dal corrispondente art. 121 *bis* c.p.i. A parte gli aspetti terminologici, dalle formulazione delle due norme emergono differenze significative circa il tipo di dati, documenti o informazioni acquisibili e i soggetti destinatari dell'ordine. Inoltre la relazione al d.lgs. 16 marzo 2006, n. 140 (con il quale gli artt. 156 *bis* e 156 *ter* sono stati introdotti nella l.d.a.) sottolinea come, a differenza delle informazioni che possono essere chieste e ottenute mediante una *discovery*, le informazioni di cui agli artt. 156 *ter* l.d.a. e 121 *bis* c.p.i. «sono oggetto di un diritto autonomamente esercitabile» (nello stesso senso è possibile rinvenire nella dottrina come dalla *discovery* si origina un diritto puramente processuale,mentre il diritto di informazione è configurato come un diritto sostanziale autonomamente sanzionabile). Si veda: UBERTAZZI L.C., *AIDA,Annuali Italiani del Diritto d'Autore, della Cultura e dello Spettacolo*,Giuffrè Ed., XVIII – 2009, pp. 1287 e ss.

12 Tale domanda in via cautelare è volta ad evitare (in via provvisoria) che durante il tempo necessario affinché il processo ordinario si svolga vengano irrimediabilmente pregiudicate le condizioni e/o i beni occorrenti per il fruttuoso esercizio dell'azione esecutiva richiesta. Siamo quindi nella circostanza dove l'eventuale accoglimento della relativa domanda avrebbe carattere integralmente satisfattivo della pretesa azionabile nel giudizio di merito.

13 Secondo cui «1. L'autorità giudiziaria sia nei giudizi cautelari che di merito può ordinare, su istanza giustificata e proporzionata del richiedente, che vengano fornite informazioni sull'origine e sulle reti di distribuzione di merci o di prestazione di servizi che violano un diritto di cui alla presente legge da parte dell'autore della violazione e da ogni altra persona che: a) sia stata trovata in possesso di merci oggetto di violazione di un diritto, su scala commerciale; sia stata sorpresa a utilizzare servizi oggetto di violazione di un diritto, su scala commerciale; b) sia stata sorpresa a fornire su scala commerciale servizi utilizzati in attività di violazione di un diritto; c) sia stata indicata dai soggetti di cui alle lettere a) o b) come persona implicata nella produzione, fabbricazione o distribuzione di tali prodotti o nella fornitura di tali servizi.
Le informazioni di cui al comma 1 possono tra l'altro comprendere il nome e indirizzo dei produttori, dei fabbricanti, dei distributori, dei fornitori e degli altri precedenti detentori dei prodotti o dei servizi, nonché dei grossisti e dei dettaglianti, nonché informazioni sulle quantità prodotte, fabbricate, consegnate, ricevute o ordinate, nonché sul prezzo dei prodotti o servizi in questione.
Le informazioni vengono acquisite tramite interrogatorio dei soggetti di cui al comma 1.
Il richiedente deve fornire l'indicazione specifica delle persone da interrogare e dei fatti sui quali ognuna di esse deve essere interrogata.
Il giudice, ammesso l'interrogatorio, richiede ai soggetti di cui al comma 1 le informazioni indicate dalla parte; può altresì rivolgere loro, d'ufficio o su istanza di parte, tutte le domande che ritiene utili per chiarire le circostanze sulle quali si svolge l'interrogatorio.
6. Si applicano gli articoli 249, 250, 252, 255 e 257, primo comma, del codice di procedura civile (141/d).»

14 Secondo cui «gli Stati membri devono inoltre assicurarsi che i titolari dei diritti possano chiedere un provvedimento inibitorio [dell'atto illecito] nei confronti degli intermediari i cui servizi siano utilizzati [in concorso] da terzi per violare un diritto d'autore o diritti connessi».

di agire in giudizio anche contro "intermediari" (Tiscali e, più in generale, gli ISP), che consentono violazioni in rete da parte degli utenti contro opere e materiali protetti. Ciò non solo al fine di impedire la continuazione e/o la ripetizione di una violazione avvenuta (art. 156 l.d.a. 1941/633), ma anche per ottenere dall'Autorità giudiziaria l'ordine di chiedere elementi per l'identificazione degli stessi soggetti implicati nella produzione e distribuzione dei prodotti/servizi di cui le ricorrenti detengono i diritti proprietari (art. 156*bis* l.d.a. 1941/633).

Le parti ricorrenti assumono inoltre di poter proporre tale domanda di *discovery* in virtù delle probabili inesattezze commesse dal legislatore nazionale in sede di attuazione e recepimento delle suddette direttive comunitarie. In particolare Techland e Peppermint, nella loro accusa, eccepiscono che, con riferimento alla direttiva 2001/29/CE, la presenza della locuzione "inibitorio" (contenuta nell'art. 8.3), anziché "ingiuntivo", sarebbe frutto di un mero errore di traduzione[15]. Tant'è vero che nella direttiva 2004/48/CE (recepita con gli artt. 156*bis* e 156*ter* della legge 1941/633), il legislatore italiano parla di ingiunzione interlocutoria come misura (provvisoria e cautelare) da emettere al fine di tutelare il diritto d'autore sebbene ometta di citare tra i destinatari di siffatto ordine di ingiunzione, i soggetti terzi possessori di queste informazioni (gli ISP).

Tuttavia, controbatte Tiscali, è pregiudiziale e contrario alla norma contenuta nell'art. 12 delle *preleggi* (le Disposizioni preliminari al Codice civile) il basare la personale interpretazione del testo normativo sul presupposto di "errore" da parte del legislatore storico. L'interpretazione e la "riproduzione" delle norme comunitarie da parte del legislatore nazionale infatti non è libera, poiché deve seguire i criteri ermeneutici contenuti nell'art. 12 di cui *supra*. Tale "vincolo" nella libertà dell'incedere del percorso interpretativo, impone quindi al giudice nazionale di usare, innanzitutto, un primo strumento "conservativo": quello dell' "interpretazione conforme" alla Costituzione italiana. Ciò non vuol certo negare quel tocco di autonomia creativa che connota da sempre ogni *decisum* del giudice: la libertà di movimento c'è, ma all'interno di confini tracciati d'un canto dai principi della Costituzione italiana, dall'altro da quelli comunitari. L'obbligo di interpretazione conforme, infatti, se da un lato orienta il giudice nella sua attività ermeneutica, d'altro lato, però, lo rende il vero protagonista del momento attuativo del diritto comunitario di cui diviene ultimo e fondamentale anello della catena.

Tuttavia, se dovesse effettivamente sussistere un "errore" interpretativo da parte del legislatore storico nazionale nel recepimento della norma comunitaria, la teoria generale dell'interpretazione prevede che si possa comunque rimediare con diversi strumenti, quali:

l'interpretazione adeguatrice o conservatrice: affinché la legge non produca antinomie con norme superiori, essa viene adattata e modificata, facendo valere in tal caso la prevalenza del parametro rispetto all'oggetto.

Il rinvio pregiudiziale: esso dà al giudice nazionale la facoltà, e se di ultima istanza l'obbligo, di chiedere alla Corte di Giustizia (ed entro alcuni limiti anche al Tribunale di 1°) una pronuncia in riferimento a quale sia la corretta interpretazione e quindi la portata di una o più norme del diritto comunitario e se la corretta applicazione di una norma comunitaria precluda l'applicazione di una norma nazionale (rinvio pregiudiziale di interpretazione). Ovviamente il rinvio pregiudiziale alla Corte di Giustizia presuppone che la questione interpretativa riguardi norme dell'Unione, che sia rilevante ai fini della decisione e che sussistano effettivi dubbi sull'interpretazione[16].

15 La differenza risiede nel fatto che l'azione inibitoria è finalizzata squisitamente a precludere la continuazione o la ripetizione (e gli effetti) conseguenti di un illecito (sia esso già consumato o sia esso possibile), mentre l'ingiunzione è un mero accertamento con prevalente funzione esecutiva, che mira ad assicurare il titolo esecutivo alla parte che lo ha richiesto tramite forme abbreviate. Il procedimento di ingiunzione *inaudita altera parte*, nell'ambito della tutela sommaria, è quindi volto ad assicurare all'avente diritto una forma di garanzia anticipatoria, più sollecita e tempestiva rispetto a quella ordinaria.

