TRIBUNALE ROMA
ORDINANZA
16 LUGLIO 2007
GIUDICE: COSTA
PARTI: TECHLAND SP.ZO.O.
PEPPERMINT JAM RECORDS GMBH
WIND TELECOMUNICAZIONI S.P.A.
GARANTE PROTEZIONE DATI PERSONALI

Diritti d'autore sulle opere di ingegno (proprietà intellettuale) • Artt. 156 e 156-*bis*, L. 633/41 • Applicabilità a dati relativi a comunicazioni elettroniche • Esclusione • Tutela della privacy • Codice in materia di protezione dei dati personali • Sussistenza nella fattispecie della scriminante *ex* art. 24, D.Lgs. 196/2003 • Esclusione • Fattispecie: condivisione di musica in reti *peer-to-peer*

*Il combinato disposto degli artt. 156 e 156-*bis *L.A. non può ritenersi applicabile ai dati ed alle informazioni che attengono alle comunicazioni* lato sensu *elettroniche, né ai dati di traffico da queste prodotte, ostando a tale estensione applicativa il divieto di trattamento e comunicazione enucleabile dal sistema normativo interno (primario e costituzionale) e comunitario che disciplina la materia della tutela della segretezza e riservatezza delle comunicazioni tra privati. né è applicabile la scriminante di cui all'art. 24, D.Lgs. 196/2003 in quanto da un lato la norma presuppone che il dato personale utilizzato dal terzo senza il consenso dell'interessato sia già in possesso dell'utilizzatore (mentre nel caso di specie sono oggetto della richiesta di esibizione), dall'altro che tale possesso sia legittimo (laddove, invece, nel caso di specie i codici IP e GUID sono stati illecitamente acquisiti in violazione degli artt. 37, 13 e 23, D.Lgs. 196/2003).*

Il G.d.,
letto il ricorso cautelare presentato dalla Techlands sp. Z o.o. e dalla Peppemint Jam Records GmbH nei confronti della Wind Telecomunicazioni s.p.a., avente ad oggetto la richiesta di comunicazione ed ostensione dei dati anagrafi ci necessari all'identificazione degli autori della violazione del diritto d'autore di cui le stesse erano titolari. e ciò in relazione all'illecita condotta di scambio e condivisione di *files* musicali e giochi elettronici dagli stessi operata mediante la rete *peer to peer* su *internet*, in considerazione del fatto che la Wind Telecomunicazioni s.p.a., in quanto *provider* per l'accesso a *internet*, aveva fornito a detti soggetti i servizi necessari di connessione al sistema informatico utilizzato per la violazione di detto diritto, ed era dunque in possesso delle complete generalità di tali soggetti;

lette le memorie di costituzione della resistente Wind Telecomunicazioni s.p.a. e del Garante per la protezione dei dati personali, intervenuto nel procedimento cautelare, e le contestazioni rispettivamente sollevate all'istanza cautelare in questione, di cui chiedevano la reiezione;

visti gli atti e documenti del procedimento;

sentiti i procuratori delle parti costituite;

sciogliendo la riserva assunta all'udienza del 31 maggio 2007.

OSSERVA. — Le società ricorrenti deducevano di aver rilevato sulla rete *internet*, e segnatamente sulla rete *peer to peer*, un'attività di scambio abusiva di specifici *files* musicali e *files* di giuochi elettronici con

omissione del pagamento dei diritti d'autore relativi alle opere dell'ingegno oggetto di tale attività di scambio in rete, diritti spettanti ad esse esponenti per i predetti *files*. Di conseguenza, sul presupposto della violazione del diritto d'autore, invocavano l'applicabilità dello speciale strumento processuale, per la tutela dell'anzidetto diritto, previsto dall'art. 156-*bis* della L. 633/41 (L.A.), in forza del quale il titolare di un diritto d'autore leso può chiedere ed ottenere, anche da soggetti diversi dagli autori della violazione, la comunicazione dei dati e delle informazioni necessarie all'individuazione dei responsabili della lesione del diritto, e ciò in quanto norma di attuazione della direttiva comunitaria 2004/48/CE (c.d. direttiva *enforcement*) per la portata applicativa della quale doveva farsi esclusivo riferimento interpretativo ai contenuti di detta direttiva che prevedeva espressamente l'applicabilità della disciplina anche a soggetti non coinvolti nella condotta illecita. Nel caso di specie, la qualità di *provider* avuta dalla Wind Telecomunicazioni s.p.a. (fornitrice del servizio di accesso ad *internet*), in relazione ai soggetti responsabili della violazione dei citati diritti, la rendeva controparte dello speciale procedimento di esibizione dei dati in parola rispetto ai propri clienti protagonisti dell'abusiva attività di scambio di *files*, dunque soggetto passivo dell'istanza cautelare in discorso. Peraltro, i dati necessari all'identificazione di detti soggetti erano stati acquisiti dalla società Logistep (su incarico di esse ricorrenti) mediante l'ausilio di un programma informatico per la rilevazione degli indirizzi elettronici degli stessi denominati codici IP e GUID, dai quali solo il *provider* poteva desumere con certezza alle esatte generalità dei titolari dell'utenza corrispondente a detti codici. Tali dati, infatti, erano stati acquisiti operando nella rete *peer to peer* e simulando l'attivazione di contatti per lo scambio di *files* col sistema della condivisione (c.d. *file sharing*), a mezzo dei quali contatti potevano rilevare gli indirizzi telematici dei medesimi poi risultati utenti di Wind Telecomunicazioni s.p.a. Siffatte informazioni telematiche costituivano, pertanto, il supporto indiziario richiesto dall'art. 156-*bis* L.A., ossia i « seri clementi », per la valutazione della fondatezza della domanda ai fini dell'accoglibilità dell'istanza di esibizione, non ostando all'accoglimento i limiti previsti dalla normativa a tutela della riservatezza delle comunicazioni, di cui al D.Lgs. 196/2003, in virtù dell'art. 24 di tale testo normativo che consentiva l'uso dei dati personali senza il consenso del titolare allorché tale dato risultava necessario a far valere un diritto in giudizio. dovendosi a tale fine ricomprendere in detta formulazione normativa anche l'esercizio delle azioni civili, di talché nel caso di specie ricorrevano tutti i requisiti per ottenere l'ostensione dei dati richiesti.

