Il conflitto tra *copyright* e *privacy* nelle reti Peer to Peer: il caso Peppermint – Profili di diritto comparato

Versione 1.0 dicembre 2007

Roberto Caso

Il conflitto tra *copyright* e *privacy* nelle reti Peer to Peer: il caso Peppermint – Profili di diritto comparato

Versione 1.0 dicembre 2007[*]

Roberto Caso

1. Introduzione

Le architetture Internet *Peer to Peer* (P2P) rappresentano un'innovazione tecnologica straordinaria. Per il loro tramite, è possibile svolgere funzioni di indubbia utilità. Il traffico P2P costituisce una porzione crescente del traffico complessivo di Internet. D'altra parte, le architetture P2P vengono usate anche per fini illeciti, tra i quali figura il *file sharing* (la condivisione, lo scambio) non autorizzato di contenuti protetti dal diritto d'autore. Le multinazionali dell'industria dell'intrattenimento additano il P2P come la più grave minaccia posta dalle tecnologie digitali al diritto d'autore.

In estrema e approssimativa sintesi, le architetture P2P sono reti non gerarchiche. A differenza, ad esempio, del World Wide Web nell'ambito del quale vi sono computer (detti *server*) che forniscono informazioni e computer (detti *client*) che acquisiscono informazioni, nelle architetture P2P tutti i computer della rete rivestono ibridamente e (appunto) paritariamente sia la

[*] Articolo già apparso in *Diritto dell'Internet*, 2007, 471.

funzione *client* sia quella *server*. Queste caratteristiche rendono difficoltoso il contrasto dello scambio non autorizzato di file protetti dal diritto d'autore. Nelle architetture gerarchiche il contrasto può far leva su misure volte ad agire su *server* (relativamente) ridotti nel numero e visibili, in quanto esposti al pubblico; mentre nelle architetture le azioni dei titolari dei diritti si scontrano con il numero altissimo dei computer connessi e con la natura privata del traffico P2P. Di fatto è possibile acquistare un CD musicale, riversare (in gergo: *to rip*) le tracce audio sul proprio *hard disk*, e caricare (*to upload*) queste ultime in una rete di *file sharing* (più precisamente: consentire ad altri utenti della rete di accedere alla porzione della propria memoria fissa dove sono caricati i file), innescando una moltiplicazione potenzialmente infinita delle copie delle tracce audio.

Le strategie di contrasto allo scambio non autorizzato di file protetti dal *copyright* nascono negli Stati Uniti, paese (finora) leader sia nel campo dell'industria dell'intrattenimento sia in quello dell'informatica.

È possibile raggruppare tali strategie nel modo seguente:

a) Aggressive campagne pubblicitarie che mirano a persuadere il pubblico del carattere illecito del *file sharing* di contenuti protetti dal *copyright* (tali campagne si basano anche su semplificazioni fuorvianti come quella che punta ad identificare il *file sharing* non autorizzato con il reato di furto)[1];

b) Produzione di sistemi di Digital Rights Management (DRM) che abilitano la gestione ed il commercio di file associati a misure tecnologiche di protezione che, tra l'altro, possono impedire la copia e la distribuzione non autorizzate[2];

c) Azioni giudiziarie, di prima generazione, volte ad inibire servizi informativi per il *file sharing*[3], e azioni giudiziarie, di seconda generazione, volte ad inibire la produzione del software che genera le reti P2P[4];

d) Azioni giudiziarie e stragiudiziarie volte a colpire gli utenti delle reti P2P.

Ci si soffermerà solo sull'ultima strategia. In quanto le vicende statunitensi che la riguardano possono aiutare a comprendere le questioni sollevate dalle pronunce qui commentate[5]. I

[1] Una nota campagna pubblicitaria così recita: "you wouldn't steal this, you wouldn't steal that. You wouldn't steal a movie, right? Movie piracy is stealing. Stealing is against the law. Piracy is a crime".

[2] Sui profili giuridici del DRM v. R. CASO, *Digital Rights Management. Il commercio delle informazioni digitali tra contratto e diritto d'autore*, Padova, 2004, ristampa digitale, Trento, 2006, disponibile all'URL: «http://www.jus.unitn.it/users/caso/pubblicazioni/drm/download.asp».

[3] V. *A&M records, Inc. v. Napster, Inc.* 239 F.3d 1004 (9th Cir. 2001).

[4] V. *MGM Studios, Inc. v. Grokster*, Ltd. 545 U.S. 913 (2005).

