L'idra del *peer to peer* fra tutela della *privacy* ed *enforcement* dei diritti d'autore

SOMMARIO: 1. Tutela giudiziale dei diritti nel contesto digitale: il modello d'azione delle *major* statunitensi. — 2. Individuazione dei responsabili ed accesso ai dati di traffico. — 3. *Segue*: l'interpretazione della Corte di giustizia nella causa C-275/06. — 4. Concreta efficacia delle azioni legali a tutela del diritto d'autore e tecniche di *enforcement*.

1. — Tredici anni or sono Nicholas Negroponte (1) scriveva: « nel mondo digitale il problema non è tanto quello che copiare è più facile e che le copie sono più fedeli... [ma che] ritagliare i *bit* è molto diverso dal ritagliare atomi » (2). Vista l'evoluzione del settore *ICT* e lo sviluppo della rete *internet*, la distanza che ci separa dal 1995 pare ora siderale, eppure, in una realtà ove i dati viaggiano attraverso i continenti a 10 *megabyte* al secondo (3), rimane immutata la validità della sintesi efficacemente formulata da Negroponte.

È infatti la digitalizzazione — più che la rete *internet* (che della prima è figlia) — ad aver ridisegnato il mondo in cui viviamo, spostando il baricentro dal materiale all'« immateriale », dal tangibile all'« intangibile ». La *reductio ad unum* che si realizza attraverso la conversione in *bit* ha poi fatto il resto, consentendo la disaggregazione e la ri-aggregazione dei contenuti, nonché il definitivo superamento della secolare distinzione fra originale e copia. Ne è derivato un nuovo contesto, in cui in molti casi un flusso di *input* ha sostituito la *res*, decretando in tal modo se non la fine, quanto meno la crisi, di un sistema giuridico prevalentemente incentrato su beni suscettibili di apprensione e di controllo nello spazio (4).

Non pare questa la sede per ribadire osservazioni ormai consuete circa le difficoltà che da tale nuovo stato di cose sono derivate per i

(1) Nicholas Negroponte, informatico ed accademico statunitense, co-fondatore del MediaLab del Massachusetts Institute of Technology, è unanimemente considerato uno dei massimi esperti dell'*Information and Communication Technology* (*ICT*).

(2) Cfr. NEGROPONTE, *Essere digitali*, Milano, 1995, p. 56.

(3) Il riferimento è alla velocità di trasmissione fruibile dagli utenti della rete attraverso l'impiego del proprio *modem*.

(4) Cfr., con riguardo ai profili relativi alla tutela del diritto d'autore, SPADA, *Copia privata ed opere sotto chiave*, in *Riv. dir. ind.*, 2004, p. 601 e RICOLFI, *A copyright for cyberspace? The european dilemmas*, in *Ann. it. dir. aut.*, 2000, p. 444 s.

soggetti dell'ordinamento giuridico chiamati ora a confrontarsi, ora a cercare di regolamentare le variegate manifestazioni del nostro « essere digitali ». Con il presente scritto si vuole invece porre specifica attenzione agli effetti che i cennati mutamenti hanno avuto sull'illecita divulgazione dei contenuti protetti dal diritto d'autore in séguito alla diffusione degli scambi di opere in formato digitale attraverso sistemi c.d. *peer to peer*, valutando altresì le strategie di *enforcement* conseguentemente adottate.

A tal proposito occorre preliminarmente osservare come negli ultimi anni vi sia stata un'evoluzione delle tecniche di *file-sharing*, passando dalle reti *peer to peer* ibride ai sistemi *peer to peer* puri (5). Così, mentre in quello che è storicamente il *leading case* in materia, ovvero il caso Napster (6), era presente un *provider* che gestiva le funzioni di ricerca e di localizzazione delle risorse digitali rese disponibili dai *peer* (7), negli attuali sistemi di *file-sharing* viene fatto ricorso a reti prive di un nodo principale di riferimento e la ricerca dei *file* è affidata direttamente ai *peer* (8).

Evidenti sono le implicazioni giuridiche in tema di responsabilità correlate alla scelta delle due diverse architetture.

Nella prima ipotesi diviene infatti difficile per l'amministratore del *server*, che funge da mediatore in uno scambio di materiale protetto dal diritto d'autore, escludere non solo la conoscenza dell'attività illecita, ma anche il proprio attivo coinvolgimento in essa (9). Ne deriva che, te-

(5) Nel caso di sistemi *peer to peer* « puri »gli utenti che compongono la rete rivestono tutti lo stesso ruolo, ovvero hanno la capacità di essere contemporaneamente *client* (ricevere dati dagli altri) e *server* (fornire dati agli altri), mentre in quelli « ibridi » è anche presente un *server* centrale, cui si collegano tutti gli appartenenti alla rete (quindi in un rapporto *client-server*), avente il compito di rendere possibile il *file sharing* fra quest'ultimi, cfr. anche *infra* note 7 e 8.

(6) Sulle prime pronunce statunitensi in materia di fruibilità *on-line* di opere musicali in formato digitale protette dal diritto d'autore cfr. PASCUZZI, *Opere musicali su Internet: il formato MP3*, in *Foro it.*, 2001, IV, c. 101 ss.

(7) La rete aveva dunque natura « ibrida » in quanto vedeva la presenza di un *server* centrale, gestito da Napster Inc., con la funzione di rispondere mediante il proprio *data base* alle richieste provenienti dai diversi *peer* e di indicare quali altri *peer* rendessero disponibile la risorsa cercata, fornendo altresì l'indirizzo informatico delle relative macchine in maniera da consentire all'utente di collegarsi autonomamente a queste ultime.

(8) Si tratta dunque di reti *peer to peer* « pure », quali Gnutella e Freenet, dove manca un *server* centrale con funzione di indicizzazione; cfr. nota precedente. Vi sono poi sistemi intermedi fra quelli delle reti *peer to peer* « pure » e quelli delle reti *peer to peer* « ibride », quali eDonkey, che, attraverso il suo *client* eMule, risulta una delle reti più utilizzate.

(9) Cfr. *A & M Records, Inc. v. Napster Inc.*, 239 F. 3d 1004 (CA9 2001), pubblicata sul sito *http://cyber.law.harvard.edu*, cfr. anche *supra* nota 7. Nella specie la corte ha ravvisato nell'attività di Napster, con riferimento alla violazione del *copyright*, i caratteri del *contributory infringement* secondo cui chi « with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a "contributory" infringer », come affermato in *Gershwin Publ'g Corp. v.*

nendo conto della centralità assunta dal nodo principale della rete, per i soggetti lesi risulta nel contempo semplice ed efficace agire in giudizio solamente contro chi ne cura la gestione, causando così il collasso dell'intera rete, come accaduto con Napster.

Diversamente nella seconda soluzione viene a mancare un fulcro del sistema di comunicazione su cui concentrare l'azione giudiziaria (10), a fronte di una pluralità di soggetti che operano secondo le medesime modalità, impiegando lo stesso *software*, e rivestendo contemporaneamente la funzione di *client* e di *server* (11). Per tale ragione le *major* statunitensi, che per prime hanno dovuto affrontare questo mutamento nella tecnologia di diffusione, hanno optato per un'azione diretta contro gli autori ed i distributori del *software* utilizzato per il *file-sharing*, al fine di ottenere un effetto inibitorio sull'attività di tutti gli utenti della rete analogo a quello conseguito chiamando in giudizio i gestori dei *server* nel caso delle reti *peer to peer* ibride (12).

Sebbene l'offensiva sia stata coronata dal successo, come dimostrato dalla decisione della Corte suprema sul caso Grokster (13), nel contempo

Columbia Artists Mgmt., Inc., 443 F. 2d 1159, 1162 (2d Cir. 1971); a parere della Corte infatti « Napster, by its conduct, knowingly encourages and assists the infringement of plaintiffs copyrights ». I giudici hanno ravvisato inoltre una *vicarious liability* nell'operato di Napster, in quanto la società che gestiva il servizio di *file-sharing* aveva la possibilità di rendersi conto delle condotte illecite poste in essere dagli utenti ed aveva altresì un interesse economico ad esse correlato. Cfr. anche la successiva pronuncia *In re Aimster Copyright Litigation*, 334 F. 3d 643 (CA7 2003), pubblicata sul sito *http://digital-law-online.info.*

(10) Proprio l'esigenza di evitare il rischio di azioni legali, risultate fatali per Napster, è stata infatti all'origine dello sviluppo di reti di questo tipo.

(11) Per maggiori dettagli di carattere tecnico sul funzionamento di tale tipologia di rete e sulle metodologie impiegate per la ricerca delle risorse rese disponibili attraverso la stessa, cfr. RUFFO, *Protezione della privacy e della proprietà intellettuale: il caso* peer-to-peer *in Italia*, in BERGADANO-MANTELERO-RUFFO-SARTOR, *Privacy digitale. Giuristi e informatici a confronto*, Torino, 2005, p. 65 ss.

(12) In tal maniera si è cercato di adottare la soluzione meno onerosa, evitando i maggiori costi che avrebbero implicato cause « di massa » contro i singoli utenti delle reti *peer to peer*; cfr. in proposito un *obiter dictum* del caso *MGM Studios Inc. v. Grokster Ltd.*, 545 US 913 (2005), pubblicata sul sito *www.supremecourtus.gov* (consultato fra il 12 aprile 2008 ed il 25 maggio 2008, come tutti gli indirizzi *internet* successivamente citati), su cui *infra* nel testo ed in nota, in cui si legge: « When a widely shared service or product is used to commit infringement, it may be impossible to enforce rights in the protected work effectively against all direct infringers, the only practical alternative being to go against the distributor of the copying device for secondary liability on a theory of contributory or vicarious infringement ».

(13) Cfr. *MGM Studios Inc. v. Grokster Ltd.*, 545 US 913 (2005), cit., in cui i giudici, richiamando la *doctrine* Sony e dandone una lettura restrittiva in termini di esclusione di responsabilità, hanno ravvisato i caratteri del *contributory infringement* nella distribuzione di un *software* finalizzato alla realizzazione di reti *peer to peer* « pure »; cfr. *Sony Corp. of America v. Universal City Studios, Inc.*, 464 US 417 (1984), disponibile in traduzione italiana in *Foro it.*, 1984, IV, c. 351 ss. Secondo la Corte, nel caso Grokster, il programma, benché fosse anche suscettibile di usi legittimi, era stato distribuito con la principale, se non unica, finalità di consentire lo scambio di materiale protetto da *copy-*

sono tuttavia emersi i limiti di una simile strategia, insiti nella facilità con cui nel contesto digitale programmi non proprietari a protocollo aperto come quelli impiegati per la realizzazione delle reti *peer to peer* possono non solo circolare ed essere replicati, ma anche mutare in séguito ad una continua implementazione.

Per queste ragioni sia i titolari dei diritti d'autore che la *Recording Industry Association of America (RIAA)* e la *Motion Picture Association of America (MPAA)* hanno deciso di intraprendere anche una serie di azioni legali dirette contro i singoli utenti delle reti *peer to peer* (14), ricorrendo altresì all'invio mensile di centinaia di *pre-litigation letter* volte a sollecitare una soluzione stragiudiziale transattiva *ante causam* (15).