La Wind Telecomunicazioni s.p.a., costituendosi nel giudizio cautelare, contestava la fondatezza ed ammissibilità dell'istanza delle ricorrenti e ne chiedeva la reiezione per la mancanza dei presupposti processuali e sostanziali di ammissibilità ed accoglibilità dell'istanza di esibizione. ln particolare, in ordine al *fumus boni iuris*, rilevava:

— che la comunicazione dei dati personali chiesti dalle ricorrenti poteva essere disposta (solo dal pubblico ministero), in base all'art. 132 del D.L. 27 luglio 2005, n. 144 (c.d. decreto Pisanu) per un arco di tempo limitato e in relazione alla repressione di specifiche ipotesi di reato (di cui all'art. 407, II comma lett. *a*) c.p.p., ed in danno ai sistemi informatici). Dunque, non sussisteva alcuna possibilità di ottenere tali dati per altri

fini, ivi compresi quelli dedotti dalle ricorrenti, trattandosi di norme speciali non applicabili in via analogica o estensiva, come anche affermato dalla stessa autorità Garante della privacy con provvedimeto del novembre 2005;

— che gli artt. 156 e 156-*bis* L.A. non consentivano la tutela cautelare ma solo quella di merito, non contenendo tali norme alcun riferimento a tale tipo di tutela anticipatoria, inoltre le stesse norme non erano suscettibili di applicazione nei confronti degli intermediari, posto che solo l'art. 163 L.A. consentiva l'azione verso l'intermediario per provvedimenti a contenuto meramente inibitorio, e sul presupposto di una sua implicazione e partecipazione alla lesione del diritto d'autore, condizione nella specie non ravvisabile in capo ad essa esponente essendosi limitata a fornire l'accesso ad *internet* senza possibilità o dovere di controllo del contenuto delle comunicazioni trasmesse dagli utenti del servizio;

— che in ordine ai dati identificativi richiesti col ricorso esisteva un'impossibilità giuridica di trattamento, come disposto dal titolo X del D.Lgs. 196/2003, e di conseguenza essa esponente non poteva essere obbligata all'ostensione di tali informazioni in quanto tale normativa (art. 123) prevede l'obbligo del fornitore del servizio telematico di cancellazione e rendere anonimi tali dati, derivandone, quindi, una sorta di impossibilità giuridica all'ostensione dei medesimi giustificata, come osservato dalla Corte Costituzionale, dall'esigenza di armonizzare interessi contrapposti di rango costituzionale, quali quello alla riservatezza e la tutela della collettività di fronte a reati di particolare gravità, laddove nel caso delle ricorrenti venivano in evidenza situazioni soggettive meramente privatistiche prive di rilevanza costituzionale;

— che i dati raccolti dalle ricorrenti, ossia gli indirizzi IP e GUID, erano inutilizzabili perché acquisiti illecitamente in violazione della normativa sulla tutela della riservatezza, non potendosi avvalere le ricorrenti della deroga prevista dall'art. 24 del D.Lgs. 196/2003 (ossia non necessità del consenso dell'interessato quanto il dato è strumentale a far valere un diritto in giudizio), poiché il consenso dell'interessato all'utilizzazione per fini processuali dei dati personali, come previsto da tale norma, doveva comunque essere « espresso ed informato », e non comprendeva anche il trattamento dei dati nella fase acquisitiva degli stessi, come viceversa fatto dalle odierne ricorrenti con l'incarico alla società Logistep, risoltosi di fatto nell'acquisizione di dati personali senza il consenso degli interessati nei confronti di migliaia di soggetti inserendosi nella rete *peer to peer*, e simulando di essere un fruitore dei servizi, analogamente al *modus operandi* dell'agente provocatore. Oltre tutto, sussisteva l'ulteriore impedimento alla loro utilizzazione per via dell'acquisizione dei dati avvenuta in territorio svizzero;