[5] Trib. Roma ord. decisa il 14 luglio 2007 e Trib. Roma ord. decisa il 9 febbraio 2007.

fatti italiani dimostrano, una volta di più, come nell'era della globalizzazione circolino rapidamente da un sistema giuridico ad un altro, non solo norme e teorie, ma anche strategie di tutela dei diritti[6].

Le strategie giudiziarie e stragiudiziarie volte a colpire direttamente gli utenti delle reti P2P sollevano numerosi problemi, tra i quali spicca il conflitto tra tutela della proprietà intellettuale e protezione della *privacy*. Lo scopo delle pagine seguenti è fornire le prime indicazioni sul modo in cui il sistema giuridico nordamericano gestisce tale conflitto. Offrendo alcuni spunti di comparazione con l'ordinamento italiano.

Il ragionamento così si articola. Nel paragrafo 2 si disegnano le linee essenziali della legge statunitense che costituisce il modello normativo delle azioni volte a colpire gli utenti delle reti P2P, dimostrando come la scelta del legislatore sia stata quella di privatizzare il contrasto delle violazioni del *copyright*, incentivando l'autotutela privata e comprimendo i margini della *privacy*. Nel paragrafo 3 si accennerà al *leading case* che ha affrontato uno degli aspetti più discussi della legge, ponendo un argine all'abuso delle strategie stragiudiziarie di contrasto del *file sharing* non autorizzato. Nel paragrafo 4 si offrirà un quadro sintetico delle critiche mosse dalla dottrina d'oltreoceano alla strategia volta a colpire gli utenti delle reti P2P, la quale si inserisce in una più ampia tendenza all'instaurazione di un regime privato (cioè non facente capo a soggetti o enti statali) e diffuso di sorveglianza delle attività svolte dagli utenti di Internet. Nel paragrafo 5 si svolgono alcune brevi considerazioni a margine della normativa italiana che fa da sfondo ai casi oggetto delle pronunce qui commentate. Nel paragrafo 6 si tracciano alcune considerazioni conclusive.

2. Il Digital Millenium Copyright Act, la privatizzazione della tutela del *copyright*, e la compressione della *privacy*

Quando, nel 1998, il Digital Millennium Copyright Act (DMCA) venne emanato, la minaccia delle reti P2P era ancora di là dall'essere percepita. La casistica presa in considerazione dal legislatore guardava piuttosto al caso dell'Internet Service Provider (ISP) che, nell'ambito delle reti a struttura gerarchica, forniva, o aiutava terzi a fornire, illecitamente al pubblico contenuti protetti da *copyright*. La scelta del legislatore fu di creare alcune esenzioni di responsabilità per gli ISP che si limitano ad offrire servizi di intermediazione (come l'accesso alla rete e la trasmissione dei dati): c.d. *safe harbor provisions*. Tuttavia, la logica posta alla base delle *safe harbor provisions* non è quella dell'esenzione totale di responsabilità.

Infatti, in base *alle safe harbor provisions*, codificate alla 17 U.S.C. § 512, una vera e propria esenzione di responsabilità vale solo per l'ISP che offre unicamente servizi di trasmissione, *routing*, e connessione.

---

[6] Si pensi, ad esempio, ai casi relativi alla modificazione dei chip della Sony Plastation, a margine dei quali v. R. CASO, *Modchip e diritto d'autore: la fragilità del manicheismo tecnologico nelle aule della giustizia penale, in Ciberspazio e diritto*, 2006, 183, disponibile anche all'URL: «http://www.jus.unitn.it/users/caso/DRM/Libro/mod_chips/download.asp»; M. FERRARI, *L'incerto cammino della tutela giuridica delle misure tecnologiche di protezione del diritto d'autore: recenti orientamenti in materia di modifica di consoles per videogiochi*, in *Dir. Internet*, 2006, 269.

Per gli ISP che offrono servizi di *caching* o memorizzazione temporanea, di *hosting* (cioè di ospitalità sui propri *server*), di *linking* o di rinvio, relativamente a materiale in violazione del *copyright*, vale il meccanismo denominato: *notice-and-takedown process*. Tale meccanismo subordina l'esenzione di responsabilità ad un determinato comportamento. L'ISP, il quale riceva un'appropriata – appropriata nel senso che deve rispondere ad alcuni requisiti stabiliti dalla legge – notifica di una lamentata violazione da parte di un titolare di *copyright*, deve provvedere rapidamente a rimuovere il materiale in violazione o a disabilitare l'accesso al medesimo materiale.