« Colpire » direttamente gli utilizzatori dei sistemi di *file-sharing* ha tuttavia una funzione essenzialmente deterrente, piuttosto che risarcitoria, posto che l'elevato numero degli utenti di tali sistemi e la massa di *file* scambiati non consentono un concreto ristoro del danno patito (16). L'obiettivo delle *major* è pertanto quello di ingenerare il timore di possibili azioni legali, essendo in ciò agevolate dalla natura « dilettantistica »

right, senza predisporre alcun dispositivo in grado di limitarne l'uso illecito; a ciò si aggiunga che i distributori traevano anche un vantaggio economico dalle inserzioni pubblicitarie connesse al *software* direttamente correlato alla frequenza dell'uso del programma medesimo.

(14) Cfr. a titolo d'esempio: *Twentieth Century Fox Film Corporation et al. v. Does 1-12* (N.D. California, 3:2004cv04862); *Universal City Studios Productions LLLP v. Does 1-8* (N.D. Georgia, 1:2004cv03343); *Universal City Studios Productions LLLP v. Does 1-53* (S.D. New York, 1:2004cv09000); *Metro-Goldwyn-Mayer Pictures Inc. v. Does 1-10* (Washington, D.C., 1:2004cv02005); *Twentieth Century Fox Film Corporation v. Does 1-9* (Washington, D.C., 1:2004cv02006); *Columbia Pictures Industries, Inc. v. Does 1-14* (D. Colorado, 1:2004cv02368); *Disney Enterprises, Inc. v. Does 1-19* (N.D. Georgia, 1:2004cv03344); *Paramount Pictures Corporation v. Does 1-19* (N.D. Georgia, 1:2004cv03345); *Warner Bros. Entertainment Inc. v. Does 1-8* (D. Colorado, 1:2004cv02369). Le pronunce ora richiamate sono pubblicate sul sito *http://w2.eff.org*. Tra le più recenti pronunce di condanna di singoli utenti responsabili di scambi di materiale protetto da diritto d'autore attraverso le reti *peer to peer*, si veda *Capitol Records Inc. et al. v. Jammie Thomas* (Minnesota, 06cv1497), in *www.morelaw.com* ed altresì riassunta in *Dir. internet*, 2007, p. 609. Non assume invece rilevanza la posizione delle società di telecomunicazioni, sulle cui reti transitano i pacchetti di dati gestiti dai programmi *peer to peer*, in virtù delle limitazioni di responsabilità derivanti dagli artt. 12 e 15 della direttiva n. 31 Ce del 2000 (attuata in Italia con il d.lgs. n. 70 del 2003) e dal U.S.C. § 512 statunitense.

(15) Cfr. *infra* nota 74.

(16) Con riferimento alle stime dell'entità del fenomeno di *file-sharing* illegale attraverso le reti *peer to peer* non è possibile disporre di dati certi in ragione delle varietà dei contenuti scambiati e della difficoltà di un monitoraggio accurato, tuttavia la Federazione contro la pirateria, sul sito *www.fimi.it*, quantifica in 10 milioni gli utenti attivi nello stesso momento, in 1,5 miliardi di brani disponibili ed in 20 miliardi di brani scaricati (dati 2005). Stime più recenti indicano in 5 miliardi i *download* mensili posti in essere sulle reti *peer to peer*, con un rapporto fra i *file* legalmente scaricati e quelli illegalmente scaricati calcolato in 1 a 40, cfr. *Universal Backs Free Music Offer*, BBC News, 29 agosto 2006, pubblicato sul sito *http://news.bbc.co.uk*.

degli autori degli illeciti, che raramente sono criminali operanti nel settore della pirateria digitale, ma ben più frequentemente comuni individui che trovano « più economico » fruire gratuitamente delle opere digitali o che attraverso i sistemi di *file-sharing* riescono a meglio personalizzare le proprie raccolte musicali superando i limiti propri del mercato discografico (17).

Quest'ultima strategia, della cui efficacia si dirà nel paragrafo conclusivo del presente lavoro, è stata poi adottata anche dai titolari di diritti d'autore in Europa e, per quanto qui interessa, in Italia (18).

2. — Perché l'azione repressiva ai danni degli utenti dei sistemi *peer to peer* possa aver effetto è condizione preliminare e necessaria l'individuazione dei medesimi.

Dal punto di vista informatico nel caso delle comunicazioni *peer to peer*, a differenza di quanto accade laddove la maggior esperienza degli autori degli illeciti costringe a confrontarsi con l'impiego di tecniche volte a cancellare le tracce dell'attività *on-line*, è possibile individuare i terminali utilizzati per lo scambio dei dati semplicemente inserendosi nella rete *peer to peer* alla stregua di un qualsiasi utente (19). In tal maniera, scambiando dati con gli altri *peer* si riescono ad acquisire sia i parametri utili ad identificare gli elaboratori connessi, ovvero l'indirizzo *IP* (20) ed il codice *GUID* (21), che i dati di traffico relativi alle operazioni di *file-sharing* poste in essere, quali il nome del *file*, il valore *hash* (22), nonché la data e l'ora di connessione (23).

(17) Cfr. in proposito ELECTRONIC FRONTIER FOUNDATION, *RIAA v. The People: Four Years Later*, agosto 2007, p. 14 s., pubblicato sul sito *www.eff.org*. I limiti maggiormente avvertiti in relazione al sistema tradizionale di distribuzione utilizzato dalle case discografiche risiedono da un lato nell'indisponibilità dei brani a distanza di un certo tempo dalla loro prima pubblicazione e d'altro canto nella predeterminazione dei brani contenuti nelle singole *compilation*.

(18) Cfr. Trib. Roma, (ord.) 16 luglio 2007, in *Dir. ind.*, 2007, p. 592 ss.; Trib. Roma, (ord.) 14 luglio 2007, in *Dir. ind.*, 2007, p. 588 ss.; Trib. Roma, (ord.) 9 febbraio 2007, in *Dir. internet*, 2007, p. 461 ss.; Trib. Roma, 19 agosto 2006, in *Dir. ind.*, 2007, p. 592 ss.

(19) Cfr. Trib. Roma, (ord.) 16 luglio 2007, cit., p. 586 e Trib. Roma, (ord.) 14 luglio 2007, cit., p. 589.

(20) L'indirizzo *IP* è un numero che identifica univocamente i dispositivi collegati all'interno di una rete informatica che impiega lo *standard Internet Protocol*. Esso può essere statico, se non subisce mai variazioni, o dinamico. Solitamente l'indirizzo *IP* di un computer collegato in rete è dinamico, poiché in tal modo chi offre la connessione, disponendo di un numero limitato di indirizzi, è in grado di fornire il servizio a più utenti.

(21) Il codice *GUID (Globally Unique Identifier)* è un codice numerico identificativo generato al momento dell'installazione del *client* per la rete *peer to peer*, ossia del *software* impiegato per le operazioni di *file-sharing*.

(22) La funzione di *hash* consente di derivare dall'insieme dei *bit* che formano un *file* una stringa di *bit* di lunghezza predefinita, fornendo così un identificatore univoco (*checksum* crittografico) di ciascun *file* condiviso mediante la rete *peer to peer*. Poiché tale funzione dipende unicamente dal contenuto dei *file*, essa permette di individuare *file* identici seppure indicati con nomi diversi e, viceversa, di distinguere *file* diversi presen-

Le informazioni così raccolte non sono tuttavia sufficienti per superare la barriera dell'elaboratore e conoscere chi si trova al di là del *monitor* o, quantomeno, trarre indizi sulla sua identità. Per raggiungere questo obiettivo è infatti necessario abbinare le stesse con i dati di traffico che sono nella disponibilità dei gestori dei servizi di telecomunicazione (24). Ma proprio quest'ultimo passo nell'individuazione dei responsabili ha dato luogo ad un significativo contenzioso, poiché le società interpellate si sono rifiutate di comunicare le informazioni relative agli utenti.

In realtà l'intera procedura mostra in maniera evidente il conflitto che viene a crearsi fra i contrapposti interessi della tutela del diritto d'autore e della protezione della vita privata, a cominciare dall'acquisizione dei dati da parte di chi effettua il controllo sull'attività dei computer collegati ad una rete *peer to peer* con finalità ignote agli utenti della stessa (25).

In generale si pone dunque il problema di stabilire quando un diverso e confliggente interesse possa prevalere sulla tutela del riserbo. L'assenza di una linea di confine trasformerebbe infatti le banche dati dei gestori delle comunicazioni in una risorsa di libero accesso cui attingere per la tutela di interessi privati in sede civile, ingenerando uno stato di continua potenziale sorveglianza sull'attività *on-line* incompatibile con la libertà individuale. L'affermazione dell'opposto indirizzo, tipico di qualsiasi società democratica, secondo cui la vita privata va tutelata da eventuali intromissioni, comporta invece l'eccezionalità dei casi di deroga e, conseguentemente, la particolare rilevanza delle cause che ne costituiscono giustificazione (26).

Al riguardo il punto di equilibrio è stato individuato dallo stesso legislatore mediante le disposizioni contenute nel d.lgs. n. 196 del 2003 che disciplinano le modalità di trattamento, conservazione e comunicazione dei dati personali. Sono state dunque tali norme a costituire oggetto della riflessione dei giudici che si sono pronunciati sulle richieste di accesso avanzate ai sensi dell'art. 156-*bis*, l. n. 633 del 1941 (in séguito l.d.a.) (27) dai titolari dei diritti di utilizzazione economica delle opere protette da diritto d'autore (28).

tati con nomi uguali. Cfr. voce *Hash*, in *Wikipedia, l'enciclopedia libera*, *www.wikipedia.it*.

(23) Cfr. in proposito Trib. Roma, (ord.) 16 luglio 2007, cit., p. 585 s. e Trib. Roma, 19 agosto 2006, cit., p. 594.

(24) I gestori dei servizi di connessione ad *internet* conservano infatti traccia dell'ora di inizio e di fine della connessione, nonché dell'indirizzo *IP* attribuito e del numero chiamante, di cui conoscono il soggetto al quale spetta la titolarità dell'utenza.

(25) Va poi aggiunto che la natura dei *file* oggetto di scambio potrebbe essere idonea a rivelare particolari inerenti la vita privata degli utenti, una volta che questi venissero identificati grazie all'accesso ai dati di traffico detenuti dai gestori delle comunicazioni.

(26) In proposito cfr. anche Corte cost., 14 novembre 2006, n. 372, in *Dir. internet*, 2007, p. 237 ss.

(27) Cfr. Trib. Roma, (ord.) 16 luglio 2007, cit., p. 592 ss.; Trib. Roma, (ord.) 14 luglio 2007, cit., p. 588 ss.; Trib. Roma, (ord.) 9 febbraio 2007, cit., p. 461 ss.; Trib. Roma, 19 agosto 2006, cit., p. 592 ss. Nello specifico l'art. 156-*bis* l.d.a. consente di

Inizialmente l'orientamento della giurisprudenza italiana è stato favorevole alla comunicazione dei dati personali relativi agli utenti da parte dei gestori dei servizi di rete, in virtù del disposto dell'art. 24, comma 1°, lett. *f*), d.lgs. n. 196 del 2003 (29). Più di recente si sono invece avute pronunce di segno opposto in cui si afferma che la tutela di interessi civili, quali quelli rappresentati dal diritto di sfruttamento economico delle opere d'ingegno, non consente di derogare ai limiti posti alla conservazione ed alla comunicazione dei dati personali dal d.lgs. n. 196 del 2003 (30).

Delle due soluzioni emerse dalle decisioni dei giudici è tuttavia l'ultima a risultare coerente non solo con il dettato del d.lgs. n. 196 del 2003, ma anche con i più generali princìpi costituzionali posti a tutela del riserbo della vita e delle comunicazioni private e per questo va condivisa (31).