16 Il ricorso è dunque diretto ad ottenere l'interpretazione delle norme europee al fine di assicurare la corretta ed

Peppermind e Techland, proprio in riferimento al rinvio pregiudiziale (di interpretazione), richiamano nella loro memoria - come ulteriore difesa - il caso C. 342/01 (avente ad oggetto proprio la domanda di pronuncia pregiudiziale proposta alla Corte, a norma dell'art. 234 CE dal Juzgado de lo Social n.33 de Madrid nella causa dinnanzi ad esso pendente tra Maria Paz Merino Gòmez e Continental Industrias del Caucho SA, sull'interpretazione di alcune direttive in materia di ferie annuali e congedo di maternità), che si è tenuto dinnanzi alla Corte di Giustizia[17]. In particolare, le ricorrenti fondano la difesa sulle conclusioni tratte dall'Avvocato Generale, il quale aveva asserito che le norme del diritto dell'Unione devono essere interpretate ed applicate in modo uniforme alla luce delle versioni di tutte le lingue dell'Unione Europea. In caso di difformità, la norma deve essere letta alla luce della lettera ed allo scopo teleologico della direttiva. Pertanto, la direttiva 2001/29/CE inerente «l'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione» e, più in generale, inerente il commercio elettronico viene "completata" dal disposto della direttiva *Enforcement*, che riguarda squisitamente e minuziosamente la tutela del diritto d'autore in un certo senso "prevaricando" sulla prima. Il giudice romano ha però sottolineato correttamente che ritenere il dettato della direttiva *Enforcement* prevalente su quello della direttiva 2001/29/CE intaccherebbe *in toto* gli stessi disposti. Infatti, per quanto riguarda le violazioni del diritto d'autore e dei diritti connessi, la normativa 2004/48/CE prevede già un ampio livello di armonizzazione «senza pregiudizio dell'articolo 8, paragrafo 3 della direttiva 2001/29/CE» . In tal modo il Giudice del Tribunale romano ha fatto cadere l'interpretazione (fallace) delle ricorrenti, evidenziando come le suddette conclusioni dell'Avv. Generale vadano in realtà a riaffermare l'utilizzo dei criteri ermeneutici come sistema per l'interpretazione di una norma valida ed efficace. Ragion questa che ha portato conseguentemente l'Organo giudicante a interpretare in maniera corretta la locuzione all'art. 8.3 della direttiva 2001/29/CE, di cui le ricorrenti lamentavano l'errata traduzione. L'espressione utilizzata nella versione italiana ("provvedimento inibitorio") risulta infatti essere sinonimo dei termini "*injunction*" e "*ordinance*" della rispettiva versione linguistica francese, nella quale peraltro non si legge la possibilità riguardo ad un'azione di *discovery*

uniforme applicazione del diritto dell'Unione in tutti i paesi membri e può essere giustamente concepito come strumento di cooperazione giudiziaria tra giudice/processo comunitario e giudice/processo nazionale. Secondo una costante giurisprudenza, le questioni relative all'interpretazione del diritto comunitario sollevate dal giudice nazionale nel contesto di diritto che egli individua sotto la propria responsabilità, e del quale non spetta alla Corte verificare l'esattezza, godono di una presunzione di rilevanza. Il rigetto, da parte della Corte, di una domanda proposta da un giudice nazionale è possibile soltanto qualora appaia in modo manifesto che l'interpretazione del diritto comunitario richiesta non ha alcun rapporto con l'effettività o l'oggetto della causa principale, qualora la questione sia di tipo ipotetico o, ancora, qualora la Corte non disponga degli elementi di fatto e di diritto necessari per rispondere in modo utile alle questioni che le sono sottoposte. Il rinvio pregiudiziale alla Corte di giustizia europea presuppone l'accertamento della congiunzione tra processo comunitario e processo nazionale nel senso che deve essere rilevante e quindi rimane precluso se non esiste alcuna relazione con la causa in discussione o quando appare solo di natura teorica oppure manchino gli elementi di fatto o di diritto necessari per una decisione della Corte. L'ordinanza di rinvio del giudice nazionale deve contenere gli elementi di fatto e di diritto delle questioni sollevate e la fondatezza delle ipotesi su cui tali questioni sono fondate. Il giudice nazionale deve indicare i motivi della scelta delle disposizioni comunitarie di cui si chiede l'interpretazione e il nesso tra quelle disposizioni e la normativa nazionale applicabile alla controversia al fine di permettere alla Corte di dare l'interpretazione che gli consenta di valutare la compatibilità di norme di diritto interno con la normativa comunitaria, nonché consentire ai governi degli Stati membri e alle altre parti interessate di presentare osservazioni. Secondo la giurisprudenza della Corte, spetta esclusivamente al giudice nazionale cui è sottoposta la controversia valutare la necessità della pronuncia in via pregiudiziale e la rilevanza delle questioni sottoposte. Anche la Corte costituzionale, quale giudice di unica istanza, ha la facoltà, ove la questione di interpretazione della normativa comunitaria non sia manifestamente infondata, di sollevare innanzi la Corte di giustizia la questione pregiudiziale sull'interpretazione del diritto "comunitario". Per ulteriori approfondimenti: www.diritto.it.

17 Si veda http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d2dc30db798d2c686374407ba571cc6c63f84900.e34KaxiLc3qMb40Rch0SaxuLc3j0?text=&docid=61727&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=316512.

che consenta l'acquisizione immediata ed in via d'urgenza della prova dell'illecito (tipico, peraltro, degli ordinamenti anglo-americani). Tale norma non regola quindi affatto l'accesso d'urgenza alla prova dell'illecito, motivo per cui non è norma applicabile alla fattispecie in esame in cui la domanda è stata ricostruita come istanza di *discovery*. Per quanto concerne gli altri articoli di legge richiamati dalle ricorrenti, si veda come la possibilità di disporre di celeri ed efficaci misure provvisorie per salvaguardare le prove relative alle presunte violazioni dei diritti squisitamente di proprietà intellettuale, espressamente garantita dall'art. 8 della direttiva *Enforcement* 2004/48/CE (detta anche IPREDI, *Intellectual Property Rights Enforcement Directive*), la si ritrova nel d.lgs. 16 marzo 2006, n. 140 che costituisce attuazione della direttiva[18].

È dunque squisitamente negli articoli di legge contenuti in questo d.lgs. che trova possibilità giuridica l'istanza di *discovery* delle ricorrenti diretta al *provider* del servizio informatico, in quanto conformi alla stessa direttiva che mira ad armonizzare non solo l'applicazione dei diritti di proprietà intellettuale, ma anche le stesse legislazioni affinché venga garantita parimenti un livello di protezione uniforme in tutto il mercato interno.

Tutte queste disposizioni convergono peraltro nell'art. 47 dell'accordo ADPIC (allegato C dell'accordo istitutivo dell'Organizzazione Mondiale del Commercio), recepito in sede comunitaria con la decisione 94/800/CE (Accordo TRIPs) che introduce il concetto di proporzionalità tra l'ordine (ed esibizione) di *discovery* (all'autore della violazione) e la gravità della violazione. Il disposto prevede quindi che qualora la parte lesa abbia fornito seri indizi di prova (*semiplena probatio*) della fondatezza delle proprie ragioni nonché presentato elementi di prova ragionevolmente accessibili e sufficienti per comprovare le sue affermazioni e abbia indicato elementi di conferma delle stesse detenuti dalla controparte, le autorità giudiziarie abbiano la facoltà di porre a carico della controparte l'onere di collaborare fornendo le informazioni necessarie per l'identificazione dei soggetti implicati nella contraffazione, disponendo che detti elementi siano forniti da quest'ultima se non eccedono la gravità dell'illecito. La prova piena dunque può essere spostata alla controparte, a cui peraltro sono più prossimi i fatti da provare, mentre a carico della parte attrice rimane "solo" la disponibilità degli elementi di prova (seri indizi). Le ragioni che han portato ad introdurre tali elementi di specialità nella *ratio* della norma dell'Accordo TRIPs è da ricercarsi sia nella volontà di compensare/livellare questa asimmetria informativa delle parti nella tutela della proprietà intellettuale, poiché la parte in possesso dei dati detiene un vantaggio maggiore rispetto alle società che non possono che supplire a questo deficit, sia nella volontà di accrescere l'efficienza della tutela contro la contraffazione da un punto di vista sia economico che materiale, giacché permette da un lato di individuare tutti i soggetti che hanno perpetrato l'atto illecito e dall'altro di diminuire il dispendio di tutto grazie alla partecipazione di tutti i soggetti concorrenti nell'illecito al medesimo processo. Del resto, su di un piano funzionale,

18 Di fatto: l'art. 156*bis* l.d.a. sia stato introdotto dal d.lgs. n. 140/2006, in attuazione dell'art. 8 della Direttiva 2004/48, a sua volta attuazione dell'art. 43 dell'accordo TRIPs. Tale norma individua la cd. *discovery* e prevede che la parte, che abbia fornito seri elementi circa il fondamento della propria domanda ed abbia individuato documenti, elementi o informazioni detenuti dalla controparte a conferma di tali indizi, possa ottenere che il Giudice ne disponga l'esibizione oppure ne chieda la comunicazione. La *discovery*, come è intuibile, può essere altamente invasiva e penetrante, di talché la legge prevede (3° comma, art. 156*bis* l.d.a.) che il giudice, nel pronunciare tale ordine, adotti tutte le misure idonee a garantire la tutela delle informazioni riservate, sentita la controparte.
L'art. 156*ter*, inserito come sopra, ricalca fedelmente la norma comunitaria che garantisce il diritto di informazione, consentendo al giudice di ordinare, su istanza giustificata e proporzionata del richiedente, che vengano fornite informazioni sull'origine e sulle reti di distribuzione di merci o di prestazione di servizi che violano un diritto di proprietà intellettuale, cioè tutte le informazioni necessarie per comprendere ed accertare le dimensioni e la portata del fenomeno contraffatorio consentendo però al soggetto leso di estendere l'azione a terzi (ed accogliendo pertanto la puntualizzazione delle ricorrenti) oppure per intentarne una nuova o chiedere la tutela in sede penale.