Lo stesso DMCA disciplina alla 17 U.S.C. § 512 (m) alcune implicazioni in termini di *privacy*, specificando che l'ISP non è obbligato a monitorare i propri servizi allo scopo di individuare attività in violazione del *copyright* o a ricercare attività in violazione, se non nei limiti richiesti dagli standard tecnici.

Il *notice-and-takedown process* poteva forse esser letto all'epoca dell'emanazione del DMCA come un discreto compromesso fra le posizioni di chi reclamava un aggravamento della responsabilità degli ISP anche sulla base di argomentazioni che indicavano gli ISP come l'unico sicuro punto riferimento per l'*enforcement* dei diritti e chi invece sosteneva la necessità di una sua compressione anche al fine di evitare di ribaltare sugli ISP un'impropria attività di censura.

Tuttavia, sono sfuggiti molti dei contraccolpi che il *notice-and-takedown process* proietta sul piano della *privacy*. Tale meccanismo infatti incentiva – nell'assenza di leggi rigorose sulla *privacy* nelle comunicazioni elettroniche – una vasta attività di sorveglianza e di investigazione privata da parte dei titolari di *copyright*. Non a caso, gli ultimi anni contano lo sviluppo incontrollato di tecnologie volte a monitorare le violazioni del *copyright*. Ad esempio, i titolari di *copyright* usano agenti software o robot (detti anche "bot") come i Web crawler che passano in rassegna i *server* e stilano liste di indirizzi Web che offrono materiali in violazione del *copyright*[7].

Ma c'è di più. Il DMCA ha affiancato al *notice-and-takedown process* un potente strumento stragiudiziale – si tratta di un *subpoena* speciale creato *ad hoc* per la tutela delle opere dell'ingegno in Internet – che consente ai titolari di *copyright* di richiedere, sulla base del mero convincimento in buona fede dell'avvenuta violazione del diritto di esclusiva, ad alcune categorie di ISP l'identità dei propri utenti che si presume abbiano commesso violazioni del *copyright*. Si tratta evidentemente di un ulteriore rilevante incentivo alla privatizzazione della tutela, in quanto il *subpoena* è, come si è accennato, uno strumento stragiudiziale che perciò si svolge al di fuori di un procedimento giurisdizionale assistito dalla garanzia del contraddittorio, senza la supervisione di un giudice. Però, come ci si accinge a chiarire, la giurisprudenza federale ha delimitato considerevolmente il campo di applicazione delle *subpoena provisions*.

[7] V. S. KATYAL, *Privacy vs. Piracy*, 7 *Yale Journal of Law & Technology* 222, 272-273 (2004), disponibile anche su SSRN all'URL: «http://ssrn.com/abstract=722441».

3. Il caso Verizon ed i limiti della tutela stragiudiziale del *copyright*

Le disposizioni del DMCA dedicate alla responsabilità degli ISP nacquero vecchie. All'indomani dell'emanazione della legge ci si dovette confrontare con la prima generazione di reti P2P (simboleggiata da Napster) e poco dopo con la seconda generazione (KaZaA, Morpheus, Grokster, eDonkey etc.).

La seconda generazione di reti P2P prescinde da qualsiasi funzione accentrata o gerarchica. Non esiste una distinzione tra *server* e *client*, in quanto tutti i computer della rete svolgono funzioni ibride. Il produttore del software per la gestione della rete mette a disposizione del pubblico – mediante Internet stessa – il proprio prodotto. Chi vuole, può scaricarlo (ad esempio, dal sito Web dell'azienda produttrice) e poi installarlo sul proprio computer. A quel punto, l'utente si dota di uno pseudonimo, detto anche *screen name*, e può cercare altri utenti della rete P2P disposti ad effettuare il *file sharing*. Può limitarsi a scaricare (*to download*), ma il più delle volte procede – secondo lo spirito ed i costumi delle comunità P2P – anche a caricare (*to upload*) file o, per meglio dire, a mettere a disposizione una parte della propria memoria fissa, ovvero del proprio *hard disk*.

Nell'ambito della strategia che mira a colpire direttamente gli utenti delle reti P2P, i titolari di file musicali protetti da *copyright* svolgono – come si è accennato sopra – attività di monitoraggio delle reti P2P allo scopo di procurarsi gli *screen names* degli utenti della rete e gli indirizzi IP corrispondenti ad attività che si assumono in violazione del *copyright*. In particolare la Recording Industry Association of America (RIIA) ha avviato da anni una massiccia campagna tesa ad individuare i soggetti che si presume commettano violazioni del *copyright* dei propri associati. Né lo *screen name*, né l'indirizzo IP, che è semplicemente un numero, consentono l'identificazione del presunto trasgressore. La RIIA è costretta chiedere all'ISP di turno l'identità dell'utenza associata all'indirizzo IP.