Va inoltre osservato come occorra interrogarsi non solo sulla legittimità della comunicazione dei dati *ex* art. 156-*bis* l.d.a. (e sulla correlata possibilità per i fornitori dei servizi di comunicazione di conservare i dati di traffico al fine di renderli disponibili a chi intenda agire in sede civile a tutela dei propri diritti), ma sia altresì opportuno valutare la correttezza dell'attività antecedente a tali richieste, ovvero il monitoraggio del traffico *on-line* posto in essere dalle società informatiche su incarico dei titolari dei diritti di sfruttamento economico sulle opere d'ingegno.

Dal momento che l'analisi del traffico risulta essere prodromica alla richiesta di comunicazione dei dati, si inizierà la disamina dei diversi profili ora indicati a partire da quest'ultimo aspetto, peraltro anche oggetto di una recente pronuncia del Garante per la protezione dei dati personali (32).

chiedere al giudice di « ordin[are] alla controparte di fornire gli elementi per l'identificazione dei soggetti implicati nella produzione e distribuzione dei prodotti o dei servizi che costituiscono violazione dei diritti di cui alla presente legge ».

(28) Va in proposito osservato che l'art. 156-*bis* l.d.a. viene invocato dai soggetti lesi ritenendo che l'àmbito di operatività della norma si estenda a comprendere anche quanti, pur non rappresentando tecnicamente la « controparte » di chi ha subìto la lesione, risultino, anche indirettamente, responsabili della violazione dei diritti di proprietà intellettuale. Tale interpretazione è stata confermata dalla giurisprudenza; cfr. in tal senso Trib. Roma, (ord.) 9 febbraio 2007, cit., p. 461, ove si afferma che « la locuzione ''controparte'' indicata dalla norma può trovare una *ratio* coerente col sistema di origine comunitaria solo estendendo anche a soggetti diversi dagli autori della violazione l'obbligo di comunicare i dati in loro possesso al soggetto leso nel diritto intellettuale ». Cfr. altresì Trib. Roma, 19 agosto 2006, cit., p. 595 e, più ampiamente, Trib. Roma, 1° marzo 2007, pubblicata sul sito *www.logistepac.com.*

(29) Cfr. Trib. Roma, (ord.) 9 febbraio 2007, cit., e Trib. Roma, 19 agosto 2006, cit. Nella specie ai gestori dei servizi di rete è stato chiesto di fornire i nominativi dei soggetti connessi individuabili sulla base dei dati di traffico raccolti dagli attori attraverso il monitoraggio delle attività di *file-sharing* (ovvero i già richiamati indirizzi *IP* e codici *GUID*, nonché i nomi dei *file* scambiati, i valori *hash*, le date e gli orari di connessione).

(30) Cfr. Trib. Roma, (ord.) 16 luglio 2007, cit., e Trib. Roma, (ord.) 14 luglio 2007, cit. A tale mutamento di indirizzo ha certamente concorso l'intervento in giudizio del Garante per la protezione dei dati personali, il quale ha offerto argomenti persuasivi nel senso di ritenere illecito il trattamento dati posto in essere.

(31) Cfr. a riguardo Trib. Roma, (ord.) 14 luglio 2007, cit., p. 591.

(32) Cfr. Gar., 28 febbraio 2008, doc. web n. 1495246; il presente documento,

In proposito va innanzitutto constatato come i riferimenti informatici « catturati » dai *software* di monitoraggio, benché non pertinenti a soggetti « identificati », risultino pur sempre riferiti a soggetti « identificabili » (33), proprio in virtù della possibilità di incrociare tali informazioni con quelle in possesso dei gestori delle comunicazioni, e pertanto rientrino pienamente nel campo di applicazione del d.lgs. n. 196 del 2003. Si deve quindi escludere la possibilità di evocare la nozione di « consenso implicito » (34) per legittimare la raccolta di simili informazioni da parte delle società di monitoraggio, posto che una tale soluzione interpretativa, cui si è fatto più volte ricorso in giurisprudenza in relazione ad atti dispositivi di diritti della personalità, è stata esplicitamente rifiutata dal legislatore nel caso del trattamento di dati personali. La disciplina in materia, al fine di garantire un'effettiva tutela del diritto all'autodeterminazione informativa, richiede infatti « il consenso espresso dell'interessato » (35).

Incidentalmente va poi osservato che la manifestazione di un consenso implicito presuppone comunque la consapevolezza dell'atto dispositivo da parte di chi agisce, mentre nei casi di specie la raccolta dei dati per finalità contenziose è avvenuta in maniera occulta (36); né si può ritenere, come invece è stato fatto da alcune corti (37), che qualsiasi attività che comporti la conoscibilità, anche indiretta (38), di informazioni attraverso una rete pubblica esprima per ciò stesso la volontà dell'interessato di permettere a chiunque di trattare liberamente dette informazioni (39).

Il monitoraggio del traffico telematico può tuttavia avvenire a prescindere dal consenso degli utenti della rete *peer to peer* ove sussistano le con-

come tutti i provvedimenti adottati dall'autorità garante successivamente citati, sono pubblicati sul sito ufficiale del Garante per la protezione dei dati personali all'indirizzo *www.garanteprivacy.it.*

(33) Cfr. art. 4, comma 1°, lett. *b*), d.lgs. n. 196 del 2003.

(34) Cfr. invece Trib. Roma, 19 agosto 2006, cit., p. 594, ove si afferma che « colui il quale utilizza un programma di *file-sharing* manifesta, per ciò solo, la volontà di accettare che il proprio indirizzo *IP* sia conoscibile da tutti gli altri utenti che utilizzano il medesimo programma ». Cfr. nello stesso senso anche Trib. Roma, 5 maggio 2007 e Trib. Roma, 27 aprile 2007, entrambe pubblicate sul sito *www.logistepac.com.*

(35) Cfr. art. 23, comma 1°, d.lgs. n. 196 del 2003.

(36) Anche a volerlo considerare implicito, il consenso sarebbe dunque non informato, poiché l'utente ignora che i propri dati vengono acquisiti non solo per lo scambio dei *file*, bensì anche con scopi di tutela giudiziaria. Né è possibile invocare l'esonero dall'informativa, di cui all'art. 13, comma 5°, lett. *a*), d.lgs. n. 196 del 2003, per il caso di specie, essendo esclusivamente previsto per l'ipotesi in cui i dati vengano raccolti presso soggetti diversi dall'interessato. Cfr. inoltre a riguardo Trib. Roma, (ord.) 14 luglio 2007, cit., p. 591.

(37) Cfr. in tal senso Trib. Roma, 27 aprile 2007, cit., e Trib. Roma, 19 agosto 2006, cit., p. 594.

(38) Nella specie infatti gli utenti del sistema *peer to peer* non comunicano direttamente ed in maniera espressa i propri dati di riferimento informatico (codici *IP* e *GUID*), bensì questi vengono rilevati automaticamente dal *software* di gestione del sistema e, in maniera analoga, vengono tracciati dal *software* impiegato dalla società di monitoraggio informatico.

(39) Cfr. in tal senso Gar., provvedimento generale, 29 maggio 2003, doc. web n. 29840.

dizioni per l'applicazione degli artt. 24, comma 1°, lett. *f*), e 26, comma 4°, lett. *c*), d.lgs. n. 196 del 2003 (40), ossia quando i dati di traffico, acquisiti « per far valere o difendere un diritto in sede giudiziaria », vengano raccolti direttamente da parte della stessa società che agisce in giudizio a tutela dei propri diritti d'autore o da soggetti diversi di cui la prima a tal fine si avvalga, qualificandoli come responsabili del trattamento (41). Anche in questa ipotesi, affinché l'apprensione dei dati personali possa ritenersi legittima, occorre però che essa non avvenga in maniera occulta e che quindi l'interessato sia informato delle caratteristiche essenziali relative al trattamento, cosa che invece non è avvenuta nei casi in esame, dove le società di monitoraggio hanno raccolto le informazioni sull'attività *on-line* di scambio dei *file* all'insaputa degli utenti delle reti *peer to peer* e per finalità differenti rispetto a quelle (funzionali all'interconnessione) per cui i dati identificativi degli elaboratori connessi vengono comunicati agli altri utenti su tali reti (42).

(40) Pare meno frequente l'ipotesi di acquisizione di dati « idonei a rivelare lo stato di salute e la vita sessuale », rispetto ai quali difficilmente sarebbe possibile superare il limite di cui all'art. 26, comma 4°, lett. *c*), ultimo periodo, d.lgs. n. 196 del 2003; cfr. altresì Gar., Autorizzazione n. 2/2007 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, punto 1.3, doc. web n. 1429775. In generale, con riguardo al trattamento dei dati sensibili, occorrerà poi valutare, a seconda delle specifiche caratteristiche del soggetto cui è affidata l'attività di monitoraggio, se questi possa valersi delle autorizzazioni generali rilasciate dal Garante, ovvero se occorra preliminarmente richiedere una specifica autorizzazione.

(41) A parere di chi scrive, qualora invece la società di monitoraggio assuma le vesti di autonomo titolare del trattamento avente ad oggetto i dati raccolti sulla rete *peer to peer*, non possono più trovare applicazioni le deroghe di cui agli artt. 24 e 26 d.lgs. n. 196 del 2003 richiamate nel testo, poiché colui che agisce in giudizio (il titolare del diritto d'autore) è un soggetto diverso da chi ha effettuato la raccolta dati e consegue gli stessi a séguito di una comunicazione ai sensi dell'art. 4, comma 1°, lett. *l*), d.lgs. n. 196 del 2003. Qualsiasi accertamento sul ruolo assunto, rispetto al trattamento dati, dalle società di monitoraggio è tuttavia assente dalle argomentazioni delle diverse decisioni che sono state pronunciate in senso favorevole alla comunicazione dei dati personali ai titolari dei diritti di sfruttamento economico sulle opere scambiate *on-line*; cfr. in proposito: Trib. Roma, 5 maggio 2007, cit.; Trib. Roma, 27 aprile 2007, cit.; Trib. Roma, 26 aprile 2007, cit.; Trib. Roma, 1° marzo 2007, cit.; Trib. Roma, 9 febbraio 2007, cit.; Trib. Roma, 27 settembre 2006, cit.; Trib. Roma, 19 agosto 2006, cit.

(42) Nella specie non possono poi essere invocate le ipotesi di deroga alla preventiva informativa di cui ai commi 2° e 5° dell'art. 13, d.lgs. n. 196 del 2003, poiché i dati sono stati raccolti da soggetti privati direttamente presso gli interessati. Cfr. Gar., 7 giugno 2006, doc. web n. 1322812, e Gar., 19 febbraio 2002, doc. web n. 1064177 e n. 1063652, e, in dottrina, MARTONI, *Il trattamento per finalità investigative*, in *Il codice in materia di protezione dei dati personali*, a cura di Monducci e Sartor, Padova, 2004, p. 423. Con riguardo al recente caso di raccolta dei dati di traffico al fine di contrastare lo scambio di *file on-line*, su cui si è pronunciato Gar., 28 febbraio 2008, doc. web n. 1495246, cit., è stato rilevato come, in ragione delle specifiche tecniche del *software* impiegato, « mentre gli indirizzi *IP* sono stati acquisiti da un terzo rispetto agli utenti (il *tracker*), gli altri dati (ossia, i *file* offerti in condivisione, data e ora del *download*) sono stati raccolti direttamente presso gli interessati ». Nella fattispecie in questione dunque, con riguardo alla prima categoria di dati, avrebbe potuto trovare applicazione l'art. 13, comma 5°, lett. *b*), d.lgs. n. 196 del 2003, sempre che la società che ha effettuato

Da ultimo va riscontrato come l'attività di sorveglianza posta in essere violi anche l'art. 37, comma 1°, lett. *d*), d.lgs. n. 196 del 2003, ai sensi del quale ogniqualvolta il trattamento dei dati è finalizzato « a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti » occorre procedere alla preventiva notificazione del trattamento all'autorità garante (43).