— che gli elementi documentali prodotti dalle ricorrenti (c.d. moduli) non poteva costituire la base dei « seri elementi » richiesti dall'art. 156-*bis* L.A., trattandosi di elementi non riscontrabili oggettivamente in ordine alla loro attendibilità (come rilevabile dalla perizia dell'ing. Zimmermann, in punto di incertezza e mutabilità dei codici IP e GUID), e unilateralmente precostituiti dalla parte interessata, sicché pur non necessitando per tale azione di esibizione di prove in senso tecnico processuale, nemmeno poteva interpretarsi la citata disposizione in senso opposto tanto da elidere l'onere probatorio ordinariamente richiesto dal nostro sistema processuale a carico della parte;

— che le ricorrenti non avevano dato prova della titolarità effettiva del diritto d'autore sulle opere asseritamente oggetto di scambio sulla rete *peer to peer*, sia perché non era certo che tali opere rispondessero ai requisiti di novità ed originalità, sia perché non era certo che, nel caso, le opere fossero state riprodotte interamente ed utilmente.

Quanto invece all'inesistenza del *periculum in mora* osservava:

— che le condotte lamentate dalle ricorrenti erano state lungamente tollerate dalle stesse, dunque non si conciliavano con l'urgenza di provvedere in via cautelare, né tale urgenza poteva ascriversi all'impossibilità di conseguire l'integrale risarcimento dei danni, ovvero la loro esatta quantificazione, atteso che il controllo e monitoraggio delle condotte medesime dipendeva unicamente dalla diligenza ed iniziativa delle ricorrenti volte a procurarsi i dati per perseguire tali eventuali illeciti. Infine, non era ravvisabile alcun rischio di reiterazione proprio perché condotte concretamente tollerate dalle dirette interessate per lungo tempo, né poteva sussistere il pericolo di sviamento della clientela, ravvisandosi al più una riduzione delle vendite delle copie delle opere, integrante un danno pacificamente quantificabile.

Interveniva nel giudizio cautelare il Garante per la Protezione dei dati personali col patrocinio dell'avvocatura erariale, che in ordine alle problematiche sulla tutela della riservatezza investite dall'oggetto del ricorso cautelare svolgeva, in senso critico e di contestazione del ricorso, ritenendo, in sintesi, che il trattamento dei dati personali relativi alle connessioni dei servizi telematici della c.d. società dell'informazione rimaneva circoscritto e limitato alle sole indagini penali condotte da autorità pubbliche direttamente preposte alla sicurezza e difesa nazionale, e che ogni diversa soluzione contrastava con i diritti fondamentali alla riservatezza e segretezza delle comunicazioni, come affermato e garantito dai principi costituzionali e del diritto comunitario, oltre che dalla Convenzione europea dei diritti dell'uomo. In buona sostanza, osservava che la compressione di tali diritti poteva avvenire, con connotati di proporzionalità, solo in relazione alla salvaguardia di beni giuridici di superiore valore tutelati dalla normativa penale. Sicché non poteva trovare accoglimento l'istanza cautelare delle ricorrenti, giacché fondata su beni di minore rilevanza e protezione giuridica rispetto a quello della segretezza delle comunicazioni. Svolgeva, quindi, le seguenti argomentazioni:

— la direttiva 2002/58/CE, in materia di trattamento dei dati personali, imponeva agli Stati la protezione e la riservatezza delle comunicazioni elettroniche e vietava la conservazione dei relativi dati di traffico (nel cui ambito si annoverava anche l'indirizzo IP e i dati anagrafici degli utenti), fatta eccezione per le finalità di prevenzione e perseguimento dei reati, quindi con esclusione degli illeciti civilistici, inoltre nel concetto di trattamento vi rientrava anche l'estrazione dei dati di traffico dalle banche dati dei fornitori dei servizi, nonché la raccolta e comunicazione degli stessi (art. 5 par. 1);

— la direttiva 2004/48/CE, in materia di protezione della proprietà intellettuale, pur disponendo il principio di tutela per tali diritti, con estensione all'obbligo di fornire informazioni sull'origine e distribuzione di merci e servizi lesivi del diritto anche a soggetti diversi dall'autore della violazione, faceva salve le limitazioni contenute nelle disposizioni normative a protezione della riservatezza ed il trattamento dei dati personali, di conseguenza queste ultime prevalevano, per scelta del legislatore comunitario, sui diritti di proprietà intellettuale;