Nella controversia sfociata nel più importante precedente in materia, la RIIA aveva chiesto, mediante lo strumento stragiudiziale del *subpoena* speciale previsto dalla 17 U.S.C. § 512 (h), a Verizon, l'ISP di riferimento, di rivelare le identità associate agli indirizzi IP tracciati dalla stessa RIIA. Verizon si era rifiutata in base ad una serie di considerazioni giuridiche.

In primo grado la RIIA ha avuto successo, ma in appello la Corte federale del Circuito di Columbia ha ritenuto illegittimo il ricorso al *subpoena*[8].

Le argomentazioni della corte si arrestano su un piano formale. La 17 U.S.C. § 512 (h) va interpretata nel senso che non è possibile fare ricorso allo strumento del *subpoena*, quando l'ISP non proceda a memorizzare sui propri computer il materiale in violazione, ma si limiti ad offrire – come nel caso delle reti P2P – la mera connessione ad Internet.

La sentenza Verizon ha rappresentato un argine solo per la deriva più estremista della privatizzazione della tutela del *copyright*: quella appunto che fa leva sul *subpoena* previsto dal DMCA.

[8] *Recording Indus. Ass'n of Am. V. Verizon Internet Servs, Inc.*, 351 F. 3d 1229 (D.C. Cir. 2003).

Cionondimeno, il contesto legislativo nordamericano rimane un terreno sostanzialmente favorevole alla strategia che mira a colpire direttamente gli utenti delle reti P2P con quel che ne deriva in termini di compressione della *privacy*. Lo comprova il fatto che la RIIA ha continuato a perseguire la sua politica di identificazione dei presunti violatori sia per via giudiziale sia per via stragiudiziale[9].

I risvolti in termini di *privacy* di questa politica non sono però sfuggiti alle associazioni per la difesa della libertà su Internet ed ampi settori della dottrina.

4. Lo spettro della sorveglianza privata: verso una disintegrazione della privacy e della libertà di pensiero in Internet?

La strategia che mira a colpire direttamente gli utenti delle reti P2P si basa sulla privatizzazione della tutela del *copyright*. Tale tendenza alla privatizzazione riguarda l'intero settore del diritto dell'era digitale.

La punta più avanzata è rappresentata dai sistemi di DRM finora utilizzati dall'industria dell'intrattenimento. Tali sistemi di DRM possono inglobare componenti volte a garantire l'autotutela tecnologica. Si può, ad esempio, confezionare un file limitando la possibilità di copia e facendo sì che il tentativo di aggirare la limitazione sia "sanzionato" dalla disattivazione totale del file. Inoltre i sistemi di DRM possono inglobare componenti destinate a tracciare l'utilizzo del contenuto digitale, anche al fine di individuare le condotte che violano la legge o i termini della licenza d'uso[10]. L'invasività dei sistemi di DRM non è una questione teorica. Lo dimostra, tra l'altro, il recente caso Sony Rootkit[11].

Secondo alcuni, il contesto digitale sembra delineare un rovesciamento della prospettiva tradizionale che vede la proprietà come baluardo della *privacy*. Di sicuro, nella dimensione di Internet la sempre più aggressiva autotutela della proprietà intellettuale tende a comprimere progressivamente i confini della *privacy*[12]. Le grandi imprese dell'intrattenimento perseguono strategie che mirano a spostare il confine tra pubblico e privato. Ad esempio la politica di identificazione degli utenti delle reti P2P prende le mosse dall'assunto che, stante il fatto che le reti

---

[9] Secondo il conteggio tenuto dall'Electronic Frontier Foundation al novembre 2005 si registravano più di 15.000 azioni intentate dalla RIIA contro utenti. Si veda il documento intitolato *RIIA v. The People: Two Yars Later*, November 3 2005, disponibile all'URL: «http://www.eff.org/IP/P2P/RIAAatTWO_FINAL.pdf»

[10] Sull'invasività dei sistemi di DRM v. J. E. Cohen, *DRM and Privacy*, 13 *Berkeley Tech. L. J.* 575 (2003), disponibile su SSRN all'URL: «http://ssrn.com/abstract=372741». Nella letteratura italiana v. CASO, *Digital Rights Management. Il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 98 ss.