Le considerazioni ora espresse portano a concludere che l'attività, preliminare alla richiesta di comunicazione dei dati detenuti dalle compagnie telefoniche, volta all'individuazione delle connessioni mediante le quali sono stati posti in essere atti illeciti, risulta già di per sé vietata e che conseguentemente i dati così raccolti sono inutilizzabili ai sensi dell'art. 11, comma 2°, d.lgs. n. 196 del 2003.

Venendo in tal maniera a mancare gli elementi probatori su cui fondare qualunque pretesa *ex* art. 156-*bis* l.d.a., perde rilievo la disamina dell'ulteriore profilo inerente la possibilità per i gestori dei servizi di comunicazione di conservare e comunicare i dati in loro possesso onde consentire a terzi un'azione in sede civile contro gli autori delle violazioni del diritto d'autore. Pur tuttavia, per completezza di trattazione, si darà conto di come, anche con riguardo a tali diversi aspetti, le disposizioni vigenti in materia di dati personali ostino comunque all'applicazione dell'art. 156-*bis* l.d.a.

Qualora infatti si prescinda dall'illiceità del monitoraggio del traffico *on-line* posto in essere, risulta in ogni caso illecita la comunicazione dei dati personali da parte del gestore della rete al terzo che ritenga di essere stato leso, non potendosi invocare l'art. 24, comma 1°, lett. *f*), d.lgs. n. 196 del 2003, come invece è stato fatto dalle corti (44), per legittimare l'acquisizione dei dati di traffico provenienti dalle società di telecomunicazione, in quanto necessaria per far valere o difendere un diritto in sede giudiziaria.

Due sono infatti le ipotesi in astratto possibili: la richiesta dei dati di traffico rivolta direttamente alla società di telecomunicazione da parte del soggetto che ritiene lesi i propri diritti e la domanda al giudice *ex* art. 156-*bis* l.d.a.

il monitoraggio fosse qualificata come responsabile del trattamento da parte del soggetto che le ha affidato tale incarico a tutela dei propri diritti, altrimenti avrebbe dovuto trovare applicazione il comma 4° della norma citata.

(43) Cfr. Trib. Roma, (ord.) 14 luglio 2007, cit., p. 591. Nella decisione Gar., 28 febbraio 2008, doc. web n. 1495246, cit., l'attività di monitoraggio degli utenti della rete *peer to peer* è stata inoltre considerata atta a violare l'art. 122, d.lgs. n. 196 del 2003; tuttavia, ai sensi dell'art. 121 della medesima normativa, il divieto di « monitorare le operazioni dell'utente » previsto dalla norma successiva pare rivolto solamente a chi fornisce servizi di comunicazione elettronica piuttosto che a chiunque operi sulle reti informatiche, ragion per cui ove non si tratti di soggetti non rientranti nella prima categoria troveranno applicazione le disposizioni generali citate nel testo.

(44) Cfr. in tal senso: Trib. Roma, 2 maggio 2007, pubblicata sul sito *www.logistepac.com*; Trib. Roma, (ord.) 9 febbraio 2007, cit., p. 462; Trib. Roma, 19 agosto 2006, cit., p. 595.

Nel primo caso, che non pare essersi verificato nelle fattispecie poste all'esame delle corti, l'art. 24 d.lgs. n. 196 del 2003 non può trovare applicazione poiché i dati personali non sono acquisiti direttamente presso l'interessato da parte di chi intende far valere il proprio diritto in giudizio (45), bensì vengono conseguiti mediante una comunicazione (46) proveniente da un terzo (il gestore dei servizi di rete) da ritenersi illecita in assenza di un esplicito consenso informato, espresso dagli utenti, che abiliti la società di telecomunicazioni a tale divulgazione (47).

Nel secondo caso dovrebbe invece trovare sì applicazione l'art. 24 d.lgs. n. 196 del 2003, ma la lettera *a*) del comma 1°, laddove si stabilisce che il consenso non occorre quando il trattamento « è necessario per adempiere ad un obbligo previsto dalla legge »; in particolare proprio la norma della legge sul diritto d'autore configurerebbe un preciso obbligo di comunicazione in capo al gestore della rete in favore del soggetto agente. Legittimata in tal maniera l'attività di comunicazione, il titolare dei diritti d'autore potrebbe allora invocare l'art. 24, comma 1°, lettera *f*) (48), onde escludere la necessità dell'acquisizione del consenso, unitamente all'art. 13, comma 5°, lett. *b*), che farebbe venir meno anche l'obbligo di fornire la relativa informativa (49). A questo punto però diviene centrale nell'argomentazione la legittimità della conservazione dei dati di traffico da parte dei gestori delle reti per finalità diverse da quelle di cui al combinato disposto degli artt. 123 e 132 d.lgs. n. 196 del 2003.

(45) Non pare sostenibile un'interpretazione dell'art. 24, comma 1°, lett. *f*), d.lgs. n. 196 del 2003, nel senso di escludere il consenso anche nell'ipotesi in cui il trattamento (in questo caso comunicazione) dei dati sia volto a consentire ad un terzo di « far valere o difendere un diritto in sede giudiziaria ». La *ratio* dell'art. 24, e la stessa previsione nell'àmbito della lettera *f*) di tale articolo anche dell'ipotesi di deroga riguardante lo svolgimento di investigazioni difensive, portano infatti a ritenere che l'azione in giudizio presa in considerazione sia solamente quella posta in essere direttamente dall'autore del trattamento.

(46) Cfr. art. 4, comma 1°, lett. *l*), d.lgs. n. 196 del 2003.

(47) Ne consegue che i dati eventualmente ottenuti in séguito alla comunicazione proveniente dalla società di telecomunicazione saranno inutilizzabili ai sensi dell'art. 11, comma 2°, d.lgs. n. 196 del 2003.

(48) Confonde invece i due diversi profili Trib. Roma, (ord.) 9 febbraio 2007, cit., p. 462, ove si afferma che « nemmeno può ravvisarsi un impedimento all'ostensibilità [*rectius* comunicazione] dei dati in questione per la protezione dei dati personali di cui all'art. 24, d. lgs. n. 196/2003, considerato che tale disciplina normativa fa salva la possibilità di utilizzazione di tali dati, anche senza il consenso del titolare, nel caso di utilizzazione per ragione di tutela giurisdizionale ». Analogo errore logico si ravvisa anche nelle precedenti pronunce Trib. Roma, 1° marzo 2007, cit., e Trib. Roma, 27 settembre 2006, pubblicata sul sito *www.logistepac.com*, e Trib. Roma, 19 agosto 2006, cit., p. 595.

(49) Va in proposito rimarcato come l'esclusione dell'informativa valga però solo per i dati provenienti dalla società di telecomunicazioni (ovvero i nominativi dei soggetti che si sono connessi alla rete *peer to peer*) e non per la diversa categoria di informazioni raccolte direttamente dalle società di monitoraggio sulla rete *peer to peer* nell'interesse dei soggetti i cui diritti d'autore sono stati pregiudicati, delle quali si è detto in precedenza.

Presupposto dell'accesso ai dati di traffico è infatti la loro conservazione nel tempo; al riguardo l'art. 123, comma 1°, d.lgs. n. 196 del 2003 prevede in generale che tali dati vengono « cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica », con le sole eccezioni, di cui ai commi successivi, inerenti le finalità di fatturazione, di documentazione in caso di contestazione della fattura o per la pretesa del pagamento e di commercializzazione di servizi di comunicazione elettronica o di fornitura di servizi a valore aggiunto. Tempi più ampi di conservazione dei dati di traffico sono poi previsti in via eccezionale dal successivo art. 132, per l'accertamento e la repressione di reati.

Dal quadro normativo si evince dunque come non vi sia la possibilità di conservare le informazioni inerenti il traffico telematico allo scopo di consentire a terzi di fruire delle medesime per tutelare i propri diritti in sede civile ([50]).

In sintesi, alla luce delle considerazioni svolte, è dunque possibile trarre le seguenti conclusioni:

— il monitoraggio da parte di soggetti privati dell'attività posta in essere dagli utenti di una rete *peer to peer* all'insaputa degli stessi è illecito in quanto contrastante con il d.lgs. n. 196 del 2003;

— i dati così acquisiti non sono pertanto utilizzabili per offrire elementi sulla base dei quali, ai sensi dell'art. 156-*bis* l.d.a., il giudice possa ordinare al gestore della rete di comunicazione di fornire i dati necessari per l'identificazione dei soggetti implicati nella produzione e distribuzione dei prodotti o dei servizi in violazione dei diritti d'autore;

— in ogni caso la conservazione dei dati di traffico da parte del gestore del servizio di comunicazione non potrebbe comunque essere finalizzata a dare conoscenza a terzi di tali dati, onde consentire loro di avanzare pretese in sede civile.

3. — In relazione alle precedenti conclusioni va ora valutata l'incidenza delle aperture recentemente manifestate dalla Corte di giustizia delle Comunità europee ([51]), volte *in primis* a legittimare la conservazione dei dati di traffico anche per finalità di tutela dei diritti — nello specifico sulle opere d'ingegno — in sede civile e, implicitamente, ad ammettere l'acquisizione di tali dati attraverso attività di monitoraggio occulto poste in essere da soggetti privati.

([50]) Cfr. Trib. Roma, (ord.) 16 luglio 2007, cit., p. 587.

([51]) Cfr. Corte di giustizia delle Comunità europee, 29 gennaio 2008, causa C-275/06 - *Productores de Música de España (Promusicae) - Telefónica de España SAU*, in *Giur. it.*, 2008, p. 1419 ss. La decisione ha per oggetto la questione pregiudiziale riguardante la conformità al diritto comunitario della scelta di uno Stato membro di limitare ai soli àmbiti delle indagini penali, della tutela della pubblica sicurezza e della difesa nazionale, l'obbligo di conservazione e comunicazione dei dati di connessione e di traffico incombente sui gestori dei servizi di comunicazione di rete.

In particolare, secondo i giudici della Corte, l'art. 15, § 1°, direttiva n. 2002/58/Ce attribuisce agli Stati membri la possibilità di prevedere la conservazione dei dati personali da parte dei fornitori di una rete pubblica o di un servizio pubblico di comunicazione elettronica anche al fine di renderli disponibili nel contesto di un'azione civile, benché, in assenza di alcun obbligo derivante dal diritto comunitario che imponga agli Stati di attivarsi in tal senso, si debba ritenere lasciata alla discrezionalità dei legislatori nazionali la scelta dell'eventuale ampliamento delle finalità giustificanti la *data retention*. Ampliamento che in ogni caso dovrebbe avvenire in maniera da garantire il « giusto equilibrio » fra le esigenze di tutela del diritto d'autore e quelle di tutela dei dati personali ([52]).