— la direttiva 2001/29/CE, in materia di diritto d'autore e diritti a questo connessi, prevedeva la possibilità di rimedi giurisdizionali a protezione del diritto d'autore consistenti in un provvedimento inibitorio ove l'azione sia rivolta al terzo, di talché nel caso di specie tale direttiva non poteva trovare applicazione, inoltre la stessa direttiva in parola conteneva (art. 9) l'espressa salvezza delle altre disposizioni, tra cui vi rientrava certamente quella sulla protezione dei dati personali;

— il D.Lgs. 196/2003 (cod. priv.) riproduceva gli stessi limiti posti dalla direttiva 2002/58/CE sopra citata, nel senso di vietare sostanzialmente ogni forma di conservazione e trattamento dei dati personali e di traffico delle comunicazioni elettroniche, fatta eccezione per la repressione e prevenzione di fatti penalmente rilevanti, contemplati dall'art. 407, II comma, lett. *a*) c.p.p. e quelli in danno dei sistemi informatici, bilanciamento ribadito anche dalla Corte Costituzionale con sentenza 372/2006 in relazione all'art. 132 cod. priv. Inoltre, il fornitore dei servizi doveva considerarsi incaricato di pubblico servizio e dunque tenuto all'obbligo del segreto d'ufficio *ex* art. 201 c.p.p., con inevitabile ostacolo giuridico all'ordine di esibizione *ex* art. 210 c.p.c. nei confronti dello stesso, di modo che non poteva avere pregio la tesi sostenuta dalle società ricorrenti della possibilità di prescindere dal consenso dell'interessato, *ex* art. 24, I comma, lett. *f*) cod. priv., anche nel caso di specie;

— in base alla stessa normativa interna, i dati personali raccolti e trattati dalle ricorrenti per la proposizione del presente procedimento cautelare dovevano ritenersi illecite perché conseguiti in violazione dei limiti posti dal D.Lgs. 196/2003, e in particolare l'attività di monitoraggio svolta dalle ricorrenti per opera della Logistep doveva essere preventivamente autorizzata dall'esponente Garante *ex* art. 37 cod. priv. oltre che dal diretto interessato *ex* art. 13 cod. priv., e tali omissioni rendevano illecita la condotta delle stesse, da cui conseguiva *ex* art. 11 cod. priv. l'inutilizzabilità dei dati cosi raccolti per ogni ulteriore trattamento;

— gli artt. 156 e 156-*bis* L.A. invocati dalle ricorrenti dovevano essere interpretati alla luce dei principi generali dell'ordinamento, quindi in considerazione dei principi Costituzionali dettati dagli artt. 2 e 15 Cost. in materia di riservatezza e segretezza delle comunicazioni, diritti comprimibili solo in presenza di valori collettivi ritraibili dalla normazione penale e non anche dal sistema di tutela dei diritti privatistici, di modo che non sussisteva alcun conflitto di norme tra siffatte disposizioni a tutela del diritto d'autore e gli artt. 123 e 132 cod. priv.

MOTIVI. — Alla luce delle difese ed eccezioni nuove svolte nel presente procedimento cautelare, rispetto a precedenti casi analoghi esaminati da questo Tribunale, anche in composizione collegiale, e ciò in considerazione anche della significativa costituzione volontaria dell'autorità Garante per la privacy, deve ritenersi l'infondatezza dell'istanza cautelare in esame.

La questione assolutamente assorbente e decisiva sottoposta all'esame del Tribunale è rappresentata invero dall'estensione del campo di applicazione della norma invocata dalle odierne ricorrenti per l'esibizione dei dati identificativi dei soggetti asseritamente autori della violazione del diritto d'autore. Infatti, l'art. 156-*bis* L.A., diretta espressione della direttiva comunitaria 2004/48/CE (cosiddetta direttiva *enforcement*) ad un primo esame si presta senza dubbio ad una possibile interpretazione estensiva,

sì da ricomprendere nel campo di applicazione della norma qualunque tipo di informazioni anche se detenute da un soggetto terzo non implicato nella violazione del diritto d'autore, e ciò proprio perché la direttiva sopra citata contempla espressamente la possibilità di estensione della richiesta dei dati anche ai soggetti diversi dagli autori della violazione che — in sintesi — abbiano fornito a questi servizi strumentalmente usati per compiere l'illecito. La stessa direttiva comunitaria enuncia la salvezza dei regolamenti esistenti a tutela della riservatezza e segretezza delle comunicazioni, sicché in base a detto inizialmente inquadramento della disciplina della fattispecie in esame le ricorrenti hanno (anche in precedenti ed analoghi procedimenti cautelari) hanno desunto la possibilità di applicazione della norma nei confronti dei *provider* per ottenere le informazioni necessarie all'identificazione degli autori della violazione del diritto d'autore, sul presupposto che tali soggetti intermediari del servizio di accesso a *internet* per i propri clienti avevano i dati richiesti e il servizio prestato era risultato strumentale alla condotta illecita.