[11] Sul caso Sony BMG Rootkit v. R. C. PICKER, *Mistrust-Based Digital Rights Management*, (April 2006), *U Chicago Law & Economics, Olin Working Paper No. 291*, disponibile su SSRN all'URL: «http://ssrn.com/abstract=899155»; J. F. DEBEER, *How Restrictive Terms and Technologies Backfired on Sony BMG*, *Internet & E-Commerce Law in Canada*, Vol. 6, No. 12, February 2006, disponibile su SSRN all'URL: «http://ssrn.com/abstract=901305». Nella letteratura italiana v. T. MARGONI, *Il conflitto tra Digital Rights Management e privacy nel caso Sony-rootkit,* in *Dir. Internet*, 2006, 519.

[12] KATYAL, *Privacy vs. Piracy*, cit., 241 ss.

oggetto di controversie sono aperte al pubblico (nel senso che chiunque può accedere alla rete), è possibile tracciare massivamente gli indirizzi IP. In altri termini, secondo questa prospettiva, l'utente che consente ad altri utenti sconosciuti di accedere e prelevare file dalla propria memoria fissa espone, per la natura stessa della rete P2P, la propria identità digitale (in particolare, il proprio indirizzo IP) al pubblico.

Spesso questa visione è supportata da argomentazioni che fanno leva sull'analogia con il contesto non virtuale, cioè con la dimensione giuridica posta al di fuori di Internet. Nel solco di tale analogia si possono incontrare argomentazioni di questo tipo: se si praticano pubblicamente atti in violazione della proprietà intellettuale altrui, allora il titolare della proprietà intellettuale può autotutelarsi anche procedendo ad acquisire informazioni sulle identità dei soggetti che compiono l'illecito.

Questo tipo di argomentazione distorce il quadro di riferimento[13]. Come sempre, nei discorsi sul diritto dell'era digitale, le analogie con la dimensione giuridica non digitale possono essere fuorvianti[14].

Il punto di partenza di qualsiasi discorso sul tema della tutela è il principio del divieto di autotutela privata, principio (e valore) cardine della tradizione giuridica occidentale[15]. Le eccezioni a tale principio sono severamente limitate

Tali limitazioni sono tanto più giustificate nel contesto specifico dell'identificabilità degli utenti della rete Internet, ed, in particolare, delle reti P2P. Il fatto che qualsiasi navigazione Web implichi l'esposizione del proprio indirizzo IP a chi è in possesso di tecnologie che ne consentono il tracciamento, non fa della stessa navigazione un'attività pubblica. Anzi, è vero esattamente il contrario: si tratta di un'attività privata eminentemente protetta dalla *privacy*. Allo stesso modo, le attività di *file sharing* su reti P2P sono attività private. In particolare, quando riguardano la sfera delicatissima del consumo dei prodotti intellettuali, consumo che si pone alla base dell'autonomia e

[13] Cfr. KATYAL, *Privacy vs. Piracy*, cit., 319 ss.

[14] Il diritto dell'era digitale presenta caratteristiche proprie. V. G. PASCUZZI, *Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche*, II ed., Bologna, 2006.

[15] Sul tema dell'autotutela nel diritto dell'era digitale v. M. J. RADIN, *Regulation by Contract, Regulation by Machine*, 160 *Journal of Institutional and Theoretical Economics* 1 (2004), disponibile su SSRN all'URL: «http://ssrn.com/abstract=534042»; ID., *Regime Change in Intellectual Property: Superseding the Law of the State with the "Law" of the Firm*, 1 *University of Ottawa Law & Technology Journal* 173 (2003-2004), disponibile su SSRN all'URL: «http://ssrn.com/abstract=534024»; D. LICHTMAN, *How the Law Responds to Self-Help*, (December 2004), *U Chicago Law & Economics, Olin Working Paper No. 232.*, disponibile su SSRN all'URL: «http://ssrn.com/abstract=629287»; K W. DAM, *Self-Help in the Digital Jungle*, (March 1999), *University of Chicago Law School, John M. Olin Law & Economics Working Paper No. 59*, disponibile su SSRN: «http://ssrn.com/abstract=157448»; J. E. COHEN, *Copyright and The Jurisprudence of Self-Help*,13 *Berkeley Tech. L. J.* 1089 (1998); P. SAMUELSON, *Embedding Technical Self-Help in Licensed Software*, 40 *Comm. ACM* 13 (Oct. 1997); H. GITTER, *Self-Help Remedies for Software Vendors*, 9 *Santa Clara Computer & High Tech. L.J.* 413 (1993). Nella letteratura italiana v. CASO, *Digital rights management. Il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 108 ss.

della libertà di pensiero[16]. Il fatto che l'utente consenta ad altro utente di "entrare" nel proprio computer allo scopo specifico del prelievo dei file messi a disposizione non può essere considerato un consenso implicito al monitoraggio ed al tracciamento, mediante potenti tecnologie che permettono l'aggregazione di immense quantità di dati, delle proprie attività.