L'intero ragionamento della Corte è incentrato sull'interpretazione del citato art. 15, con riferimento al rilievo assunto dal richiamo ivi presente all'art. 13, § 1°, direttiva n. 95/46/Ce ([53]). Secondo i giudici proprio questo inciso permetterebbe infatti di favorire la *data retention* attraverso l'estensione della possibilità di limitare le garanzie relative alla riservatezza delle comunicazioni e dei dati di traffico, di cui agli artt. 5 e 6 direttiva n. 2002/58/Ce ([54]), anche al di là delle ipotesi espressamente menzionate di « salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica » e di « prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica ». In particolare sarebbe possibile comprendere anche tutti i casi previsti dall'art. 13, § 1°, direttiva n. 95/46/Ce, benché non esplicitamente richiamati.

Con specifico riferimento alla tutela dei diritti sulle opere d'ingegno, diverrebbe così consentito « comprimere » il diritto alla riservatezza ove

([52]) Cfr. punti 53, 54, 68, 69 e 70 della decisione della Corte. Le norme eventualmente poste in essere dovranno quindi essere interpretate in modo da non ingenerare conflitti con gli altri diritti fondamentali ed andranno lette alla luce del principio di proporzionalità.

([53]) Il testo dell'art. 15, § 1°, direttiva 2002/58/Ce è il seguente: « Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, § 1, della direttiva n. 95/46/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai princìpi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea ».

([54]) Nella specie, con riguardo al caso concreto sottoposto all'attenzione da parte del giudice del rinvio, vengono in particolar rilievo da un lato il divieto di intercettazione e di sorveglianza delle comunicazioni di cui all'art. 5, § 1°, direttiva n. 2002/58/Ce, e dall'altro l'obbligo di cancellazione o di trasformazione in forma anonima dei dati di traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal gestore della rete telematica, di cui al successivo art. 6, § 1°.

ciò si rendesse necessario per la protezione « dei diritti e delle libertà altrui », ai sensi dell'art. 13, § 1°, lett. *g*), direttiva n. 95/46/Ce (55).

Tale argomentazione non pare tuttavia coerente con il dato testuale dell'art. 15 direttiva n. 2002/58/Ce, laddove la locuzione « ai sensi dell'art. 13, § 1°, della direttiva n. 95/46/Ce » ha come unica finalità quella di indicare il fondamento normativo della « restrizione » eventualmente apponibile ai diritti riconosciuti dalla direttiva n. 2002/58/Ce, attraverso il richiamo alla disposizione che, nella direttiva in cui si delineano i princìpi fondamentali in materia di trattamento dei dati personali, prevede in via generale la possibilità di limitare la tutela di tali informazioni (56).

La specialità della direttiva in materia di trattamento dei dati personali nel settore delle comunicazioni elettroniche (57), unitamente alla restrizione delle ipotesi espresse di deroga solo ad alcune delle fattispecie menzionate dal più generale art. 13 direttiva n. 95/46/Ce, portano dunque ad escludere ogni interpretazione estensiva dell'art. 15, § 1°, direttiva n. 2002/58/Ce (58).

Venendo così meno la possibilità di ampliare il dettato dell'art. 15 (59), si deve concludere che scarso valore assume la previsione contenuta in altre direttive comunitarie circa la possibilità di adottare strumenti giuridici volti alla tutela del diritto d'autore che comportino una limitazione delle garanzie di riservatezza riconosciute dall'ordinamento comunitario nelle comunicazioni elettroniche, posto che le direttive in questione fanno in ogni caso salve le disposizioni sul trattamento dei dati personali (60).

Occorre tuttavia constatare come, sebbene le argomentazioni della Corte di giustizia paiano criticabili sotto il profilo argomentativo, debba

(55) Cfr. punto 53 della decisione della Corte.

(56) Conferme in tal senso derivano altresì dal testo francese della direttiva, in cui figura la locuzione « comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE », nonché da quello in lingua inglese (« as referred to in Article 13(1) of Directive 95/46/EC ») e da quello in lingua spagnola (« a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE »). Cfr. a riguardo anche le Conclusioni dell'avvocato generale J. Kokott, presentate il 18 luglio 2007, punto 87, pubblicate sul sito ufficiale della Corte di giustizia delle Comunità europee *www.curia.europa.eu.*

(57) Cfr. 4° considerando direttiva 2002/58/Ce ed ora anche 2° considerando direttiva 2006/24/Ce.

(58) Cfr. a riguardo le Conclusioni dell'avvocato generale J. Kokott, cit., punto 86, nonché il 10° considerando della direttiva n. 2002/58/Ce. La lettura dell'art. 15 effettuata dalla Corte è altresì contraddetta dall'11° considerando della direttiva 2002/58/Ce, ove nell'indicare le ragioni a fondamento dei « provvedimenti » di cui al successivo art. 15 non viene fatta menzione alcuna alle esigenze di tutela dei diritti, né viene richiamato l'art. 13 direttiva n. 95/46/Ce.

(59) Cfr. altresì a riguardo il 4° considerando della più recente direttiva n. 2006/24/Ce in materia di *data retention*, ove si ribadisce che le finalità di tutela dell'ordine pubblico e di perseguimento dei reati e dell'uso non autorizzato dei sistemi di comunicazione elettronica sono le uniche ad animare le deroghe previste dall'art. 15, § 1°, direttiva n. 2002/58/Ce, contraddicendo così l'interpretazione datane dalla Corte di giustizia.

(60) Cfr. art. 1, § 5, direttiva n. 2000/31/Ce; art. 9, direttiva n. 2001/29/Ce; artt. 2, § 3, e 8, § 3, lett. *e*), direttiva n. 2004/48/Ce.

essere condiviso l'intento che ha animato i giudici, essendo infatti giunto il tempo di prendere piena coscienza di come non sia possibile un'effettiva tutela dei diritti in *internet* senza accettare, entro certi limiti, una parziale compressione del diritto alla riservatezza delle comunicazioni.

Le peculiarità delle reti telematiche, unite alla sofisticata evoluzione dei *software* ed all'abilità di non pochi utenti, rendono ormai impensabile l'individuazione degli autori degli illeciti posti in essere *on-line* prescindendo da un monitoraggio delle comunicazioni. Il problema che si pone non è quindi quello di ammettere o negare tali forme di controllo, bensì piuttosto quello di definire il confine fra la tutela legittima dei propri diritti e l'indebita intrusione o, peggio, la schedatura di massa.

Al riguardo la soluzione non può essere quella di cui all'art. 15, § 1°, direttiva n. 2002/58/Ce ed all'art. 132 d.lgs. n. 196 del 2003, consistente nell'individuare nella sussistenza di una fattispecie penale la giusta causa per consentire la conservazione e la comunicazione dei dati di traffico, laddove la semplice introduzione di una sanzione penale, ancorché minima, comporterebbe un mutamento del regime di trattamento dei dati. Pare invece più opportuno sostituire un approccio formalistico basato solamente sulla natura della tutela (civile o penale) offerta, con un più ponderato e pertinente giudizio incentrato sul rapporto fra gli interessi contrastanti. In questo senso va condivisa la posizione assunta dalla Corte di giustizia delle Comunità europee che in sostanza rimette al legislatore nazionale, qualora questi lo ritenga opportuno, il compito di fissare il punto di equilibrio fra le opposte esigenze della difesa della proprietà intellettuale e della protezione dei dati personali, a prescindere dal rilievo penale delle fattispecie considerate.

Con riferimento all'ordinamento italiano, va poi precisato che le previsioni di reato di cui agli artt. 171, comma 1°, lett. *a-bis*) (61) e 171-*ter*, comma 2°, lett. *a-bis*) (62), l.d.a., semplificano solo parzialmente la soluzione del problema, in quanto riguardano unicamente l'*upload* di opere protette dal diritto d'autore, mentre non puniscono il comportamento di chi, pur connesso ad una rete *peer to peer*, si limiti a scaricare i *file* (63),

(61) L'efficacia deterrente dell'art. 171, comma 1°, lett. *a-bis*), l.d.a. risiede nel punire la semplice messa a disposizione del materiale protetto dal diritto d'autore, a prescindere dall'effettiva utilizzazione dello stesso da parte di terzi o dalla sua diffusione, superando dunque i limiti che invece sono emersi in relazione alla normativa statunitense nella recente pronuncia, emessa in sede di procedimento cautelare, sul caso *Atlantic Recording Corporation, et al. v. Pamela and Jeffrey Howell* (Arizona, cv06-02076-PHX-NVW) pubblicata in *www.eff.org*, ove il giudice, in relazione ad una fattispecie di *upload* di *file* musicali resi accessibili attraverso il sistema di *file-sharing* denominato KaZaA, ha ritenuto che « an offer to distribute does not constitute distribution ».

(62) L'art. 171-*ter*, comma 2°, lett. *a-bis*), l.d.a. richiede tuttavia la sussistenza del dolo specifico consistente nel « fine di lucro », non sempre ravvisabile nei casi in considerazione, come rilevato in Cass. pen., sez. III, 9 gennaio 2007, n. 149, in *Riv. dir. ind.*, 2007, II, p. 77 ss., con nota di Franceschelli, ed in *Dir. internet*, 2007, p. 258 s.; cfr. altresì Chimenti, *La nuova proprietà intellettuale nella società dell'informazione. La disciplina europea e italiana*, Milano, 2005, p. 186 s.

(63) Va tuttavia osservato che le medesime reti, al fine di ostacolare comporta-

dando luogo ad un comportamento che non assume rilevanza di reato ed è solamente soggetto alla sanzione amministrativa di cui al seguente art. 174-*ter*, comma 1° (64).

A ciò si aggiunga che il combinato disposto dell'art. 171, comma 1°, lett. *a-bis*), l.d.a., o del successivo art. 171-*ter*, comma 2°, lett. *a-bis*), e dell'art. 132 d.lgs. n. 196 del 2003 non è destinato ad operare nelle ipotesi in cui la parte lesa agisca solamente in sede civile, ove le finalità perseguite non sono quelle di « accertamento e repressione di reati » (65), bensì quelle risarcitorie o inibitorie.

Per questi motivi si deve ritenere che avrebbe ragion d'essere uno specifico intervento normativo volto ad estendere la conservazione dei dati di traffico e l'accesso agli stessi anche per finalità di protezione del diritto d'autore di fronte al giudice civile.

Va però rilevato come, anche laddove l'eventuale sussistenza dell'illecito penale o la previsione di una disposizione *ad hoc* consentano di superare gli attuali limiti posti all'acquisizione delle informazioni da parte del gestore della rete di comunicazioni, non viene comunque meno l'illiceità della condotta, necessariamente preliminare a tale richiesta, con cui la società di monitoraggio entra in possesso di dati personali al fine di provare le violazioni del diritto d'autore mediante l'individuazione degli indirizzi informatici verso i quali o dai quali sono stati inoltrati *file*. Questa attività infatti, benché non concretizzi un'ipotesi di intercettazione di comunica-

menti « parassitari » che limiterebbero l'offerta e l'agevole reperimento dei materiali, spingono gli utenti alla condivisione dei *file*, assicurando una maggior velocità di *download* a chi condivide un maggior numero di *file* ovvero richiedendo necessariamente un « conferimento » minimo per accedere agli scambi. Ne consegue che solitamente gli utenti di una rete *peer to peer* compiono attività di *upload* che, in quanto attinenti a materiali protetti dal diritto d'autore, possono senza problema rientrare nell'àmbito di operatività dell'art. 171, comma 1°, lett. *a-bis*), l.d.a. Con riferimento al dettato di tale norma meritano tuttavia considerazione le osservazioni di chi sottolinea come, in ragione delle modalità di comunicazione *peer to peer*, in realtà l'« immissione » dell'opera « in un sistema di reti telematiche » avvenga solamente quando un *peer* ne faccia richiesta ad un altro *peer*, mentre ciò che è « messo a disposizione del pubblico » sia solamente l'indicazione della disponibilità ad inviare alcuni *file* a chi ne faccia domanda. In tal senso la comunicazione *peer to peer* non darebbe mai vita alla fattispecie di cui all'art. 171, comma 1°, lett. *a-bis*), l.d.a., mancando al momento dell'offerta l'immissione dell'opera in rete ed al momento dell'invio dei *file* la comunicazione a soggetti diversi dal solo richiedente degli stessi; cfr. a riguardo FARINA, *Il dolo specifico e la tutela penale del diritto d'autore: il caso della pirateria altruistica* on line, in *Dir. pen. e proc.*, 2007, p. 1029.