la posizione di Tiscali si pone in rapporto alla pretesa violazione dei diritti d'autore allo stesso modo di quella del produttore del sistema operativo utilizzato dagli utenti o, piuttosto, della società costruttrice del PC. Queste peculiarità nella *ratio* della norma nel sistema di acquisizione della *discovery* decretano la stessa come speciale e non come eccezionale, giacché altre norme inerenti la proprietà intellettuale derogano alla disponibilità e onere della prova (come quelle ad esempio della consulenza tecnica) introducendo anch'esse *rationes* di specialità. La norma è quindi suscettibile di interpretazione estensiva ed analogica. Parallelamente l'ammissibilità della prova raccolta in via preliminare con la *discovery* come azione di istruzione preventiva non inerisce una mera azione di merito, bensì il processo *in toto* assicurando una prova assicurar una prova altrimenti a rischio vanificazione, come per l'appunto le informazioni volatili detenute dalla resistente [19]. I dati, infatti, trattati e memorizzati dal fornitore della rete pubblica o del servizio pubblico di comunicazione elettronica

19 L'azione ed il processo cautelare costituiscono per il Giudicante uno strumento d'azione necessario per l'effettiva tutela del diritto controverso, costituzionalmente rilevante ai sensi dell'art. 24 della nostra Carta fondamentale, allorché si prospetti una situazione di pericolo nel ritardo, che, in quanto tale, non tollera attese e necessita di una risposta di tutela a volte immediata. Ivi mi permetterei di sollevare una questione sulla natura dei conflitti tra *privacy* e diritti di azione e di difesa, esercitati ai sensi dell'art. 24 Cost: derivano essi da aporie del sistema oppure sono il prodotto di fisiologici rapporti di forza tra fenomeni giuridici sufficientemente disciplinati dal legislatore? Ancora, si può immaginare che esista una soglia, sia sul fronte della *privacy* che su quella del processo, oltre la quale non dovrebbe essere lecito spingere il contrasto, al costo di determinare fratture insanabili su entrambi i versanti? Lo sforzo volto ad individuare quel limite è un'impellenza pratica prima ancora che teorica, che ha condotto spesso a risultati instabili e raramente sussumibili a regola generale: gestire questo tipo di flessibilità, anziché privilegiare la cristallizzazione di schemi rigidi e ineludibili dove ricondurre la tutela di un diritto, quello della riservatezza, che è proteiforme ed in incessante evoluzione, ma che al contempo esige un elevato standard di protezione in forza della sua appartenenza alla categoria dei diritti della personalità, è una soluzione accettabile o comporta sacrifici sproporzionati rispetto agli esiti? I rischi insiti nell'avventurarsi nel delicato campo dell'individuazione dei limiti del diritto alla riservatezza sono principalmente due e corrispondono al pericolo di accordare alla *privacy* una dimensione troppo estesa, comprimendo altri interessi pure rilevanti o di restringerla oltremisura, vanificando in concreto il riconoscimento astratto del diritto stesso. L'art. 24 Cost., riassume nei concetti di azione e di difesa un'amplissima varietà di attività processuali capaci di influire sulla decisione giudiziale, sì che qualsiasi istituto, indifferentemente sostanziale o processuale, che abbia l'attitudine di pregiudicare l'esercizio dei poteri processuali garantiti e quindi di impedire alle parti di influire sugli esiti decisori del giudice, dovrebbe stimarsi incostituzionale. Distinguendo poi tra limiti esterni (che riguardano la tutela di interessi estranei alla funzionalità degli strumenti processuali) e limiti interni all'azione (che si giustificano proprio per consentire il perseguimento dei fini del processo), l'illegittimità dei primi, causata dalla sproporzione tra le finalità da essi perseguite e la forza con cui comprimono i poteri processuali delle parti, è il frutto di una valutazione lato *sensu* politica con cui si graduano, in un determinato periodo storico, le priorità sottese a quei differenti fini. Orbene, una conquista dei nostri tempo è indiscutibilmente il valore della persone e dei suoi dati, permeato dal concetto etico, ma positivizzato, che è peraltro richiamato dal Codice della *privacy*. Che il diritto alla *privacy* sia un diritto fondamentale della persona, è una premessa non revocabile e non in dubbio; ciò che preme chiarire è che l'interesse preminente non può tuttavia essere determinato a priori, in base ad un giudizio astratto, ma solo a seguito di un bilanciamento operato in un'ottica relativistica e fattuale.
E di fatto il processo in cui è possibile utilizzare tali prove può essere anche cautelare come rilevato dall'art. 156*ter*, attuando pienamente l'art. 24 Cost. (che tutela in egual modo il diritto di azione giurisdizionale ordinaria di merito nonché quella cautelare per assicurare una tutela immediata dei diritti). L'art. 24 Cost. infatti comporta non solo la possibilità di una tutela attraverso l'impugnazione di provvedimenti in vista del loro annullamento, ma anche la possibilità di chiedere al giudice misure cautelari per evitare che la durata del giudizio produca un danno irreparabile all'interesse del ricorrente. Naturalmente devono esserci: a) i presupposti per l'instaurazione del processo, ovvero la domanda proposta a giudice competente e la capacità processuale della parte che sta in giudizio (persone che abbiano il libero esercizio dei propri diritti - art. 75 c.p.c); b) le condizioni dell'azione, e perciò la proponibilità della domanda, ovvero la possibilità giuridica (valutare se l'azione rientra nella fattispecie normativa esistente), la legittimazione ad agire (corrispondenza tra colui che pone la domanda e colui che è titolare del diritto), l'interesse ad agire (il soggetto che propone la domanda deve avere interesse alla tutela giurisdizionale del diritto che afferma).

devono essere di norma cancellati o resi anonimi quando non più necessari ai fini della trasmissione della comunicazione.

Avuto riguardo della qualificazione dell'azione di *discovery* come strumento in via preventiva e della sua effettiva possibilità giuridica, il Tribunale romano – in riferimento alle altre questioni sollevate dall'ISP, ovvero alla questione di legittimazione del gestore della rete e di pericolo – deve ora indagare se Tiscali è tenuta all'ostensione o meno dei dati identificativi richiesti dalla controparte. La soluzione di tale questione è rinvenibile all'interno dell'art. 156 *ter*[20], prevede che colui che si assume essere danneggiato possa chiedere al giudice, anche nei confronti di soggetti diversi dagli autori della violazione, un ordine di esibizione dei dati e delle informazioni necessarie all'individuazione dei responsabili dell'illecito, come appunto i *gate keeper* (i gestori di connettività *web*). Tale norma fonda quindi di per sé la legittimazione a resistere dell'ISP nel procedimento in esame.

In altre parole, non è rilevante il fatto che quanto più viene protratta l'attività illecita di *download*, tanto maggiore sarà il numero di persone che possono acquisire il *file* e, di conseguenza, a loro volta offrirlo in *upload* ad altri utenti che ancora non lo fanno causando «un danno grave ed al contempo irreparabile», quanto in realtà il fatto che l'ISP sia un prestatore di servizio di memorizzazione temporanea grazie al sistema di *catching*. La difficoltà di identificazione di tutti i singoli utenti che hanno effettuato il *downloading* dei file a distanza di tempo dalla loro azione commessa è insita pertanto nella stessa natura della galassia Web. Internet infatti permette con grande rapidità una moltitudine di accessi agli innumerevoli siti di *file sharing* ma al contempo anche un'estrema volatilità dei contenuti elettronici.

20 Secondo tale norma l'ordine di *discovery* «di fornire informazioni sull'origine e sulla reti di distribuzione di merci o di prestazione di servizi che violano un diritto di cui alla presente legge da parte [...] da ogni altra persona» diversa dall'autore della violazione che al punto b) «[...] sia stata sorpresa a fornire su scala commerciale servizi utilizzati in attività di violazione di un diritto».

## 3. Approfondimento sulle normative comunitarie

Alla base dell'intervento delle figure a tutela dei consumatori vi sta l'apparente disarmonia normativa tra, da un lato, la norma dell'art.8 della direttiva *enforcement* e la sua applicazione tramite le norme italiane (*ergo*, gli artt. 156 *bis* e 156 *ter* che tutelano i diritti di proprietà industriale) e, dall'altro, la normativa n. 196 del d.lgs. 30 giugno 2003 (Codice in materia di protezione dei dati personali, cd. Codice della *privacy*) nonché alcune norme delle direttive comunitarie in materia di società dell'informazione. In realtà tale questione era già stata risolta dalla giurisprudenza del Tribunale di Roma con diversi orientamenti non scevri da errori ed equivoci interpretativi ed ora affrontata dal processo C 275/06 del 29 gennaio 2008 dinnanzi alla Corte di Giustizia europea[21]. Tale questione pregiudiziale (C. 275/96) traeva origine dall'iniziativa giudiziaria da parte dell'associazione spagnola senza scopo di lucro a tutela degli interessi degli autori ed editori (Promusicae appunto) nei confronti del *provider* Telefonica de Espana SA U, il quale si era opposto alla richiesta di fornire identità ed indirizzo fisico degli utenti accusati di scaricare con programmi *peer-to-peer* contenuti protetti al fine di tutelarne la *privacy*. La Corte di Giustizia dell'Unione Europea aveva così affermato che «la comunità non impone agli Stati membri l'obbligo di comunicare i dati personali degli utenti dell'internet in caso di contenzioso civile. [...] La comunicazione dei dati richiesti è autorizzata esclusivamente nell'ambito di un'indagine penale o per la tutela della pubblica sicurezza e della difesa nazionale»[22]. Quindi