La tesi qui esposta e sostenuta dalle ricorrenti non può accogliersi.

Il combinato degli artt. 156 e 156-*bis* L.A., ma anche quest'ultima norma singolarmente considerata, non può ritenersi estensibile come campo di applicazione ai dati ed informazioni che attengono alle comunicazioni *lato sensu* elettroniche, né ai dati di traffico da queste prodotte, ostando a tale estensione applicativa il divieto di trattamento e comunicazione di tali dati enucleabile in sintesi dal sistema normativo interno (primario e costituzionale) e comunitario che disciplina la delicata materia della tutela della segretezza e riservatezza delle comunicazioni tra privati. Infatti, dall'esame complessivo di tale articolata disciplina, oltre al citato divieto assoluto di trattamento, emerge come unica eccezione a tale divieto l'uso e la comunicazione dei dati relativi alle comunicazioni solo per la tutela di valori di rango superiore e che attengono alla difesa di interessi della collettività ovvero alla protezione dei sistemi informatici, di conseguenza l'eccezione al divieto di trattamento dei dati è ristretto a specifiche ipotesi delittuose senza alcun altra possibilità di estensione a ipotesi diverse da queste. In particolare, si ricava l'impossibilità di utilizzazione e trattamento di tali dati per ragioni di carattere contenzioso civile, come viceversa sostenuto dalle odierne ricorrenti sulla base dell'art. 24, I comma, D.Lgs. 196/2003. Tale norma, infatti, consente l'uso di dati personali senza il consenso del medesimo ove gli stessi siano strumentali a far valere un diritto in giudizio, il che evidentemente comprende per definizione il contenzioso civile, dato che solo e propriamente in tale ambito trova espressione naturale la tutela dei diritti soggettivi, tuttavia la norma presuppone che il dato personale utilizzato dal terzo senza il consenso del diretto interessato sia già in possesso dell'utilizzatore e, sopra tutto, che tale possesso sia avvenuto legittimamente.

Nel caso di specie si verte in una diversa ipotesi da quella invocata dalle ricorrente con riferimento all'art. 24 citato, giacché la fase in cui si verte è ben anteriore all'utilizzazione dei dati personali, posseduti legittimamente, avendo al contrario ad oggetto proprio la richiesta di acquisizione del dato personale, di modo che si tratta di un ambito logicamente e temporalmente anteriore rispetto all'ipotesi contemplata dall'art. 24, sicché la norma richiamata non può costituire valida base argomentativa della presente richiesta di esibizione dei dati personali. A ciò deve aggiungersi che il possesso dei dati parziali avuto dalle ricorrenti sui presunti autori

delle violazioni lamentate, ossia i codici IP e GUID, sempre in virtù della disciplina dettata dal D.Lgs. 196/2003 risulta illecito, trattandosi di dati acquisiti in assenza di autorizzazione dell'autorità Garante per la privacy (in base all'art. 37) e del consenso informato dei diretti interessati (art. 13 e 23). Dunque, la norma dell'art. 24 D.Lgs. 196/2003 non può operare in senso favorevole alle ricorrenti per entrambi i motivi testè illustrati, con l'ulteriore rilievo che la connotazione illecita dell'acquisizione dei citati codici IP e GUID da parte delle ricorrente determina la completa inutilizzabilità di tali dati anche in sede giudiziale ai sensi dell'art. 11, II comma, del medesimo decreto, sicchè gli stessi non possono costituire la base indiziaria (seri elementi) richiesta dall'art. 156-*bis* L.A. per la valutazione del Giudice in ordine alla fondatezza della domanda, e ciò rappresenta esso stesso un elemento ostativo per l'accoglimento dell'istanza cautelare in esame in quanto, in base alle specifiche norme richiamate (artt. 13, 23 e 37 D.Lgs. 196/2003), le ricorrenti non potevano compiere le attività di acquisizione e conservazione (quindi il trattamento) dei dati posti dalle stesse a fondamento della richiesta cautelare, quali « seri elementi » di prova della fondatezza della domanda.

Pur risultando detto aspetto autonomamente ostativo all'accoglimento dell'istanza cautelare, non di meno deve rilevarsi come la questione fondamentale dell'infondatezza di tale pretesa sia rappresentata dall'anzidetto limite della segretezza delle comunicazioni elettroniche e telematiche tra privati, quale diretta espressione di tutela di interessi di rilevanza Costituzionale (art. 2 e 15 Cost.), che la normativa esistente consente di superare solo in funzione della tutela di valori ed interessi della collettività con eguale e superiore rilevanza Costituzionale, e sempre in un'ottica di equilibrio e comparazione. Infatti, l'unica possibilità ammessa di compressione di tali diritti personalissimi è quella strumentale all'accertamento, prevenzione e repressione di illeciti penali di particolare gravità, ossia quelli previsti dall'art. 407, II comma lett. *a*) del c.p.p. (delitti associativi con finalità di terrorismo, di tipo mafioso ecc., e delitti per i quali è previsto l'arresto obbligatorio in flagranza, giacché puniti con pena detentiva superiore, nel minimo, ad anni cinque di reclusione) e quelli in danno di sistemi informatici.