(64) L'art. 174-*ter*, comma 1°, l.d.a. prevede la sanzione amministrativa pecuniaria per « chiunque abusivamente utilizza, anche via etere o via cavo, duplica, riproduce, in tutto o in parte, con qualsiasi procedimento, anche avvalendosi di strumenti atti ad eludere le misure tecnologiche di protezione opere o materiali protetti ». Rispetto alla connotazione della condotta derivante dall'avverbio « abusivamente », nel caso di scambio *peer to peer* occorrerà far riferimento al disposto dell'art. 71-*sexies* l.d.a., ravvisandosi nello scambio gratuito un fine « indirettamente commerciale » consistente nel risparmio di spesa derivante dal mancato acquisto. Cfr. in argomento anche FARINA, *op. cit.*, p. 1030 s. e LAVAGNINI, *Riproduzione privata ad uso personale*, in *Commentario breve al diritto della concorrenza*[3], a cura di L.C. Ubertazzi, Padova, 2004, p. 1410.

(65) Cfr. art. 132, commi 1° e 3°, d.lgs. n. 196 del 2003.

zioni elettroniche (66), deve comunque ritenersi illegittima in assenza di una preventiva informativa circa le reali finalità perseguite, quand'anche nell'ipotesi di sussistenza di un illecito penale (67). Proprio in riferimento al monitoraggio per finalità difensive si manifesta dunque evidente la necessità di uno specifico intervento normativo che, circoscrivendo in maniera puntuale la fattispecie, consenta di derogare agli obblighi informativi previsti dal d.lgs. n. 196 del 2003 (68).

4. — Gli scenari che paiono aprirsi in séguito alla decisione della Corte di giustizia sembrano dunque mostrare un rafforzamento degli strumenti volti a perseguire gli autori della divulgazione *on-line* di opere protette dal diritto d'autore. Si tratta di un risultato indubbiamente utile nella lotta alla « pirateria digitale », la cui reale efficacia può però essere apprezzata solamente alla luce del contesto globale di tale fenomeno, di cui vanno analizzate dimensioni e ragioni.

(66) Gli indirizzi informatici necessari per l'instradamento dei dati vengono acquisiti dalla società che effettua il monitoraggio comportandosi semplicemente come un utente della rete, attraverso lo scambio di *file*. È infatti il *software* impiegato per la comunicazione *peer to peer* che rende automaticamente disponibili tali dati.

(67) Ai sensi dell'art. 13, comma 2°, d.lgs. n. 196 del 2003, nel caso di dati raccolti direttamente presso l'interessato, è infatti consentito omettere gli elementi dell'informativa la cui conoscenza può ostacolare l'attività d'indagine solamente nell'ipotesi dell'espletamento « di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati » da parte di un soggetto pubblico. Cfr. altresì Gar., Autorizzazione n. 6/2007 al trattamento dei dati sensibili da parte degli investigatori privati, 28 giugno 2007, doc. web n. 1429963.

(68) In proposito, si potrebbe operare sulla falsariga dell'art. 2, comma 1°, Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica di cui all'Allegato A al d.lgs. n. 196 del 2003, in virtù del quale è consentito al giornalista di omettere qualsiasi informazione circa il trattamento ove ciò « renda altrimenti impossibile l'esercizio della funzione informativa ». Analogamente nel caso di specie si potrebbe evocare l'impossibilità, in costanza di informativa, di perseguire le finalità cui è correlata l'attività di trattamento dati, consistenti nella legittima tutela di un diritto fondamentale. La diversità degli scopi perseguiti, unitamente all'assenza di una specifica professionalità e di organi di categoria di controllo, dovrebbe però comportare per il caso in esame l'esclusione della discrezionalità dell'autore del trattamento circa la scelta di non fornire l'informativa, come è invece previsto dalla norma riguardante l'attività giornalistica, essendo invece auspicabile un dettagliato intervento autorizzatorio di carattere generale da parte del Garante, onde evitare il rischio di eventuali abusi. Tale soluzione pare conforme allo spirito del d.lgs. n. 196 del 2003, laddove all'art. 13, comma 3°, prevede la possibilità per il Garante di definire « modalità semplificate per l'informativa »; nel caso di specie una norma *ad hoc*, in specifiche ipotesi, potrebbe consentire al Garante di autorizzare la totale esclusione dell'informativa preventiva. Cfr. altresì art. 13, comma 2°, sebbene riferito ai soli soggetti pubblici. In ogni caso dovrebbe poi farsi salvo l'obbligo di fornire tempestivamente l'informativa successivamente all'acquisizione dei dati, nel momento in cui tale comunicazione non sia più in grado di pregiudicare l'attività di monitoraggio; ipotesi di informativa successiva all'acquisizione dei dati sono peraltro già previste dal d.lgs. n. 196 del 2003.

In tal senso occorre prendere atto dell'entità decisamente notevole assunta dagli scambi *peer to peer* di contenuti multimediali, cui ha contribuito anche la crescente ampiezza di banda disponibile; secondariamente va constatato come non si sia in presenza di pochi soggetti dediti alla commissione di illeciti per finalità lucrative, bensì di una moltitudine di singoli che agiscono con l'intento di condividere in maniera « altruistica » le proprie risorse musicali. Ad animare gli utenti delle reti di *file-sharing* non è però il solo scopo di risparmiare sui costi di acquisto, ma anche quello di poter scegliere liberamente i brani di proprio interesse, compresi quelli non più distribuiti attraverso i canali commerciali, al di fuori dei prodotti preconfezionati offerti dalle case discografiche, di cui per altro in molti casi non si esclude l'acquisto ([69]).

Va inoltre constatato come dal 2003, anno della « caduta » di Napster, al 2007 i produttori di musica abbiano citato in giudizio, solo negli Stati Uniti, oltre 20.000 cittadini comuni colpevoli di aver immesso in rete per finalità non commerciali contenuti protetti dal diritto d'autore ([70]) e come, sempre negli USA, negli stessi anni il numero di chi scambia materiale soggetto a *copyright* sia passato dai 3/4 milioni di utenti di Napster ([71]) agli attuali oltre 9 milioni ([72]).

([69]) Cfr., con riguardo all'Italia, FONDAZIONE L. EINAUDI, *I comportamenti di consumo di contenuti digitali in Italia. Il caso del* file sharing, 2006, pp. 11 e 43 ss., pubblicato sul sito *www.fondazione-einaudi.it*, ove sulla base di un'indagine campionaria su 1600 utenti di *internet*, effettuata nel maggio 2006, è emerso che « nel complesso l'impatto del *download* sui consumi culturali è stato pressoché identico sia per i *pay* che per i *free* », ovvero per coloro che hanno scaricato da *internet* prevalentemente contenuti a pagamento (*downloader pay*) e per coloro che hanno scaricato da *internet* prevalentemente in modalità gratuita da altri utenti, ovvero tramite *file-sharing* (*downloader free*). Se poi si confrontano i dati inerenti la propensione all'acquisto di CD musicali risulta che i c.d. *downloader free* mediamente ogni mese acquistano più di quanto non facciano coloro che non scaricano in alcun modo musica da *internet*, né a pagamento, né mediante *file-sharing*. È emerso inoltre che attraverso il *file-sharing* si mira prevalentemente (43% dei casi) ad acquisire musica degli ultimi 5 anni, mentre solo nel 30% dei casi vengono scaricati brani corrispondenti alle *hits* del momento e nel 25% dei casi vengono invece cercati brani « storici ». A riprova poi del fatto che il *file-sharing* è, almeno in parte, indotto dall'esigenza di superare il modello commerciale offerto dalle case discografiche incentrato sugli album piuttosto che sui singoli brani, è emerso che « i brani musicali sono sicuramente il prodotto di maggiore successo (91%) rispetto agli album (21%) ». In particolare, con riguardo alle motivazioni che portano al *file-sharing*, si legge che « alla luce della rilevazione, emerge la necessità di riconsiderare l'equazione "*file-sharing*=pirateria", poiché le motivazioni che portano all'uso di queste tecnologie sono da ricercarsi soprattutto nelle mutate esigenze di consumo da parte dei consumatori di contenuti culturali », come dimostrato dal fatto che solo nel 37% dei casi è stato il movente economico (gratuità) a rappresentare la prima ragione dell'uso dei sistemi di *file-sharing*, mentre nei restanti casi hanno prevalso motivi correlati alla fruibilità dei contenuti (possibilità di operare da casa, valutazione preventiva dell'acquisto, ampiezza di scelta e di reperimento di brani non più disponibili, possibilità di condivisione della musica con amici/appassionati).

([70]) Cfr. ELECTRONIC FRONTIER FOUNDATION, *op. cit.*, p. 2.

([71]) Cfr. BALSAMO, *Distribuzione* on-line *di file musicali e violazione del* copyright*: il caso Napster*, in *Riv. dir. aut.*, 2001, p. 58.

([72]) I dati sono stati dedotti dall'analisi dei picchi di utilizzo delle principali reti

Da questi sintetici dati si possono sin da subito trarre due considerazioni. In primo luogo è evidente che, a prescindere dagli strumenti processuali a disposizione, l'intento delle *major* che hanno proposto azioni legali non può essere stato quello di conseguire un ristoro dei danni patiti, stante la sproporzione fra il numero dei convenuti e quello dei soggetti dediti allo scambio di materiale protetto da *copyright*; secondariamente emerge come il ricorso alle vie legali non sembra essere servito ad arginare il fenomeno (73).

Nello specifico l'azione delle *major*, anche in Italia, sembra più che altro finalizzata a dissuadere dalla commissione di illeciti, attraverso la minaccia di un eventuale contenzioso, come dimostrato dalla prassi dell'invio di lettere volte a conseguire una soluzione in via transattiva della controversia, prevedendo in via residuale l'ipotesi di azione in giudizio (74). D'altra parte il fenomeno ha assunto una dimensione così vasta che una concreta repressione dello stesso richiederebbe risorse eccessive per i privati, nel caso di tutela in sede civile, e non disponibili per l'autorità giudiziaria, rispetto all'azione penale (75).

Dell'efficacia di una simile « strategia del terrore » è però lecito dubitare per una serie di ragioni.

Innanzi tutto, a livello generale, come già osservato, depone in senso avverso l'esperienza storica statunitense in materia: Napster è stato fatto chiudere, ma sono nate altre reti più difficili da reprimere (in quanto decentrate), per non parlare dei diversi accorgimenti informatici adottati per ostacolare la tracciabilità degli utenti o l'identificazione degli stessi.