L'acquisizione di informazioni relative all'identificazione degli utenti delle reti P2P si basa su tecnologie, costruite da privati, particolarmente invasive che conferiscono ad altri privati (le industrie dell'intrattenimento) un inedito potere di sorveglianza che può portare alla disintegrazione non solo della *privacy*, ma anche della libertà di pensiero[17].

Le vicende americane dimostrano che il tracciamento attuato mediante le tecnologie c.d. antipirateria sono soggette ad un elevato numero di errori e si prestano ad abusi opportunistici. Le industrie dell'intrattenimento, una volta ottenute (magari per via stragiudiziale) le identità corrispondenti agli indirizzi IP tracciati, contattano i soggetti identificati e li minacciano di azione giudiziaria offrendo contemporaneamente l'alternativa di una costosissima transazione. Si tratta di una strategia di difesa ai limiti (in alcuni casi, oltre i limiti) della condotta estorsiva[18].

In un settore come quello del *copyright* dove l'estensione del diritto di esclusiva è circondata da confini indistinti (si pensi all'incertezza che sostanzia la teoria universale della dicotomia tra idea, non protetta, e forma espressiva, protetta, o il *fair use* statunitense, ma anche le libere utilizzazioni di stampo continentale), anche chi compie attività lecite potrebbe essere bloccato dalla paura di essere tracciato e raggiunto dai titolari di proprietà intellettuale.

Messo in termini di analisi economica del diritto: se è vero che la sorveglianza privata può comportare (oltre che benefici privati anche) benefici sociali in termini di risparmio dei costi della sorveglianza statale, è altresì vero che la sorveglianza privata può comportare enormi costi sociali in termini di compressione della *privacy* e della libertà di pensiero[19].

5. Il panorama legislativo del caso Peppermint

Questa rapida ricognizione delle vicende statunitensi in materia di identificazione degli utenti delle reti P2P può aiutare ad interpretare il quadro legislativo sottoposto all'attenzione delle pronunce qui commentate? Forse sì. Non c'è dubbio che il diritto d'autore euro-italiano marci verso un rafforzamento anche più esasperato del *copyright* nordamericano[20]. Però, a differenza dell'ordinamento statunitense, il contesto giuridico euro-italiano può contare su una normativa generale in materia di protezione dei dati personali assai rigorosa.

---

[16] Sul tema v. Cohen, *DRM and Privacy*, cit.

[17] Cfr. KATYAL, *Privacy vs. Piracy*, cit., 290 ss.

[18] Si veda il già citato documento dell'Electronic Fronier Foundation intitolato *RIIA v. The People: Two Yars Later*.

[19] Cfr. KATYAL, *Privacy vs. Piracy*, cit., 328 ss.

[20] Per una dimostrazione di questa affermazione con riferimento alla disciplina delle misure tecnologiche di protezione dei diritti d'autore v. CASO, *Digital rights management. Il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 152 ss.

Al fine della corretta risoluzione delle controversie oggetto delle pronunce qui commentate, è di fondamentale importanza la ricostruzione del rapporto tra tutela del diritto d'autore, regime generale della protezione dei dati personali e regime speciale della protezione dei dati personali nelle comunicazioni elettroniche.

Se si sposa la visione qui proposta, in base alla quale la *privacy* nelle comunicazioni elettroniche merita una maggiore protezione rispetto alle attività di sorveglianza privata, allora la ricostruzione del rapporto tra i tre regimi può essere semplice.

Sul piano dei fatti delle controversie oggetto delle pronunce qui commentate permangono molte zone d'ombra. Da quel che risulta dalle narrative dei provvedimenti, imprese titolari di diritti d'autore su file musicali si servono della Logistep, impresa operante nel settore dell'informatica, per tracciare presunte attività illecite sulla rete Peer to Peer. L'esatto funzionamento dei software della Logistep e la tipologia dei dati trattati dalla stessa Logistep non sono chiari. Quel che sembra certo è che la Logistep traccia gli indirizzi IP ed i Globally Unique Identifier (GUID) da riconnettere alle utenze mediante le quali sono commesse le presunte attività illecite. La stessa Logistep pubblicizza le proprie attività su un sito Web, dichiarando di essere in grado di identificare più di due milioni (al giorno) di *upload* e *download* illegali su reti P2P. Essa dichiara inoltre di esser capace di tracciare la "storia" di ogni utente delle rete P2P senza essere vista dagli stessi utenti[21].