Tale limite si trae, come detto, dal complesso sistema normativo comunitario e nazionale, in base ai contenuti delle direttive in materia di protezione e segretezza delle comunicazioni elettroniche, e della tutela del diritto d'autore (*enforcement*) che fa salva la precedente normativa per la tutela della riservatezza e protezione dei dati personali. In particolare, gli artt. 8 e 9 della direttiva 2004/48/CE (sui diritti di proprietà intellettuale) enunciano la necessità di adozione — da parte degli Stati — di normative volte alla tutela di tali diritti, e la possibilità di ottenere dall'autore della violazione informazioni sull'origine e reti di distribuzione, ovvero dai terzi che abbiano fornito servizi utilizzati per commettere la violazione, non di meno la stessa direttiva (art. 8 par. 3) fa salva tutta la normativa regolamentare sulla protezione, riservatezza e protezione dei dati personali, di talché non può evincersi dalla direttiva invocata dalle ricorrenti, sulla protezione del diritto d'autore, una base interpretativa di tale portata rispetto all'ampiezza dell'art. 156-*bis* L.A. tale da ricomprendere anche l'esibizione dei dati personali in questione, proprio perché la protezione di tali dati è fatta salva, con espresso rinvio, dalla medesima direttiva. Per altro verso, la direttiva 2002/58/CE, sulla protezione dei dati personali nelle co-

municazioni elettroniche, pone espressi divieti di conservazione dei dati di traffico delle comunicazioni, e nel contempo indica essa stessa le ipotesi derogatorie — in via di eccezioni non estensibili in via interpretativa — a tale divieto, che attengono in via esclusiva alla sicurezza dello Stato, alla difesa, alla pubblica sicurezza, alla prevenzione, ricerca, accertamento e repressione di reati, come disposto dall'art. 15 della citata direttiva.

La prevalenza sulla riservatezza, quale valore fondamentale della persona, è stata recentemente ribadita dalla Corte Costituzione con la sentenza 372/2006 in relazione alla legittimità costituzionale dell'art. 132 D.Lgs. 196/2003 ed alla possibilità di conservazione dei dati di traffico delle comunicazioni tra privati per un tempo maggiore rispetto a quello previsto dalla stessa norma, ritenendo la legittimità della norma in considerazione della necessità del contemperamento e bilanciamento del diritto alla riservatezza solo per esigenze di tutela di beni della collettività prevalenti minacciati dai gravi illeciti penali.

Tutto ciò esclude, quindi, la possibilità di applicazione dell'art. 156-*bis* L.A. e dell'art. 24 del D.Lgs. 196/2003 al trattamento dei dati personali relativi alle comunicazioni elettroniche e telematiche tra privati per finalità connesse alla tutela dei diritti soggettivi dei privati.

Consegue, da ciò, il rigetto del ricorso cautelare in premessa.

La complessità e particolarità della fattispecie in esame consente la completa compensazione delle spese del procedimento.

P.Q.M. — Il Tribunale, definendo il procedimento cautelare, così provvede:

1. rigetta il ricorso cautelare proposto dalla Techlands sp. Z.o.o. e dalla Peppermint Jam Rccords GmbH nei confronti della Wind Telecomunicazioni s.p.a.;

2. compensa integralmente le spese del procedimento cautelare tra tutte le parti costituite.

IL CASO « PEPPERMINT »: IL PREVEDIBILE CONTRASTO TRA PROTEZIONE DEL DIRITTO D'AUTORE E TUTELA DELLA PRIVACY NELLE RETI PEER-TO-PEER

1. IL CASO.

Nel corso del mese di maggio 2007, migliaia di cittadini italiani hanno ricevuto una raccomandata, inviata da uno studio legale di Bolzano: in nome e per conto di una piccola casa discografica tedesca, la Peppermint Jam Records GMbH, i legali chiedono la cancellazione di alcuni *file* contenenti brani musicali di artisti di cui la Peppermint detiene i diritti di sfruttamento del diritto d'autore. Tali brani sarebbero stati messi a disposizione di altri utenti di *internet* attraverso programmi di *file sharing* senza autorizzazione alcuna e dunque in violazione dei diritti esclusivi; per tale illecito viene richiesto il versamento, a titolo di « *parziale risarcimento per danni, spese legali e spese tecniche sostenute per l'individuazione* », della somma forfetaria di euro 330,00.

In difetto vengono minacciate azioni sia in sede civile che penale.

Dalla lettura della missiva si evince come la Peppermint abbia dato incarico ad una società svizzera, la Logistep AG[1], affinché con un apposito *software* (definito antipirateria) raccogliesse e registrasse alcuni dati relativi ad utenti connessi in rete, rei, a loro dire, di effettuare attività di condivisione in reti P2P di opere tutelate in violazione del diritto di cui all'art. 16 L.d.A.