Dubbi sorgono poi anche sulla reale efficacia individuale del ricorso al giudice, laddove non pare affatto sicuro che dall'identificazione, per altro anch'essa non così infallibile (76), di un elaboratore si possa con cer-

peer to peer da parte della società BigChampagne e sono riportati in ELECTRONIC FRONTIER FOUNDATION, *op. cit.*, p. 11 s. Argomenti di segno opposto sono invece addotti nel rapporto IFPI (International of the phonographic industry), in *Digital Music Report 2007*, gennaio 2007, p. 18, disponibile sul sito *www.ifpi.org*, dove si afferma che i risultati di alcune ricerche condotte nei principali mercati europei « suggest that IFPI's campaign against large-scale uploader is having an impact », riferendo però dati evidentemente positivi solo in relazione al mercato tedesco.

(73) Si legge in ELECTRONIC FRONTIER FOUNDATION, *op. cit.*, p. 2: « but as it was winning the legal battles, the recording industry was losing the war. After Napster was shut down, new networks quickly appeared... The number of filesharers, as well as the number of P2P software applications, has kept growing, despite the recording industry's early courtroom victories ».

(74) Sul modello statunitense delle *pre-litigation letter* cfr. ELECTRONIC FRONTIER FOUNDATION, *op. cit.*, p. 4 ss.

(75) Peraltro, in considerazione degli elevati carichi di lavoro che incombono sulle procure italiane e della commissione di ben più gravi reati *on-line*, nonché del numero ridotto degli investigatori della polizia postale, risulta difficile assicurare priorità alla repressione dei reati connessi allo scambio di materiale protetto da diritto d'autore su reti *peer to peer*.

(76) L'attività di monitoraggio delle comunicazioni *peer to peer* alla ricerca degli autori di illeciti commessi a danno dei diritti d'autore non è infatti esente da errori, consistenti soprattutto in falsi positivi.

tezza risalire al soggetto responsabile dell'uso illecito del medesimo. Vale infatti la ricorrente osservazione secondo cui non si potrà mai sapere chi davvero stia al di là del *monitor* (77). Solamente la tecnica giuridica potrebbe offrire dei rimedi volti a semplificare l'onere probatorio, ad esempio ricorrendo a presunzioni o creando vere e proprie ipotesi di responsabilità oggettiva o semi-oggettiva, ma allo stato attuale tali soluzioni non paiono agevolmente percorribili, se non al prezzo di demonizzare gli strumenti d'uso quotidiano, costringendo ciascuno a vigilare sul proprio computer, sul cellulare e su tutti quei dispositivi elettronici — e sono sempre più — in grado di scambiare contenuti attraverso reti di comunicazione (78).

Anche nel caso delle reti *peer to peer* ci si è dunque chiesti se non fosse più agevole lasciare da parte le soluzioni tradizionali incentrate su norme comportamentali per ricorrere, come già si è fatto in altri àmbiti a contenuto tecnologico, a soluzioni basate sulla regolamentazione tecnica. La conformazione delle strutture informatiche o dei contenuti in grado di circolare su di esse secondo *standard* incompatibili, o scarsamente compatibili, con la realizzazione di condotte illecite in violazione delle norme sul diritto d'autore può infatti fornire un'efficace tutela preventiva, riducendo così le ipotesi in cui occorra intervenire successivamente alla commissione dell'illecito sulla base di disposizioni incentrate sul comportamento del soggetto agente.

Una possibile soluzione in tal senso è rappresentata dalle c.d. *Technological Protection Measure* (*TPM*) (79) poste a fondamento dei sistemi di *Digital Rights Management* (*DRM*) (80), mediante i quali è possibile rego-

(77) Un'interpretazione in senso contrario è stata invece avanzata, negli Stati Uniti, nella pronuncia *Capitol Records Inc. et al. v. Jammie Thomas* (Minnesota, 06cv1497), cit., ove si è ritenuto che l'indirizzo *IP* ed il *nickname* utilizzati per l'accesso ad una piattaforma di *peer to peer*, unitamente al *download* di materiale protetto da *copyright* ed al possesso di 24 *file* scaricati attraverso detta piattaforma, costituissero prove sufficienti per fondare una condanna per riproduzione illegale di opere musicali.

(78) Per una più ampia esposizione delle considerazioni a riguardo cfr. volendo MANTELERO, *Attività di impresa in Internet e tutela della persona*, Padova, 2004, p. 43 ss.

(79) Ai sensi dell'art. 102-*quater* l.d.a. le misure tecnologiche di protezione « comprendono tutte le tecnologie, i dispositivi o i componenti che, nel normale corso del loro funzionamento, sono destinati a impedire o limitare atti non autorizzati dai titolari dei diritti ».

(80) Sulla nozione di *DRM* cfr. CASO, Digital Rights Management. *Il commercio delle informazioni digitali tra contratto e diritto d'autore*, ristampa digitale, 2006, p. 5 ss., disponibile sul sito *www.jus.unitn.it*; più in generale sui c.d. *trusted system* come strumento a tutela della proprietà intellettuale in un contesto digitale, cfr. STEFIK, *Shifting the Possibile: How Trusted System and Digital Property Rights Challenge Us to Rethink Digital Publishing*, in *Berkeley Technology Law Journal*, 12:1 (Spring 1997), pubblicato sul sito *www.law.berkeley.edu*. Per una dettagliata disamina della struttura e del funzionamento dei *DRM* cfr. invece MONTAGNANI, *Dal* peer-to-peer *ai sistemi di* Digital Rights Management*: primi appunti sul* melting pot *della distribuzione* on line, in *Riv. dir. aut.*, 2007, p. 36 ss. e RENDA, *Architettura, controllo e DRM: notizie dal fronte*, in *Proprietà digitale. Diritti d'autore, nuove tecnologie e* digital rights management, a cura di Monta-

lare e proteggere la circolazione di un'opera creativa gestendo, attraverso la conformazione di uno o più prodotti tecnologici (siano essi *file*, *software* o *hardware*), le modalità di accesso e di godimento dei contenuti digitali secondo il contratto di licenza stipulato fra titolare dei diritti e fruitore dell'opera ([81]).

Si tratta tuttavia di un rimedio non privo di punti critici.

In primo luogo, poiché l'adozione di tali soluzioni tecnologiche consente di riaffermare un controllo di tipo proprietario anche in presenza di contenuti dematerializzati ([82]), il ricorso alle *TPM* comporta il rischio che vengano introdotte barriere aventi finalità *contra legem*. Con specifico riferimento alle opere musicali o cinematografiche ciò che preoccupa, oltre all'eventualità di un illecito trattamento di dati personali ([83]),

gnani e Borghi, Milano, 2006, p. 91. Cfr. inoltre le considerazioni espresse in termini di analisi economica del diritto da DREXL, *Diritto d'autore in ambiente digitale: dall'efficienza «economica» all'efficienza «normativa»*, in *Proprietà digitale. Diritti d'autore, nuove tecnologie e* digital rights management, a cura di Montagnani e Borghi, cit., p. 53 ss.

([81]) Cfr. a riguardo PROSPERETTI, *Il DRM per la creazione di regole certe nel rapporto tra consumatore e titolare dei diritti nella circolazione dei contenuti audiovisivi digitali*, in Digital rights management. *Problemi teorici e prospettive applicative. Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 21 ed il 22 marzo 2007*, a cura di Caso, Trento, 2008, p. 273 ss., disponibile sul sito *www.jus.unitn.it*, il quale osserva come il ricorso al *DRM* sia funzionale alla definizione delle politiche di gestione dei diritti digitali, ragion per cui esso non comporta necessariamente l'utilizzo di *TPM*, le quali verranno adottate solamente ove le politiche di gestione mirino alla protezione dell'opera, mentre non saranno necessarie ove si persegua il fine di agevolarne la circolazione. Più in generale sul tema si vedano, oltre agli ulteriori contributi contenuti in AA.VV., Digital rights management. *Problemi teorici e prospettive applicative. Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 21 ed il 22 marzo 2007*, a cura di Caso, cit.; MONTAGNANI, *op. cit.*, p. 1 ss. e AA.VV., *Proprietà digitale. Diritti d'autore, nuove tecnologie e* digital rights management, a cura di Montagnani e Borghi, cit.

([82]) Nello specifico le *TPM* consentono di conformare i diversi elementi che permettono la fruizione di un'informazione in formato digitale, a partire dall'informazione medesima, sino al *software* impiegato per la lettura/riproduzione della stessa e persino all'*hardware* utilizzato. In tal maniera si riesce *a priori* a rendere tecnicamente impossibili gli impieghi non autorizzati dell'opera protetta dal diritto d'autore, ad es. non permettendone la copia, ovvero impedendo al *software* di riprodurre *file* non regolarmente licenziati o ancora limitando la compatibilità dei *file* a specifici dispositivi ad essi dedicati.

([83]) L'eventualità che attraverso i *DRM* si ponga in essere un trattamento illecito di dati personali, per lo più consistente nell'attività di profilazione occulta dell'interessato, sussiste soprattutto nelle ipotesi in cui i *file* vengano scaricati da un distributore su abbonamento o in fruizione temporanea, ovvero attraverso la c.d. super-distribuzione (su queste modalità cfr. *infra* nel testo), laddove dunque vi può essere l'individuazione del soggetto contraente. Ove invece i *DRM* vengano impiegati al fine di differenziare le tipologie di prodotto, consentendo *a priori* diverse opzioni d'uso in maniera indipendente dall'identità del singolo utilizzatore e determinando dunque regole generali incentrate sul *file* e non sul fruitore, non vi dovrebbe essere raccolta alcuna di dati personali, anche in ottemperanza al generale principio di necessità di cui all'art. 6, § 1, lett. *c*), direttiva n. 95/46/Ce, recepito nel nostro ordinamento mediante gli artt. 3 e 11, comma 1°,

è la possibilità che i *DRM* siano impiegati per circoscrivere i diritti riconosciuti dal legislatore al legittimo fruitore dell'opera (quale ad esempio quello della copia privata ad uso personale) o per estendere i diritti di privativa al di là dei limiti consentiti dall'ordinamento, in pregiudizio delle libere utilizzazioni e della caduta in pubblico dominio dell'opera ([84]).

Occorre dunque che le forme tecnologiche di protezione non risultino in conflitto, bensì coerenti con le disposizioni normative ([85]), costituendone una particolare attuazione di significativa efficacia preventiva degli illeciti, ma pur sempre un'applicazione e non uno strumento per l'affermazione di (diverse) regole di tipo privatistico espressione della posizione di forza di chi controlla gli strumenti informatici ed i prodotti digitali ([86]).

Un ulteriore contrasto fra norma e *DRM* può poi derivare dalla fissità che viene a connotare la regola di diritto una volta incorporata in un dispositivo tecnologico, in contrapposizione con l'evoluzione del fenomeno legislativo, da cui il rischio che siano apposte barriere operative non più

lett. *d*), d.lgs. n. 196 del 2003. Sul rapporto fra *privacy* e utilizzo di *DRM*, cfr. ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working document on data protection issues related to intellectual property rights*, 18 gennaio 2005, p. 2 s., pubblicato sul sito ufficiale dell'Unione europea, *www.europa.eu*, e in dottrina CASO, *op. cit.*, p. 98 ss.