Le osservazioni che seguono si limiteranno alle implicazioni giuridiche della fattispecie di tracciamento degli indirizzi IP che costituisce il filo conduttore dei fatti oggetto dei provvedimenti su riportati e, più in generale, dell'attività di contrasto del *file sharing* illegale finalizzata a colpire i singoli utenti delle reti P2P.

Gli indirizzi IP sono – in base agli art. 2 della dir. 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e 4 lett. b) del d. lgs. 196/2003, codice in materia di protezione dei dati personali[22] – dati personali, in quanto consentono l'identificabilità della persona interessata.

L'art. 156-*bis* della legge n. 633 del 1941 sul diritto d'autore non fonda alcun diritto di procedere privatamente al tracciamento di massa di presunte attività illecite. Si tratta infatti di

[21] Sul sito della Logistep (http://www.logistepag.com/en/technologie.php) si legge: "by means of its "illogical network" (patent Pending), LOGISTEP fulfils a variety of tasks; which to date were only possible to complete with the use of enormous server capacity. A sole, specially developed server, which handles the entire process, is capable of identifying more than 2 million illegal down- and up-loads per day. The monitoring software used has already been evaluated by several IT experts and has been described as one of the most innovative procedures in the last years. In addition, a publicly sworn IT expert has rendered an expert opinion iro. of LOGISTEP's protocolled data. This certifies that all protocolled information is correct. Through the "illogical network" for IP filters systems, as for example Peer Guardian, LOGISTEP can not be detected. In full compliance with all relevant laws and regulations we produce a history for each user. IP Jumps, Firewalls or Proxy have no influence on the unambiguous identification of the users. The user identification in all P-2-P protocols is fully accurate".

[22] Si veda anche il Parere 2/2002 del Gruppo europeo dei garanti per la tutela dei dati personali (ex art. 29 Dir. 95/46 CE), sull'uso di identificativi esclusivi negli apparecchi terminali di telecomunicazione: l'esempio dell'IPv6, 10750/02/IT/def.WP 58, nel quale si legge a pag. 3: "[i]l gruppo mette in evidenza che gli indirizzi IP attribuiti agli utenti Internet costituiscono dati personali".

norma che riguarda sia la dimensione di Internet sia quella esterna alla rete e che parla solo della fase in cui si sono già acquisiti i "seri elementi" o "indizi" che occorre fornire al giudice quale presupposto della richiesta di ostensione di informazioni detenute da controparte.

Se questo diritto esiste, esso deve trovare fondamento nel d. lgs. 196/2003, codice in materia di protezione dei dati personali.

A quanto è dato rilevare dai provvedimenti in epigrafe, coloro che chiedono l'identificazione delle utenze pretendono di fondare il proprio diritto al trattamento degli indirizzi IP sull'art. 24 del codice in materia di protezione dei dati personali. L'art. 24 consente di prescindere dal consenso della persona interessata e di procedere al trattamento dei dati personali (con esclusione della diffusione) quando, tra l'altro, il trattamento sia finalizzato a "far valere un diritto in sede giudiziaria sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento"[23].

La norma esenta solo dall'acquisizione del consenso della persona interessata e non dagli altri presupposti per la liceità del trattamento.

In ogni caso, quand'anche siano rispettati tutti gli altri presupposti (tra i l'informativa *ex* art. 13 del codice in materia di protezione dei dati personali), la norma non autorizza al trattamento degli indirizzi IP. Tale conclusione si desume dalle cautele che circondano il regime speciale della *privacy* nell'ambito delle comunicazioni elettroniche.

In questo ambito, il principio fondante è fotografato dall'art. 121, in base al quale: "[…]è vietato l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente".

Si badi che la norma parla di fattispecie che non implicano necessariamente il trattamento dei dati personali. Dunque, in base a tale principio generale, qualsiasi monitoraggio delle operazioni dell'utente (compreso il tracciamento degli indirizzi IP) che avvenga senza il consenso di quest'ultimo deve ritenersi illecito.

Ovviamente il principio è limitato da una serie di eccezioni. Tra le quali, però, non figura la possibilità del monitoraggio nascosto, e dunque senza il consenso informato delle persone interessate, degli indirizzi IP a scopi di indagine privata relativa ad illeciti.