21 Si veda http://www.ippt.eu/files/2008/IPPT20080129__ECJ__Promusicae__v__Telefonica__concerning__KaZaa.pdf.

22 Nell'ambito della controversia pendente tra la Promusicae (associazione senza scopo di lucro), che agisce per conto dei titolari dei diritti di proprietà intellettuale che ne fanno parte, e la Telefonica, in cui quest'ultima si rifiuta di fornire alla prima dati personali relativi all'utilizzo di Internet mediante connessioni da essa fornite, il Judzgado Mercantil ha sospeso il processo e rinviato alla Corte di Giustizia per pronuncia pregiudiziale. La Corte spagnola chiedeva alla Corte di Giustizia europea se il diritto comunitario

la Corte, interpretando pregiudizialmente le disposizioni comunitarie[23], enunciava il principio secondo cui «non si impone agli Stati membri [...] di istituire un obbligo di comunicare dati personali per garantire l'effettiva tutela del diritto di autore nel contesto di un procedimento civile» pur affermando che l'art. 15 della direttiva 2002/58 attribuisce (agli Stati) la facoltà di siffatto obbligo. Essa aveva quindi confermato che il diritto comunitario consentiva agli Stati membri di circoscrivere all'ambito delle indagini penali o della tutela della pubblica sicurezza e della difesa nazionale – a esclusione, quindi, dei processi civili – il dovere di conservare e mettere a disposizione i dati sulle connessioni e il traffico generato dalle comunicazioni effettuate durante la prestazione di un servizio da parte degli operatori di rete e servizi di comunicazione elettronica. Secondo la giurisprudenza quindi il dovere di collaborazione degli ISP non poteva e non può spingersi fino alla comunicazione in favore del richiedente delle generalità degli intestatari dell'*account* e della linea telefonica. La giustificazione del suesposto orientamento pretorio trova un forte ancoraggio nella disciplina sul trattamento dei dati personali che in assenza di idonea informativa e acquisizione del consenso dell'interessato esclude l'acquisizione dei dati elettronici altrui. La via da seguire e vincolante per gli Stati membri, come indicato dalla Corte nonché dal Giudice europeo in tale pronunzia, risulta dunque quella del giudizio da adottarsi caso per caso impostato sulla tecnica del bilanciamento tra i diritti in gioco atto a individuare il giusto equilibrio. La tutela dei dati personali e la necessità del conseguimento degli obiettivi di rafforzamento della tutela della proprietà intellettuale vanno pertanto equamente bilanciate e ciò deve essere fatto, innanzitutto, operando correttamente nell'ambito del regime delle ipotesi eccezionali delineato dalle stesse direttive sulla protezione dei dati nonché del bilanciamento dei diversi diritti fondamentali delineati dal sistema comunitario e dei riflessi che questo ha su quello interno. Il presupposto tanto dell'operatività della causa di esclusione del consenso, quanto della realizzazione dell'eventuale bilanciamento è che i dati sensibili siano trattati per le finalità espressamente indicate dal legislatore e per il tempo strettamente necessario al loro conseguimento. Avuto riguardo di ciò, la tutela del diritto d'autore e della proprietà intellettuale non può spingersi fino al punto di comprimere altri diritti fondamentali come la tutela dei dati personali, la libertà di ricevere e comunicare informazioni e la libertà di impresa. La Corte, per questa serie di motivazioni, si esprimeva a favore delle eccezioni espresse dal *provider* evidenziando come la tutela del diritto d'autore non sia un diritto intangibile e che pertanto è suscettibile di flessioni allorquando venga a misurarsi con i diritti fondamentali di pari rango, come la libertà d'impresa del *provider,* o con diritti superiori, come la tutela dei dati personali (quali gli indirizzi IP degli utenti nel caso *de quo*), la tutela della segretezza delle comunicazioni, la tutela della libertà di comunicare o ricevere informazioni. Veniva quindi di fatto rimessa al giudice nazionale, in sede di ricostruzione del sistema, il bilanciamento tra gli interessi in conflitto e, perciò, tra l'interesse alla protezione del diritto di autore quale diritto di proprietà intellettuale ed il diritto alla protezione dei dati personali[24].

Merita sottolineare come in materia di di-

(specificatamente art. 15 e 18 della direttiva 2000/31, l'art. 8 della direttiva 2001/29 e l'art. 8 della direttiva 2004/48 nonché gli articoli 17 e 42 della Carta di Nizza del 7 dicembre 2000) consentano agli Stati membri di escludere nei processi civili, l'obbligo di conservare e mettere a disposizione i dati sulle connessioni ed il traffico generati dalle comunicazioni effettuate, durante la prestazione di un servizio della società dell'informazione, da parte degli operatori di rete e di servizi di comunicazione elettronica nonché ai fornitori di accesso alle reti di telecomunicazioni.

23 E specificatamente i seguenti articoli di legge di disposti comunitari: artt. 15 e 18 della direttiva 2000/31, art. 8 paragrafo 1 e 2 della direttiva 2001/29, art. 8 della direttiva 2004/48 nonché gli artt. 17 e 47 della Carta di Nizza, più avanti spiegati nel dettaglio.

24 La Corte quindi da un lato richiama gli Stati membri, nella trasposizione delle direttive comunitarie, ad una interpretazione delle medesime (quindi in sede di attuazione delle misure di recepimento delle dette direttive) tale da essere conforme al diritto comunitario e dall'altro ad un'interpretazione delle direttive stesse che garantiscano un giusto equilibrio tra i diversi diritti fondamentali tutelati dall'ordinamento giuridico comunitario, adeguando il significato alla protezione dei diritti come quello di proporzionalità.

ritto d'autore, il contesto normativo comunitario a cui tener fede sia da rinvenirsi nel:

L'art. 2 della Direttiva *enforcement*, che fa salva l'applicazione delle direttive 95/46/CE (relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati)[25], 1999/93/CE (relativa ad un quadro comunitario per le firme elettroniche)[26] e 2000/31/CE (relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno, cd. infatti "direttiva sul commercio elettronico")[27];

L'art. 3 della stessa direttiva *enforcement*, il quale prevede che non si possa disporre un obbligo di vigilanza attiva sui dati degli utenti per prevenire violazioni dei diritti di proprietà intellettuale, in quanto onere incompatibile con il principio del suddetto articolo (secondo cui le misure contemplate devono essere eque, effettive, proporzionate e non eccessivamente costose);

Il comma 3 dell'art. 8 della stessa direttiva che fa salve le altre disposizioni regolamentari che «[...] e) disciplinano la protezione o la riservatezza delle fonti informative o il trattamento di dati personali»;

l'art. 156 della legge 1941/633 comma 3 che infine ben esplica il concetto di *discovery* affinché «siano adottate le misure idonee a garantire la tutela delle informazioni riservate» per quanto concerne l'ordine di *discovery*.

Quanto alla definizione di trattamento dei dati personali, soccorrono quelle contenute nella norma comunitaria 95/46/CE soprarichiamata, secondo la quale (all'art. 2) per "dati personali" si intende «qualsiasi informazione concernente una persona fisica identificata o identificabile (persona interessata)» anche indirettamente «mediante riferimento a qualsia-

25 Essa definisce un quadro normativo volto a stabilire un equilibrio tra un livello elevato di tutela della vita privata delle persone e la libera circolazione dei dati personali all'interno dell'UE. A tal fine, la direttiva fissa limiti precisi per la raccolta e l'utilizzazione dei dati personali e chiede a ciascuno Stato membro di istituire un organismo nazionale indipendente incaricato della protezione di tali dati. La disciplina sulla tutela della *privacy* o, meglio, sulla protezione dei dati personali fa la sua prima apparizione nel nostro Paese l'8 maggio 1997, con l'entrate in vigore della legge 31/12/96, n. 675 (emanata in attuazione della suddetta disposizione comunitaria ed internazionale con la Convenzione di Strasburgo n. 108 del 1981). Dopo ben nove decreti legislativi in sette anni, in linea con gli orientamenti dell'epoca in tema di semplificazione, il Governo è stato infine delegato ad adottare un "testo unico", divenuto poi Codice contenente tutte le disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali e delle disposizioni "connesse". Si veda www.governo.it/Presidenza/USRI/confessioni/.../direttiva_95_46.pdf.

26 L'estrema varietà delle normative adottate o, nella maggior parte dei casi, solo proposte, dai Paesi membri, in materia di riconoscimento giuridico delle firme elettroniche, ha richiamato l'intervento del legislatore comunitario volto a dettare un quadro comune, applicabile a tutti gli Stati membri, relativo alle condizioni e requisiti da applicarsi alle firme elettroniche e a rimuovere quegli ostacoli all'uso delle comunicazioni elettroniche e del commercio sulle reti telematiche. E così che nasce la "*Direttiva 1999/93/CE del Parlamento Europeo e del Consiglio relativa ad un quadro comunitario per le firma elettroniche*" entrata in vigore il 19 gennaio del 2000. La "firma elettronica" è un termine generale privo di qualsiasi prerogativa tecnico-giuridica che fa riferimento a qualsiasi tecnica finalizzata all'autenticazione elettronica che consente di associare dati ad altri dati (per esempio firma e documento).I metodi di autenticazione elettronica utilizzati per le firme elettroniche possono essere raggruppate in tre categorie, "qualcosa che sai", "qualcosa che sei", "qualcosa che hai", a seconda che il meccanismo di autenticazione si basi sulle conoscenze dell'utente (per esempio, la conoscenza di una parola chiave o di un numero di identificazione personale), sulle caratteristiche fisiche dell'utente (come l'impronta digitale o della retina) o sul possesso di un oggetto da parte dell'utente (come una tessera magnetica o una *smart card*). La direttiva comunitaria, ispirata al principio di "neutralità tecnologica" e contrariamente alla scelta fatta in precedenti comunicazioni, ha optato per la firma elettronica avendo il legislatore adottato "un approccio aperto alle varie tecnologie e servizi che consentono di autenticare i dati in modo elettronico". Infatti, il legislatore comunitario nel predisporre la disciplina della firma elettronica si è preoccupato della funzione che tale firma deve svolgere evitando qualsiasi riferimento alle tecniche informatiche utilizzate al fine della sua creazione, permettendo così una facile apertura al progresso tecnologico. Si veda www.interlex.it/testi/99_93ce.htm.