([84]) Cfr. a riguardo SPADA, *op. cit.*, p. 601 ss. e RICOLFI, *op. cit.*, p. 465 s., nonché, più recentemente, CASO, *Relazione introduttiva. Forme di controllo delle informazioni digitali: il* digital rights management, in Digital rights management. *Problemi teorici e prospettive applicative. Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 21 ed il 22 marzo 2007*, a cura di Caso, cit., p 48 ss. e GRANIERI, *DRM vs. diritto d'autore: la prospettiva dell'analisi economica del diritto giustifica una protezione assoluta delle opere dell'ingegno di carattere creativo?*, ivi, pp. 84 e 91 s. Non vanno poi trascurati i profili inerenti le dinamiche di mercato e la libertà di concorrenza correlati all'impiego dei *DRM*, in termini di barriere all'ingresso o di abuso di posizione dominante conseguenti alle limitazioni poste all'interoperabilità fra formati digitali e apparati di riproduzione; cfr. a riguardo: MONTAGNANI, *DRM e tutela della concorrenza*, in Digital rights management. *Problemi teorici e prospettive applicative. Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 21 ed il 22 marzo 2007*, a cura di Caso, cit., p. 215 ss.; MAZZIOTTI, *DRM e abuso di posizione dominante: il caso iTunes*, ivi, p. 239 ss.; MAGNANI-MANDERIEX-MONTAGNANI, *I sistemi di* Digital Rights Management *e il diritto della concorrenza: l'individuazione del mercato rilevante e la definizione delle barriere all'ingresso*, in *Proprietà digitale. Diritti d'autore, nuove tecnologie e* digital rights management, a cura di Montagnani e Borghi, cit., p. 223 ss.

([85]) Cfr. SPADA, *op. cit.*, pp. 597 e 603.

([86]) Va tuttavia osservato come queste considerazioni paiano ad oggi essere almeno in parte contraddette con riferimento alla divulgazione delle opere protette dal diritto d'autore *on-line*: gli artt. 71-*quinquies*, comma 3°, e 71-*sexies*, comma 3°, l.d.a., conseguenti alla novella del 2003, prevedono infatti che i titolari dei diritti non siano tenuti a rimuovere le *TPM* al fine di consentire le utilizzazioni di cui agli artt. 55, 68, commi 1° e 2°, 69, comma 2°, 70, comma 1°, 71-*bis* e 71-*quater*, o la riproduzione privata ad uso personale. L'interpretazione degli artt. 71-*quinquies*, comma 3°, e 71-*sexies*, comma 3°, l.d.a. non è stata tuttavia oggetto di particolare approfondimento in dottrina ed attualmente manca una netta indicazione nel senso di ritenere tali disposizioni, pensate per i servizi *on demand* — v. dir. n. 2001/29/Ce, 53° considerando —, estensibili all'ipotesi del *file-sharing*; cfr. però in senso affermativo FARINA, *op. cit.*, p. 1030 e MONTAGNANI, *op. cit.*, p. 26.

giustificate dal dettato normativo. È dunque opportuno che i sistemi *DRM* vengano, sin dall'origine, predisposti in maniera tale da consentire i successivi necessari aggiornamenti dei diritti riconosciuti all'utente.

Da ultimo, anche sotto il profilo commerciale, l'impiego di *DRM* può poi comportare alcuni problemi, a causa dei limiti di interoperabilità di tali sistemi ([87]). In specie al consumatore che « scarichi » lecitamente musica può capitare di poter riprodurre la stessa utilizzando solamente alcune specifiche tipologie di dispositivi, ragion per cui le principali case discografiche si sono recentemente orientate verso la distribuzione di *file* musicali *DRM-free* ([88]), almeno nell'ipotesi di *download* di singoli brani o album, mantenendo invece l'impiego dei *DRM* per i servizi su abbonamento ([89]), per quelli di « super-distribuzione » ([90]) o di fruizione temporanea ([91]).

Considerate le diverse implicazioni problematiche proprie dell'introduzione di barriere tecnologiche incidenti sulle modalità di fruizione dei contenuti digitali, recentemente si è anche pensato di adottare soluzioni tecniche incidenti non sui contenuti, bensì sulla circolazione in rete degli stessi. In tal senso è stata ricercata la collaborazione dei *provider* per contrastare in maniera attiva lo scambio illecito di *file* mediante l'adozione di filtri volti ad impedirlo ([92]). È però lecito dubitare della reale efficacia di una simile soluzione che, a secondo del livello di incidenza del monitoraggio delle comunicazioni e del filtraggio, o si rivela facilmente aggirabile oppure eccessivamente onerosa per i fornitori di connessione e, in quanto tale, incompatibile con il mantenimento dell'accesso alle rete a costi di mercato ([93]).

([87]) Cfr. IFPI, *Digital Music Report 2007*, cit., p. 22.

([88]) Cfr. IFPI, *Digital Music Report 2008*, gennaio 2008, p. 15, disponibile sul sito *www.ifpi.org.*

([89]) In questo caso, a fronte di un abbonamento temporaneo (solitamente mensile), l'utente può « scaricare » un numero illimitato di *file*.

([90]) Si tratta di servizi in cui agli utenti è concesso di scambiare musica con altri entro specifici limiti definiti dai *DRM*; in questa maniera *file* lecitamente acquistati possono anche essere immessi nelle reti *peer to peer*.

([91]) In questa ipotesi il *download* illimitato di *file* musicali costituisce una prestazione accessoria rispetto a quella principale (consistente ad esempio nella fornitura di connessione ad *internet* con abbonamento *flat*) ed è possibile fruire del materiale « scaricato » solamente finché perdura il contratto relativo alla prestazione principale. Più in generale sui differenti modelli di distribuzione cfr. MONTAGNANI, *op. cit.*, p. 44 ss.

([92]) In tal senso si è orientato il governo francese, firmando un accordo con i produttori di materiale audiovisivo e con i fornitori di connessione *internet* (per altro dando vita a qualche dubbio circa la terzietà della commissione di studio creata *ad hoc*, posto che è stata presieduta dall'amministratore delegato del gruppo Fnac). L'esempio francese è stato seguito anche da Inghilterra e Giappone, cfr. a riguardo FRANCESCHI DE MARCHI, Peer to Peer*, via la connessione a chi scarica: il Giappone adotta la « dottrina Sarkozy »*, marzo 2008, in *www.ilsole24ore.com.*

([93]) Cfr. a riguardo DINI, *Sarkozy vuole civilizzare la rete con il filtro anti « pirateria »*, 29 novembre 2007, in *www.ilsole24ore.com*. Vale poi sempre l'osservazione formulata da RICOLFI, *op. cit.*, p. 447, secondo cui « telephone companies and telecoms are quite understandably more concerned about the amount of traffic which goes through

Più agevole, sebbene di minor efficacia, è invece dissuadere il ricorso al *peer to peer* rendendo più lunghi i tempi di connessione per la trasmissione dei *file*, ma in questo caso vi possono essere implicazioni in termini di mancato adempimento agli obblighi contrattuali da parte di chi offre la connettività, anche alla luce del fatto che non necessariamente l'uso di connessioni *peer to peer* è indice di una violazione dei diritti d'autore, né sulla base della sola analisi della tipologia di *file* condivisi (es. *file* musicali) si può escludere che si tratti di opere non protette o di libero scambio (94).

La disamina delle principali soluzioni tecniche al problema del *file sharing* mostra dunque come, se da un lato le sole norme di tipo comportamentale, incentrate sui divieti imposti dalla legge e sul necessario ricorso ai giudici per ottenerne l'*enforcement* (oltre che il ristoro dei danni subiti), non si dimostrino sufficienti per una reale tutela, d'altra parte anche le soluzioni tecnologiche che incorporino il dettato normativo, almeno in termini di tutela dell'opera, non vanno esenti da problemi, benché in definitiva possano ritenersi più efficienti.

Sulla base della passata esperienza in materia di contraffazione delle opere protette dal diritto d'autore, va poi aggiunto che all'inventiva dimostrata da chi si adopera per contrastare l'impiego illecito di tali opere solitamente corrisponde altrettanta inventiva di chi trova le soluzioni per superare le barriere via via frapposte, come ben insegna l'esperienza della protezione del *software*. Ragion per cui le soluzioni tecniche non fanno che dar vita ad una continua corsa al rafforzamento delle difese adottate, non certo priva di costi.

È alla luce di tutti questi elementi che quindi occorre interrogarsi, se non sulla valenza dell'esclusiva dello sfruttamento economico riconosciuta all'autore sulle proprie opere, quantomeno sull'opportunità di ripensare i criteri distributivi e commerciali attualmente prevalenti nel settore discografico e, più in generale, dei *media*.

A favore di nuovi modelli di *business* (95) depongono alcune considerazioni, quali la netta riduzione dei costi sostenuti dai produttori attraverso la distribuzione *on-line* e la possibilità di offrire servizi personaliz-

the [information] superhighway than about the ownership and licensing requirements of whichever ''vehicle''... rides on it».

(94) Proprio per le ragioni indicate non sono mancate le reazioni da parte degli utenti a fronte dell'adozione di simili misure di riduzione della velocità di connessione; si veda al riguardo per gli Stati Uniti il caso Comcast e per l'Italia il caso Tele2, su cui sono attualmente disponibili solamente notizie di fonte giornalistica, cfr. WEISS, *Class Action Filed Against Comcast for File-Sharing Slowdowns*, 28 febbraio 2008, pubblicato sul sito *www.abajournal.com* e LONGO, *Tele2 limita il «peer to peer». E parte la denuncia dei consumatori*, 14 gennaio 2008, pubblicato sul sito *www.repubblica.it.*

(95) Per un'analisi di alcune possibili soluzioni cfr. RENDA, *op. cit.*, p. 97 ss. e THE BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD LAW SCHOOL-DIGITAL MEDIA PROJECT, *Content and Control: Assessing the Impact of Policy choices on Potential Online Business Models in the Music and Film Industries*, 7 gennaio 2005, pubblicato all'indirizzo *http://cyber.law.harvard.edu.*

zati che si discostino dalla tradizionale vendita di brani aggregati in un album in maniera non negoziabile ([96]).

Ovviamente un ripensamento delle strategie aziendali non è da solo sufficiente a scoraggiare la pulsione opportunistica di ottenere gratuitamente quanto è a pagamento ([97]), per questo occorre una sinergia fra le diverse opzioni sin qui esaminate, ricorrendo alle vie legali nei casi più gravi di violazione del diritto d'autore, introducendo tecnologie conformate (ma non tali da creare ostacoli alla lecita piena fruizione dei contenuti, socialmente intollerabili in quella che è definita la « società dell'informazione »), sviluppando nuovi modelli di *business* coerenti con la digitalizzazione dei contenuti.

ALESSANDRO MANTELERO
Ricercatore del Politecnico di Torino

([96]) Molti degli utenti delle reti *peer to peer* sono infatti anche acquirenti di prodotti musicali tradizionali, ma si servono dei sistemi di *file-sharing* per contenere i costi e per avere un servizio caratterizzato da maggior fruibilità, anche in termini di personalizzazione; cfr. *supra* nota 69.

([97]) Il noto sistema di distribuzione musicale *iTunes* ideato dalla Apple ha infatti registrato 2 miliardi di *download* musicali fra l'aprile 2003 ed il gennaio 2007, cfr. *iTunes Store Tops Two Billion Songs*, 9 gennaio 2007, in *www.apple.com*, a fronte di 5 miliardi di *download* al mese sulle reti *peer to peer*, di cui il 97,5% risulta illegale, cfr. *Universal Backs Free Music Offer*, BBC News, 29 agosto 2006, cit.