In particolare, risultano esser stati oggetto di trattamento, quanto meno, data e ora di connessione dell'utente alla rete, suo indirizzo IP e nome del *file* condiviso.

Il meccanismo di funzionamento del *software* antipirateria utilizzato dalla Logistep AG pare un sintesi il seguente: il *software* si inserisce nella rete e registra gli indirizzi IP degli utenti connessi ad un programma di *file sharing* (quali utenti? Tutti? Solo quelli che condividono file musicali degli artisti prodotti dalla Peppermint? Solo quelli che condividono o anche quelli che scaricano?), registrandone i relativi dati (indirizzo IP, data e ora della connessione, *file* condiviso) su di un'apposita banca dati, a sua volta gestita da un altro *software*.

Sulla base di tali dati la Peppermint, per individuare i destinatari delle missive, presentava diversi ricorsi *ex* art. 156-*bis*, L.d.A., nei confronti dei diversi ISP cui facevano capo le utenze « intercettate » al fine di ottenere ordini di esibizione dei dati anagrafici dei titolari degli indirizzi IP.

Inizialmente il Tribunale di Roma accoglieva i ricorsi, in particolare con le due ordinanze in commento emesse in data 19 agosto 2006 e 1 marzo 2007; successivamente, in data 16 luglio 2007, con pronuncia contraria, lo stesso Tribunale rigettava identico ricorso della Peppermint Jam Records GmbH e della Techland sp. Z.o.o. (società polacca produttrice di videogiochi).

Il netto contrasto giurisprudenziale parrebbe trovar ragione, a fronte di identici ricorsi ed identica autorità giudicante, nella costituzione in giudizio dell'Autorità Garante per la protezione dei dati personali, intervenuta per la prima volta nel procedimento conclusosi con l'ordinanza 16 luglio 2007.

La vicenda ha in vero dimensioni transnazionali: l'attività della Logistep AG è stata utilizzata per azioni in vari paesi (tra gli altri Spagna, Francia, Germania) e pare esser in Europa il primo vero tentativo di reazione nei confronti della condivisione di opere protette con sistemi P2P da parte dei titolari di diritti connessi al diritto d'autore.

Le problematiche ad essa sottese sono molteplici: oltre le ormai consuete tensioni legate ai difficili equilibri che le leggi sul Diritto d'Autore dovrebbero presidiare (titolarità ed esercizio del diritto dell'autore e del produttore da un lato e il diritto alla diffusione e fruizione delle opere dell'ingegno e della cultura dall'altro) la vicenda rende concreti alcuni timori da più parti sollevati circa l'attuale deriva della normativa volta ormai a tutelare più degli Autori, i titolari di diritti connessi.

---

[1] Società investigativa specializzata nell'antipirateria, partner, guarda caso, dello studio legale firmatario della missiva che tutela gli interessi della Peppermint! Cfr., *http://www.antipirateria.it/Ital/Chi%20siamo.html* (così al 16 ottobre 2007).

Tali diritti prettamente commerciali, che « connessi » son solo più di nome, sono talvolta in contrasto con gli interessi degli Autori stessi[2] ed hanno assunto nelle attuali normative una valenza preponderante che snatura ed infrange gli equilibri originari del Diritto, detto appunto, d'Autore[3].

In questa deviata prospettiva, la concreta applicazione della 2004/48/CE — cd. direttiva *enforcement* 1 — come emerge sul piano europeo con il caso Logistep AG, evidenzia i rischi di una privatizzazione dell'indagine e la intollerabile forzatura ad azioni cautelari a fini meramente investigativi o, peggio, lucrativi.

La vicenda, figlia della cosiddetta società della tecnica e dell'informazione, vede la tanto criticata legge sulla protezione dei dati personali ergersi come valido e necessario baluardo a tutela dei cittadini, siano essi fruitori o meno di opere dell'ingegno (ma in verità non è ipotizzabile oggi non fruire di opere tutelate!).

Mai come nel caso ormai noto come « Peppermint » è emersa in concreto l'importanza e la necessità di efficaci norme a tutela della riservatezza ed una rigorosa vigilanza da parte dell'Autorità Garante per la protezione dei dati personali.

D'altra parte, merita riflessione il fatto che tanto l'attuale criticabile normativa sul Diritto d'Autore (frutto di caotiche e frequenti modifiche della vecchia L. 633/1941) quanto il Codice Privacy trovino oggi nella sorprendente evoluzione tecnologica legata al digitale ed all'informatica la loro primaria ragion d'essere.

Se però il diritto alla riservatezza si è trasformato con chiarezza dal « *right to be alone* » al diritto alla protezione dei dati personali[4], non così chiara appare l'evoluzione del diritto d'autore, e la vicenda « Peppermint » ne è prova.