27 Tuttavia, la direttiva non è volta ad introdurre nuove forme specifiche (e probabilmente pleonastiche) di diritto internazionale privato sui conflitti di legge, né si occupa di individuare la competenza degli organi giurisdizionali. Si veda www.camera.it/parlam/leggi/deleghe/03070dl.htm.

si altra informazione, ivi compreso un numero di identificazione», mentre per "trattamento dati personali" (rinvenibile all'art. 4 del Codice della *privacy*) qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione dei dati stessi, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione. È chiaro come le operazioni elencate, in specie in riferimento alla raccolta, alla conservazione ed alla comunicazione, siano legate tra loro da un nesso di sequenzialità e strumentalità. I dati infatti vengono prima raccolti, poi conservati per essere in un secondo momento comunicati alle condizioni di legge. La finalità di tale disposizione appare evidente: i dati personali vanno tutelati sempre, indipendentemente dalla loro comunicazione e diffusione, dalla possibilità stessa della lesione del valore sociale dell'individuo.

La stessa direttiva 95/46/CE all'art. 7 in riferimento ai principi relativi alla legittimazione del trattamento dei dati personali asserisce che il trattamento «può essere effettuato soltanto quando è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata, che richiedono tutela ai sensi dell'art. 1 paragrafo 1». Tuttavia l'art. 13 direttiva 95/46/CE nella sezione delle deroghe e delle restrizioni alla lettera d) limita la portata degli obblighi e dei diritti previsti dalle disposizioni a protezione dei dati personali agli Stati membri, se tale restrizione costituisce una misura necessaria alla salvaguardia «della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate»[28].

La direttiva 2000/31/CE all'art. 15 comma 2° invece, inerente l'assenza dell'obbligo generale di sorveglianza, statuisce altresì la facoltà per gli Stati membri di «stabilire che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati» e all'art. 18, in riferimento ai ricorsi giurisdizionali, prevede inoltre di porre rapidamente provvedimenti urgenti, anche provvisori, «atti a porre fine alle violazioni e a impedire ulteriori danni agli interessi in causa». Sul punto è forse il caso di specificare che, mentre ai sensi del comma 1 dell'art. 15 della direttiva sul commercio elettronico 2000/31/CE (recepito dall'Italia con l'art. 17 del D.Lgs. 70/2003), gli Stati membri nella prestazione dei servizi di "*mere conduit*"[29], "*caching*"[30]

28 Si veda www.governo.it/Presidenza/USRI/confessioni/.../direttiva_95_46.pdf ed il link eur-lex.europa.eu/homepage.html?locale=it per le direttive successive.

29 In forza del disposto dell'art. 14 del D.Lgs. 9 aprile 2003, n. 70 l'attività di *mere conduit* ossia di "semplice trasporto" di cui all'art. 12 della direttiva E-commerce consiste nella trasmissione di informazioni su una rete di comunicazione ovvero nella mera fornitura di accesso alla rete. La giurisprudenza ha, in considerazione della posizione di neutralità rispetto ai contenuti di fatto veicolati *on line* dai *carrier* (ossia dagli operatori telefonici) ovvero dagli *access provider* (ossia dai fornitori di connettività), è solita ritenere tali soggetti esonerati da responsabilità (cfr: Tribunale di Catania, 29 giugno 2004; Tribunale di Napoli, 8 agosto 1997; Tribunale di Roma 4 luglio 1998; Tribunale di Cuneo 19 ottobre 1999; Tribunale di Milano 3 giugno 2006). Vale, comunque, segnalare che il terzo comma dello stesso art. 14 consente che le autorità giudiziarie od amministrative aventi funzioni di vigilanza possano esigere anche in via d'urgenza che il prestatore dei servizi di *mere conduit* impedisca o ponga fine alle violazioni per suo tramite commesse.

30 In forza del disposto dell'art. 15 del D.Lgs. 9 aprile 2003, n. 70 l'attività di *caching* di cui all'art. 13 della direttiva E-commerce consiste nell'attività di memorizzazione automatica, intermedia e temporanea delle informazioni effettuata ai fini dell'efficace successivo inoltro al destinatario; anche il secondo comma del citato art. 15 prevede che le autorità giudiziarie od amministrative aventi funzioni di vigilanza possano esigere anche in via d'urgenza che il

ed "*hosting*"[31] non impongono agli Internet Service Provider un obbligo generale di sorveglianza sulle informazioni trasmesse o memorizzate, né un obbligo generale di ricercare attivamente i fatti o le circostanze atti ad individuare eventuali attività illecite, ai sensi del 2° comma dello stesso art. 15 il legislatore comunitario concede agli Stati membri la facoltà di stabilire alcuni obblighi di informazione a carico degli *Internet Service Provider*, sebbene il legislatore italiano non si sia avvalso di tale facoltà.

Sebbene le direttive 2000/31, 2001/29, 2002/58 e 2004/48 non impongano agli Stati membri, in una situazione come quella oggetto della causa principale, di istituire un obbligo di comunicare dati personali per garantire l'effettiva tutela del diritto d'autore nel contesto di un procedimento civile, la Corte ha tuttavia dichiarato che essa non ha escluso, *sic et simpliciter*, la possibilità per gli Stati membri di stabilire un dovere di informazione a carico del fornitore di accesso a Internet, in applicazione all'art. 8, n. 1 della direttiva 2001/29. Tant'è vero che al paragrafo 3 del medesimo articolo prevede l'inibitoria nei confronti «degli intermediari i cui servizi siano utilizzati da terzi per violare un diritto di autore o diritti connessi». Si deve altresì rilevare che all'art. 9 la stessa Corte fa invece salva l'applicazione delle disposizioni sul rispetto della vita privata, secondo cui la tutela della proprietà intellettuale non deve essere d'ostacolo alla tutela dei dati personali, anche su Internet. Certo è che, in sede di applicazione delle misure di trasposizione delle suddette direttive, le autorità ed i giudici degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme a tali direttive, ma anche fare attenzione per evitare di fondarsi su un'interpretazione di queste ultime che entri in conflitto con i diritti fondamentali o con gli altri principi generali del diritto comunitario (come il principio di proporzionalità).

Del resto, la cd. direttiva sulla *privacy* (2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle telecomunicazioni), sancisce all'art. 5 il principio di tutela della riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione, ma al contempo prevede legislativamente all'art. 15 limiti alla suddetta tutela con misure che siano necessarie, opportune e proporzionate all'interno di una società democratica per la salvaguardia - tra gli altri interessi - di quelli lesi da reati e, quindi, per la prevenzione, la ricerca e l'accertamento degli stessi, ai sensi anche della direttiva 1995/46/CE del 24 ottobre 1995 (tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di dati). Ciò è emblematico della difficoltà di tracciare il giusto equilibrio tra diritti di valore costituzionale, tanto significativi e socialmente rilevanti (quale la riservatezza, la libertà di espressione, la segretezza delle comunicazioni – da un lato – e la sicurezza dello Stato e pubblica, dall'altro lato).

Emblematica è anche la Carta di Nizza. Questo prodotto di diritto costituzionale comparato internazionale ed europeo, costituisce un modello di regolamentazione "combinato", che introduce un sistema comunitario di tutela dei diritti congeniale alle peculiari esigenze dell'UE. La Carta infatti era al momento – e fino a che non venne inserita nei Trattati – uno

prestatore dei servizi di *caching* impedisca o ponga fine alle violazioni per suo tramite commesse.

31 In forza del disposto dell'art. 16 del D. Lgs. 9 aprile 2003, n. 70 l'attività di *hosting* di cui all'art. 14 della direttiva E-commerce, consiste nell'attività di memorizzazione delle informazioni di talché che il fornitore di *hosting* corrisponderà al titolare del *server* presso cui sono conservati e resi accessibili al pubblico dati e materiali: anche il terzo comma del citato art. 16 prevede che le autorità giudiziarie od amministrative aventi funzioni di vigilanza possano esigere anche in via d'urgenza che il prestatore dei servizi di *hosting* impedisca o ponga fine alle violazioni per suo tramite commesse. Perché si configuri una responsabilità penale del fornitore del servizio di *hosting* è necessario che costui sia effettivamente a conoscenza del fatto che l'attività o l'informazione memorizzata sono illecite di talché è verosimile ritenere che egli cooperi per la realizzazione del sito con l'autore dell'immissione di contenuti protetti (Cfr: Tribunale di Catania, 29 giugno 2004 che fra l'altro configura la possibilità di una responsabilità a titolo di colpa nel caso in cui l'ISP consapevole dell'esistenza di materiale sospetto si astenga dall'accertarne l'illiceità e dal rimuoverlo dal proprio *server*; Tribunale di Cuneo 19 ottobre 1999; Tribunale di Milano, 18 marzo 2004).

strumento di *soft law*, la cui utilità si rilevava soprattutto a fini interpretativi. Enunciava infatti i diritti e i principi che dovevano essere rispettati dalla UE in sede di applicazione del diritto comunitario. Ecco allora che gli art. 17 e 47 tutelano quali diritti fondamentali rispettivamente il diritto di proprietà, a cui può ascriversi anche il diritto di proprietà intellettuale, ed il diritto ad un ricorso effettivo dinnanzi al giudice, mentre gli artt. 7 e 8 garantiscono rispettivamente il diritto al rispetto della vita privata e il diritto alla tutela dei dati personali, riproducendo l'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e richiamati nel secondo *considerando* della citata direttiva sulla *privacy* 2002/58 secondo cui «la presente direttiva mira a rispettare i diritti fondamentali e si attiene ai principi riconosciuti in particolare dalla Carta dei diritti fondamentali dell'Unione Europea. In particolare, la presente direttiva mira a garantire il pieno rispetto dei diritti di cui agli articoli 7 e 8 di tale Carta».