Il trattamento degli indirizzi IP rientra nel trattamento dei "dati relativi al traffico". La norma cardine della disciplina del trattamento (l'art. 123 del codice in materia di protezione dei dati personali) stabilisce che tali dati "sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica". Sono fatte salve una serie di ipotesi in cui è lecita la conservazione di alcuni tipologie di dati ("dati relativi al traffico strettamente necessari a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione", "dati relativi

[23] Sul punto cfr. le osservazioni di Guido Scorza a margine dei provvedimenti qui commentati in *Diritto dell'Internet*, 2007.

al traffico telematico, esclusi comunque i contenuti delle comunicazioni") per alcune finalità ("a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento", "per finalità di accertamento e repressione dei reati", "per esclusive finalità di accertamento e repressione dei delitti di cui all'articolo 407, comma 2, lettera a) del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici") e per periodi limitati di tempo.

Si tratta, evidentemente, di una disciplina severa in ragione della natura dei dati. Il trattamento dei dati relativo al traffico è consentito solo ad alcuni soggetti, solo per alcune finalità e solo per periodi limitati di tempo. La natura speciale della disciplina delle comunicazioni elettroniche rende inapplicabile la norma generale dell'art. 24, con la conseguenza che il tracciamento degli indirizzi IP ed il monitoraggio nascosto delle attività degli utenti delle reti P2P devono considerarsi attività illecite che non possono essere poste alla base di un'azione *ex* art. 156-*bis* della legge n. 633/1941. In particolare, l'illecito trattamento degli indirizzi IP comporta l'applicazione del comma 2 dell'art. 11 del codice in materia di protezione dei dati personali secondo il quale "i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati"[24].

6. Conclusioni

Ad una prima superficiale impressione, il quadro legislativo statunitense relativo alla materia delle reti P2P sembra andare verso una scala di valori che antepone la tutela del *copyright* alla tutela della *privacy* e della libertà di pensiero. Questa scala di valori non è giustificata dal mutamento indotto dalle tecnologie digitali nel campo della proprietà intellettuale, della *privacy* e della libertà di pensiero. La potenza delle tecnologie digitali minaccia (e protegge) non solo la proprietà intellettuale, ma anche la *privacy* e la libertà di manifestazione del pensiero. Un quadro legislativo corretto deve porre i tre settori almeno sullo stesso piano. Inoltre, le difficoltà che l'*enforcement* statale incontra nella dimensione di Internet non giustificano la totale dismissione di funzioni delicate fondamentali della tutela giuridica come quelle che concernono l'identificazione dei soggetti che violano la legge.

Se correttamente interpretato, l'attuale assetto dell'ordinamento italiano delinea un maggiore equilibrio tra tutela del diritto d'autore e protezione dei dati personali. In particolare, il sistema giuridico italiano non lascia spazio ad un'attività di sorveglianza privata invasiva della *privacy* degli utenti delle reti P2P, cioè basata sul monitoraggio nascosto delle attività degli utenti ed in particolare sul tracciamento massivo, senza il consenso informato delle persone interessate, degli indirizzi IP.

La tendenza alla privatizzazione della tutela della proprietà intellettuale su Internet sembra, peraltro, una deriva che comporta enormi costi sociali senza (forse) apportare i benefici (privati e sociali) sperati. Molti (e fra questi, le stesse multinazionali dell'intrattenimento) sostengono che il fenomeno del *file sharing* illecito non registri una flessione. A dispetto di strategie di difesa della proprietà intellettuale tanto aggressive, il comportamento delle masse sembra muoversi nella

[24] V. i rilievi di Guido Scorza sui provvedimenti in epigrafe in *Diritto dell'Internet*, 2007.

convinzione dell'impunità o della liceità. C'è da chiedersi seriamente se non sia il caso di dare ascolto a quelle voci che da alcuni anni propongono alternative alla contrapposizione frontale tra titolari e fruitori della proprietà intellettuale puntate a rendere lecito lo scambio di opere protette e, nello stesso tempo, a retribuire i titolari dei diritti[25]. L'esplorazione di tali alternative, se non altro, è suggerita da una dato di fatto incontestabile: le tecnologie sulle quali è stato edificato più di cinquecento anni fa il commercio dei diritti d'autore non sono quelle che dominano la dimensione virtuale dei nostri giorni.

Arroccarsi dietro mura tanto alte e spesse da apparire invalicabili non serve a nulla. Il tuono di nuovi cannoni pronti a sbriciolarle rimbomba all'orizzonte.

[25] V., fra gli altri, N. W. NETANEL, *Impose a Non Commercial Use Levy to Allow Free Peer-to-Peer File Sharing*, 17 *Harv. J.L & Tech.* 1 (December 2003), disponibile su SSRN all'URL: «http://ssrn.com/abstract=468180».