## 4. Approfondimento sulle normative nazionali interessate

Se quello finora visto era il contesto comunitario a cui ascrivere la soluzione del procedimento, il contesto normativo interno e nazionale a cui si rifà il Tribunale capitolino è il d.lgs. 30 giugno 2003, n. 196 contenente delle norme-guida per chi deve far valere in giudizio un proprio diritto. Il legislatore storico si era dunque preoccupato di disegnare dei modelli di bilanciamento tra i divergenti interessi sottesi alle posizioni di chi pretende il rispetto della *privacy* e di chi, per agire o difendersi dinnanzi ad un giudice, ha bisogno di trattare i dati personali (sensibili o supersensibili) delle parti o di estranei al processo. Tale Codice della *privacy* fissava pertanto alcuni principi generali che governano la sua intera struttura e, quindi, disciplinano il trattamento dei dati personali; in particolare:

1 Principio di finalità (art. 11, comma 1, lett b), in base al quale il trattamento è lecito soltanto se alla sua base sussiste una ragione che lo giustifica, appunto la finalità. In base al suddetto principio le finalità devono essere determinate, esplicite e legittime e di pertinenza del Titolare del trattamento.

2 Principio di necessità (art. 3): i sistemi informativi e i programmi informatici devono essere configurati, già in origine, in modo da indurre al minimo l'utilizzo di informazioni relative a utenti identificabili. Il trattamento di dati personali non è, pertanto, lecito se le finalità del trattamento possono essere perseguite con dati anonimi e solo indirettamente identificativi;

3 Principio di proporzionalità (art. 11, comma 1, lettera d): tutti i dati personali e le modalità del loro trattamento devono essere pertinenti e non eccedenti rispetto alle finalità perseguite (è sproporzionato, per esempio, il trattamento di dati che per la finalità dichiarata non è necessario trattare).

Da ciò ne si evince come i dati non siano accessibili *de plano*, solo perché servono ad esercitare il diritto di difesa, bensì soltanto dopo un'attenta ponderazione su tutela della riservatezza e funzione giudiziaria volta a tutelare diritti costituzionalmente garantiti. Di fatto gli artt. 123 e 132 del Codice in materia di protezione dei dati personali, con i quali sono stati trasposti nell'ordinamento italiano gli articoli 5, 6 e 15 della direttiva 2002/58/CE in materia di trattamento dei dati personali e di tutela della vita privata nel settore delle comunicazioni elettroniche evidenziano:

i. L'art. 123, che riguarda il trattamento dei dati relativi al traffico, individua in particolare il periodo di tempo entro il quale il fornitore può trattare i dati strettamente necessari. Vieta infatti in generale la conservazione dei dati relativi al traffico generati nel corso delle comunicazioni, a eccezione della conservazione espressamente autorizzata per i fini indicati nella direttiva medesima (quali la prevenzione, la ricerca, l'accertamento ed il perseguimento dei reati). Partendo dal principio secondo il quale i dati non devono essere formati se non sono necessari e proporzionati ai fini della funzionalità della rete o della prestazione del servizio (artt. 3 e 11 del Codice ), il legislato-

re ha stabilito altresì il divieto generale di conservazione dei dati relativi al traffico (art. 123, comma 1 cit.), con le seguenti eccezioni:

a) è consentito il trattamento di dati strettamente necessario a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione (nei limiti e con le modalità di cui all'art. 123, comma 2) o, previo consenso dell'utente, a fini di commercializzazione di servizi di comunicazione elettronica, per la durata a ciò necessaria (art. 123, comma 3);

b) è prescrittala conservazione dei dati di traffico per esclusive finalità di accertamento e repressione dei reati (art. 132 del Codice).

ii. La norma contenuta nell'art. 132 riguarda invece la facoltà di derogare al divieto assoluto di trattamento dei dati (anche se di ciò lo Stato italiano non si è valso). Il nostro legislatore ha tuttavia scelto di limitare le deroghe, in riferimento alle norme protettive della riservatezza e del trattamento dei dati personali, squisitamente al caso di illeciti penali, senza estenderle al caso di illeciti civili. Tale scelta risulta peraltro conforme al diritto comunitario come interpretato dalla Corte di Giustizia con la pronuncia della Promusicae, la quale esclude per l'appunto l'obbligo di comunicazione dei dati in processi civili. Pertanto la deroga al divieto di trattamento dei dati senza consenso risulta ristretta solo al caso di azioni giudiziari penali, in cui vige l'obbligo di conservare i dati per un limitato periodo di tempo, parametrato sulla gravità del reato commesso, al fine dell'utilizzazione e comunicazione delle informazioni stesse come prova nel processo penale[32].

## 5. L'annosa questione del bilanciamento dei diritti fondamentali

Nell'attuale quadro normativo interno, pur esistendo una definizione generale di "dati relativi al traffico", dettata dall'art. 4 comma 2 del Codice della *privacy*, lett. b), tali dati non vengono né enumerati né distinti espressamente *(dati relativi al traffico telefonico vs quelli inerenti al traffico telematico)*. La definizione delle diverse categorie di dati risulterebbe invece necessaria, dal momento che il legislatore italiano, differentemente da quello comunitario[33], ha

32 Quindi prescrive ai fornitori di servizi di comunicazione elettronica di conservare, per finalità di accertamento e repressione di reati, i dati relativi al traffico telefonico, inclusi quelli concernenti le chiamate senza risposta, e i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, rispettivamente per ventiquattro e sei mesi (art. 132, comma 1 del Codice). Prescrive, inoltre, agli stessi fornitori di conservare tali dati per un periodo ulteriore, rispettivamente di ventiquattro e sei mesi, per l'accertamento e la repressione dei delitti tassativamente individuati dall'art. 407, comma 2, lett. a), c.p.p., nonché dei delitti in danno di sistemi informatici o telematici (art. 132, comma 2). Infine, prevede che la conservazione dei predetti dati sia effettuata nel rispetto di specifiche misure ed accorgimenti a garanzia degli interessati. L'individuazione di tali cautele è stata demandata al Garante per la protezione dei dati personali (cfr. artt. 17 e 132, comma 5 del Codice). Prima dell'adozione della direttiva 2002/58/CE, il pubblico ministero poteva raccogliere i dati del traffico telefonico presso i *service providers*, ove fossero conservati per ragioni di fatturazione, con decreto ex. art. 256 c.p.p. A tale proposito, la Suprema Corte a sezione unite aveva affermato che, ai fini dell'acquisizione dei tabulati contenenti i dati esterni identificativi delle comunicazioni telefoniche conservati in archivi informatici presso il gestore del servizio, è sufficiente il decreto motivato dell'autorità giudiziaria, non essendo necessaria, per il diverso livello di intrusione nella sfera di riservatezza che ne deriva, l'osservanza delle disposizioni relative all'intercettazione di conversazioni o comunicazioni di cui agli artt. 266 c.p.p. Secondo i giudici di legittimità, «*l'estensione della tutela costituzionale dei dati esterni delle intercettazioni è un risultato conseguibile in via interpretativa come soluzione costituzionalmente orientata, suggerita dal giudice che l'individua nell'art. 256 c.p.p. etero integrato dal precetto costituzionale dell'art. 15, norma quest'ultima che è di matrice unica della tutela della segretezza e della riservatezza delle comunicazioni*». La normativa qui esaminata accoglie quindi il principio di "neutralità dei mezzi", garantendo un uniforme livello di tutela, qualunque sia la tecnologia – digitale o analogica – utilizzata per la fornitura del servizio senza discriminare i mezzi che, almeno nell'immaginario comune, hanno un maggiore grado di pericolosità.

33 La direttiva 2006/24/CE contiene infatti specifiche indicazioni sui tempi di conservazione (minimo sei mesi e massimo due anni) e sulla individuazione delle categorie dei dati da conservare, elencate nell'art. 5: a) i dati necessari per rintracciare e identificare la fonte di una comunicazione; b) i dati necessari per rintracciare e identificare la destinazione di una comunicazione; c) i dati necessari per determinare la data, l'ora e la durata di una comunicazione; d) i dati necessari per determinare il tipo di conversazione; e) i dati necessari

individuato diversi periodi di conservazione in relazione alla natura telefonica o telematica del dato da conservare. Ed infatti, l'attuale meccanismo legislativo della *data retention* prevede un preciso vincolo di conservazione dei dati per finalità di accertamento e repressione di reati, che comporta conseguentemente una precisa limitazione per i fornitori nell'eventualità in cui essi ricevono richieste volte a perseguire scopi diversi.

Il legislatore nazionale ha quindi in qualche modo già effettuato il bilanciamento tra i diritti fondamentali di proprietà intellettuale e di riservatezza, giustificando che la prevalenza del diritto di proprietà intellettuale sul diritto alla riservatezza sia possibile solo nel caso in cui sia in gioco la lesione di interessi della collettività protetti nell'ambito del diritto penale[34]. Nel caso in cui però, come accaduto, sia leso soltanto l'interesse individuale del titolare che detiene il diritto di esclusiva circa la proprietà intellettuale la prevalenza sarà data al diritto alla riservatezza. La protezione offerta dal diritto d'autore non può quindi finire con l'erodere i margini dei diritti fondamentali garantiti tramite il sistema delle eccezioni e limitazioni. Il novero dettagliato e tassativo delle eccezioni previste dal diritto dell'Unione non permette infatti un'interpretazione delle medesime in linea con i tempi, imponendo pertanto di spostare la risoluzione del conflitto – e il conseguente accoglimento di nuove istanze che siano maggiormente al passo con lo sviluppo tecnologico e del mercato – all'esterno dell'istituto del diritto d'autore e ricorrendo così ai diritti dell'uomo, sia per l'interpretazione delle eccezioni e limitazioni già esistenti, sia per invocare l'inserimento di nuove ipotesi di sfruttamento delle opere dell'ingegno da parte dei singoli e della collettività. Si veda peraltro

per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature ; f) i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile. In ogni caso, anche alla luce del Provvedimento generale del Garante per la protezione dei dati personali del 24 luglio 2008, nella categoria dei servizi "telefonici" sono compresi: le chiamate telefoniche, incluse le chiamate vociali, di messaggeria vocali, in conferenza e di trasmissione dati tramite telefax, i servizi supplementari incluso l'inoltro e il trasferimento di chiamata, la messaggeria ed i servizi multimediali, inclusi i servizi sms; vanno invece ricondotti nella categoria dei servizi "telematici", l'accesso alla rete Internet; la posta elettronica; i fax inviati per mezzo Internet, la telefonia via Internet.

34 Come è ormai noto, per bilanciamento o ponderazione si intende una tecnica argomentativa il cui uso si rende necessario allorché la questione da decidere non sia o non sembri direttamente regolata da una norma giuridica univoca e precisa, e anzi sembri parimenti sussumibile contemporaneamente sotto due o più norme: in altre parole, quando la premessa maggiore del sillogismo giudiziale non contiene (o meglio, non contiene ancora) una regola precisa e univoca da applicare in maniera sussuntiva al caso. In simili casi, il giudice ha davanti a sé una pluralità di norme tutte valide e rilevanti per il caso da decidere, ovvero, guardando la stessa situazione da una prospettiva diversa, una pluralità di interessi tutti giuridicamente rilevanti. Nell'assenza di un criterio giuridico chiaro e predeterminato che assegni prevalenza in via generale e astratta ad una delle due norme o interessi in conflitto, il giudice dovrà scegliere quale norma o interesse ritenere "più" rilevante nel caso concreto, e quindi prevalente rispetto agli altri o anche, se possibile, cercare un contemperamento (un bilanciamento appunto) tra le norme o interessi in conflitto. Le circostanze presenti nell'ordinanza fanno sì che il concorso conflittuale riguardi normi che hanno (cui è attribuita) la qualificazione di principi, e specialmente principi "fondamentali", che esprimono diritti a loro volta fondamentali. Il bilanciamento ha dunque una natura bifronte, in quanto aspira a colmare lo spazio vuoto che divide le due anime del diritto: quella sapienziale (se non addirittura "buonista"), che vorrebbe ancorare la decisione giuridica all'apprezzamento quasi equitativo delle esigenze che emergono nel caso concreto, soppesando volta per volta le ragioni e i torti; e quella formalistica, se non legalistica, che aspira alla certezza del diritto e alla prevedibilità delle decisioni giudiziali adottate sulla base di norme generali e astratte. Ecco quindi che il bilanciamento, apparentemente incompatibile con la razionalità deduttiva propria del sillogismo giudiziale, cerca la sua legittimazione in altre forme di razionalità "sostanziale" (la ricerca di un ordine oggettivo di valori), o in forme di razionalità scientifica o aritmetica che assicurano la misurabilità e la non arbitrarietà delle scelte di volta in volta adottate. La necessità di bilanciare principi o diritti costituzionali ha come presupposto il fatto che principi o diritti configgano, ossia una situazione in cui due o più diritti non possono essere soddisfatti contemporaneamente. La pervasività del fenomeno del bilanciamento sembrerebbe implicare che anche i conflitti tra diritti o principi siano altrettanto pervasivi, ma di fatto questa posizione è controversa. Le posizioni che sono state espresse su questo punto sono alquante articolate. Per un simposio rimando a http://www.unipa.it/gpino/Conflitto%20e%20bilanciamento.pdf.

anche la sentenza della Corte costituzionale n. 372/2006 con cui si ribadisce la prevalenza sulla riservatezza quale valore fondamentale della persona in relazione alla legittimità costituzionale dell'art. 132 D.lgs. 196/2003 ed alla possibilità di conservare i dati di traffico delle comunicazioni tra privati per un tempo maggiore rispetto a quello previsto dalla stessa norma. In tale sentenza la Corte legittima la norma - in considerazione della necessità di contemperamento e bilanciamento del diritto alla riservatezza – solo perché riferita ad esigenze di tutela di beni della collettività minacciati dai gravi illeciti penali. Tutto ciò esclude, quindi, la possibilità di applicazione nell'ordinanza analizzata dell'art. 156 *bis* d.l.a. e dell'art. 24 del d.lgs. 196/2003 concernente il trattamento dei dati personali relativi alle comunicazioni elettroniche e telematiche tra privati per finalità connesse alla tutela dei diritti soggettivi degli stessi. Il tribunale romano infatti asserisce che questa prevalenza del diritto di *privacy* dei consumatori sul diritto proprietario non va a costituire una sottrazione di ogni tutela a fronte del fenomeno del *downloading*, ben potendosi ragionare in termini di responsabilità dei gestori della rete *peer-to-peer*[35] così come dei produttori e fornitori di servizi di *file sharing* specialmente dopo una dedita attenzione ai *leading case* statunitensi. In altre parole, il diritto fondamentale alla riservatezza può essere letto come lo strumento attraverso il quale limitare la "deriva protezionistica" del diritto d'autore. Poiché se è vero che il diritto di informazione e suoi corollari si fermano lì dove incominciano i diritti dei terzi – tra cui i diritti d'autore – ciò non equivale certo a permettere che l'espansione ingiustificata del diritto d'autore aumenti indiscriminatamente le ipotesi in cui la libertà di manifestazione del pensiero e i diritti succitati vengono ristretti a favore degli interessi privati di terzi. A ben vedere, la pedissequa ricerca di un bilanciamento tra questi istituti invocati altro non è che l'esteriorizzazione palese del mancato raggiungimento, all'interno del diritto d'autore, di un punto di equilibrio tra interesse privato e interesse generale.

Tuttavia a mio avviso, l'esigenza di garantire effettività alla tutela del diritto d'autore non può sfociare nello snaturamento del senso delle norme sulla responsabilità dei *provider*. Gli intermediari non possono essere gravati da un ordine volto all'adozione di sistemi di filtraggio, in quanto porterebbero, nei fatti, ad una sorveglianza generalizzata sulle informazioni trasmesse. Quanto alla tutela dei dati personali, non vi è dubbio che i *provider* sarebbero costretti a effettuare una raccolta e un'identificazione sistematica degli indirizzi IP degli utenti; rispetto alla garanzia della libertà di informazione, un sistema di filtraggio non potrebbe distinguere tra contenuti illeciti e leciti, finendo così, inevitabilmente, per infirmare la libertà degli utenti di ricevere e comunicare informazioni e ledere il diritto alla vita privata, diritto fondamentale forse molto più importante del diritto al trattamento dei dati personali[36].

35 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. Il fenomeno ha avuto inizio con "Napster", uno dei primi *software* di *file sharing* che in seguito a una lunga disputa legale è stato chiuso dalla giustizia americana. Napster metteva a disposizione dei propri utenti (tutti coloro che creavano un *account* e scaricavano gratuitamente da internet il suo programma proprietario) una vastissima libreria musicale formata dalle opere caricate dagli utenti stessi, da cui era possibile prelevare gratuitamente i brani prescelti. Non si trattava ancora di un vero e proprio sistema *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 diretto responsabile dell'attività illecita, ingiungendogli di interrompere tale attività. Lo sviluppo della decentralizzazione delle reti *peer to peer* è stata la risposta degli utenti di Internet alle reazioni dei titolari del diritto d'autore, in quanto le reti decentralizzate sono più difficilmente attaccabili in via giudiziaria, dal momento che non sono imputabili ad un singolo individuo o entità, come nel caso di Napster. Si sono così diffusi programmi di *file sharing*, grazie ai quali gli utenti possono condividere materiale protetto senza interfacciarsi con una piattaforma centrale, rendendo difficile risalire ad un unico responsabile; di conseguenza, anche le azioni legali delle *major* discografiche sono state meno efficaci.

36 Con riguardo alle questioni concernenti la responsabilità penale del provider, si rimanda a D. Minotti, *Responsabilità penale: il provider è tenuto*

## 6. Conclusioni

Dalle osservazioni che precedono deriva che il tema del diritto d'autore appare agli occhi delle istituzioni europee un argomento complesso nel quale devono però trovare risposta le legittime esigenze di tutela degli autori nel rispetto dei diritti e libertà fondamentali degli utenti, affinché venga favorita la diffusione della cultura nonché la promozione del mercato dei contenuti. La libertà di espressione e il diritto d'autore sono due valori fisiologicamente in tensione: non solo si scontrano laddove la libertà di accedere alla rete viene limitata per rendere effettiva la tutela di opere protette, ma esse si atteggiano naturalmente e quasi geneticamente come due prerogative in conflitto, in quanto il diritto d'autore garantisce una privatizzazione della conoscenza che stride con la libertà di ricercare e di ottenere informazioni da parte degli utenti, che costituisce, a sua volta, uno dei profili essenziali della libertà di espressione. Mentre il compromesso fisiologico tra libertà di ricercare e accedere alle informazioni e diritto d'autore vanta un'origine antica poiché attiene, per l'appunto, alla dimensione genetica dei diritti in gioco, il momento patologico di conflitto rappresenta per lo più un portato dell'innovazione tecnologica cui si è assistito nell'ultimo ventennio, e l'esplosione di Internet non è stata da meno a questo proposito. Infatti, l'avvento della tecnologia digitale ha moltiplicato le occasioni di emersione, ed a volte di esplosione, di tale conflitto, proiettandolo in una nuova dimensione, quella che si è definita patologica, poiché ha universalizzato l'accesso alle risorse tecniche che permettono la fruizione, lecita o meno, di opere protette.

La repressione con mezzi sproporzionati delle violazioni del diritto d'autore, oltre ad essere difficilmente attuabile, non ritengo sia l'obiettivo da perseguire. Ciò che diventa fondamentale è la ricerca di un equilibrio che veda quantomeno ridotte le violazioni ad un livello fisiologico. Gli studiosi più lungimiranti di fatto suggeriscono a gran voce che la portata del *copyright* sia ridimensionata, onde evitare che questo strumento rischi di trasformarsi in un freno all'innovazione e alla diffusione della cultura[37]. Le parole di Lessig su questo tema sono come sempre tra le più illuminanti: «La legislazione sul *copyright* non è mai stata la rocca di Gibilterra. Non è una serie di rigide imposizioni di cui, per qualche misteriosa ragione, adolescenti e appassionati di informatica ora vogliono farsi beffa. Al contrario, il potere del *copyright* è cresciuto in maniera notevole in un breve periodo di tempo, contemporaneamente alla trasformazione delle tecnologie per la distribuzione e la creatività, e alla spinta da parte dei lobbisti per assegnare un maggior controllo ai titolari del *copyright*. I cambiamenti del passato in risposta alle trasformazioni della tecnologia suggeriscono che potrebbero rendersi necessari mutamenti analoghi in futuro. E questi cambiamenti devono andare verso la riduzione del raggio d'azione del *copyright*, per contrastare lo straordinario aumento del controllo attivato dalla tecnologia e dal mercato».[38]

Si è quindi dinnanzi alla mancanza di criteri interpretativi idonei a fondare su solide basi dogmatiche il bilanciamento tra opposti interessi, nel rispetto sia dell'esigenza di certezza del diritto che dei limiti imposti dalla legislazione comunitaria. L'*impasse* esegetica appare ancora più aggravata dalla vaghezza dei criteri di proporzionalità e ragionevolezza dell' "equo bilanciamento" tra diritto d'autore e diritti fondamentali proposti dal legislatore

*ad "attivarsi"?*, in "InterLex", www.interlex.it,www.interlex.it/regole/minotti8.htm, il quale osserva che "il decreto, agli artt. 14, 15 e 16, solleva i prestatori da ogni responsabilità (diverse da quelle amministrative fissate nel decreto) a condizione che essi non intervengano sulle informazioni (i.e. i dati) da loro memorizzate o veicolate. Previsione di mero valore riproduttivo, atteso che, anche senza il decreto, l'intervento ('causale') sulle informazioni (consapevolmente illecite) poteva già condurre, per i principi generali di diritto penale, ad ipotesi di concorso commissivo".
Si veda anche M. Cammarata, *Le trappole nei contratti di hosting*, in "InterLex", www.interlex.it, www.interlex.it/regole/trappole.htm.

37 Si veda boa.unimib.it/bitstream/10281/30053/1/Phd__unimib__724942.pdf.

38 L. Lessig, *Cultura libera. Un equilibrio fra anarchia e controllo, contro l'estremismo della proprietà intellettuale*, Apogeo (www.apogeonline.com), 2005.

e dalla giurisprudenza comunitaria e dal fatto che tale vaghezza possa essere risolta solamente attribuendo al diritto d'autore uno specifico rango gerarchico costituzionale. L'operazione, già ostacolata dall'assenza di una classificazione sistematica unitaria della privativa ad opera degli ordinamenti nazionali, è resa ancora più ardua dalla "proprietarizzazione" del diritto d'autore europeo, operata dalle giurisprudenze CGUE e CEDU e ora consacrata dalla Carta Europea dei Diritti Fondamentali, che oltre a mancare di gerarchizzazione tra diritti fondamentali protetti, sembra far discendere dalla privativa al paradigma proprietario una sua lettura in termini ancora più assoluti, ben poco coerente con il concetto continentale di proprietà limitata dalla sua funzione sociale. Dinnanzi a tale quadro, è evidente come il tradizionale approccio atomistico e frammentato che da sempre ha contraddistinto la materia del diritto d'autore non sia più in grado di fornire risposte adeguate e come solo un più radicale sforzo di ricostruzione sistematica possa aiutare a risolvere i problemi oggi posti dall'interrelazione non sempre pacifica tra fonti civilistiche e costituzionali multilivello.

Si potrebbe affermare che al fine di tutelare il diritto d'autore, a seguito dello sviluppo e della diffusione delle reti di comunicazione elettronica, sia necessario, nonostante le complessità giuridiche e le problematiche tecnologiche di cui si è trattato, emanare una nuova normativa in materia di rimozione selettiva (e preventiva ?) dei contenuti illecitamente condivisi *online*, aggiornata e puntuale. Tuttavia una normativa da sola non è sufficiente a sconfiggere la cultura della pirateria, ma deve essere accompagnata dall'affermazione di un mercato dei contenuti *online* legale, funzionale e completo nonché dallo sviluppo di nuove licenze per il diritto d'autore che siano multiterritoriali e in grado di adattarsi maggiormente alla comunicazione su internet. Una possibile soluzione intermedia, che possa contemperare la tutela di chi produce e la libertà di chi fruisce, pur muovendosi all'interno del sistema giuridico attualmente in vigore, è quella che viene definita *open licensing* (si pensi a tutto il contesto del *software* libero e *open source* e al mondo dell'*open content*, come le licenze Creative Commons e similari).

Avuto riguardo di tutto ciò finora asserito, appare palese come l'ordinamento giuridico debba essere alla ricerca di un bilanciamento d'interessi interno: da un lato, l'interesse ad ampliare quanto più possibile l'accesso alla conoscenza e all'informazione in una società sempre più interconnessa mediante Internet e le reti sociali; dall'altro, l'interesse a far sì che tale accesso e la conseguente fruizione delle opere dell'ingegno si sviluppi in modi e forme tali da incoraggiare e premiare la creatività e l'innovazione, favorendo la crescita economica. In Europa un bilanciamento d'interessi accettabile risulta più arduo che altrove a causa di divergenze nella legislazione, nelle pratiche commerciali e nell'approccio dei legislatori nazionali a questioni giuridiche fondamentali che oltre vent'anni di direttive europee nell'ambito del diritto d'autore non hanno rimosso o attenuato. Dal 2010 l'Agenda Digitale della Commissione Europea persegue esplicitamente l'obiettivo di favorire la creazione di un Mercato Unico che riguardi, sempre più, i contenuti creativi digitali. La Commissione intende di fatto creare le condizioni affinché la domanda e l'offerta di contenuti protetti dal diritto d'autore possano svilupparsi - e verosimilmente crescere, a vantaggio dell'economia e dell'industria culturale e dell'informazione nel suo complesso - a livello paneuropeo o transnazionale, e non più all'interno dei singoli Paesi membri, come ancora accade nonostante l'intrinseco carattere transfrontaliero delle reti di telecomunicazione.

Concludendo, è di fondamentale importanza in un periodo storico così denso di mutamenti che il diritto si apra sempre più agli eventi, cambiando i propri schemi interpretativi, aggiornando le normative e gli orditi legislativi e, quando possibile, anticipando i fenomeni, in modo tale da non trovarsi impreparato e limitarsi ad offrire soluzioni tampone in delicati settori[39].

39 Si osservi come in parte il diritto si sia già adeguato al contesto mutevole della società tecnologica: http://www.filodiritto.com/corte-di-giustizia-i-provider-devono-bloccare-i-contenuti-che-violano-il-diritto-

*Monica Suerz è dottoressa magistrale in Scienze della Comunicazione Pubblica, d'Impresa e Pubblicità presso l'Università degli Studi di Trieste. Attualmente studentessa del Master in Imprenditorialità e Strategia Aziendale alla SDA Bocconi di Milano.*

monicasuerz@gmail.com

dautore-ma-hanno-liberta-di-scelta-delle-misure-piu-ragionevoli/#.U6GxBPl_vAg.