L'intreccio delle due normative, in virtù della loro attuale comune « ragion d'essere » nell'informatica e nella digitalizzazione dei dati, era stato per altro da tempo evidenziato da attenta dottrina proprio per l'utilizzo della rete Web ed in particolare per i sistemi *peer-to-peer* ed ha trovato di recente una concreta, sebbene preoccupante, applicazione nella giurisprudenza americana[5].

Il caso « Peppermint » è dunque emblematico.

---

[2] A riprova di quanto affermato basta leggere il manifesto della Canadian Music Creators' Coalition, che raccoglie i più importanti artisti canadesi di musica pop, desiderosi di un nuovo regime di libertà lontano dai vincoli imposti dall'industria della produzione musicale ed affermano nel loro manifesto che i produttori hanno denunciato i loro fan contro il loro volere e le leggi che giustificano queste denunce non possono essere sostenute con i loro nomi. Cfr., *http://www.musiccreators.ca/wp*.

[3] Oltre trent'anni fa Giorgio Jarach metteva in guardia dal pericolo che « *il diritto d'autore, fondato sul titolo della creazione, si trasformi in un semplice privilegio industriale…perdendo la sua meritata patente di nobiltà* » (G. JARACH, *Manuale del Diritto d'Autore*, Mursia, 14).

[4] La tesi già da tempo nota in dottrina, è in ultimo chiaramente espressa da U. PAGALLO, *Lezioni americane sulla privacy*, Giappichelli, in corso di pubblicazione.

[5] Cfr. G.RUFFO, *Protezione della privacy e della proprietà intellettuale: il caso del* peer-to-peer *in Italia*, in *Digitalica*, Vol. 2, Giappichelli, 2005, nonché l'assai criticata decisione emessa a fine agosto 2007 dal Giudice federale americano F-M. Cooper nel caso TorrentSpy vs. MPAA (Motion Picture Association of America).

Nel momento in cui il Garante si è determinato ad intervenire in giudizio ponendo in luce le problematiche relative alla tutela del diritto alla riservatezza sottese alla vicenda, il Tribunale di Roma, sezione specializzata in materia di proprietà industriale ed intellettuale, ha emesso in data 16 luglio 2007 l'ordinanza di segno contrario in commento, rigettando il ricorso presentato dalla Peppermint Jam Records GmbH e dalla Techland sp. Z.o.o. volto ad ottenere l'esibizione da parte dalla Wind Telecomunicazioni S.p.a. dei dati anagrafici necessari all'identificazione di (presunti) responsabili di violazioni del diritto d'autore di cui le stesse sono titolari.

L'Autorità Garante ha inoltre deciso di richiedere a diverse società interessate e a gestori telefonici tutti gli elementi utili per una piena valutazione del caso[6] e sta al contempo esaminando i reclami presentati contro la Peppermint.

Le argomentazioni addotte dal Tribunale per motivare il rigetto dell'istanza confermano e danno ampio e pieno riscontro alle osservazioni giuridiche da più parti sollevate dopo l'emissione delle precedenti pronunce.

Prima di analizzare le problematiche legate alla privacy paiono però opportune alcune sintetiche considerazioni sull'applicazione del 156-*bis* L.d.A.

2. L'art. 156-*bis*, L.d.A.

L'interpretazione e la concreta applicazione dell'art. 156-*bis*, L.d.A.[7], introdotto dal D.Lgs. 16 marzo 2006, n. 140, in attuazione della Direttiva 2004/48/CE, pone più di un quesito:

— qual è la « controparte », legittimata passiva del ricorso *ex* art. 156-*bis*?

— per la violazione di quali diritti è consentita l'azione?

— quali limiti incontra il diritto di informazione di cui all'art. 8, Direttiva 2004/48/CE?

Dubbi e questioni che certamente trovano in Italia fondamento nell'infelice recepimento delle disposizioni contenute nella direttiva[8].

Nella norma comunitaria, controparte del diritto di informazione di cui all'art. 8 è l'autore della violazione ovvero ogni altra persona che sia stata trovata in possesso di merci oggetto di violazione, ovvero che utilizzi servizi oggetto di violazione ovvero « *che sia stata sorpresa a fornire servizi* » utili alla violazione.

---

[6] Cfr., *http://www.garanteprivacy.it/garante/doc.jsp?ID=1406297*.

[7] L'art. 156-*bis*, L.d.A. prescrive che: « *Qualora una parte abbia fornito seri elementi dai quali si possa ragionevolmente desumere la fondatezza delle proprie domande ed abbia individuato documenti, elementi o informazioni detenuti dalla controparte che confermino tali indizi, essa può ottenere che il giudice ne disponga l'esibizione oppure che richieda le informazioni alla controparte. …(omissis)…* ».

[8] Pare doveroso segnalare che in data 18 maggio 2007 è stato presentato in Parlamento un disegno di legge, a firma dell'on. Paola Balducci, contenente una proposta di modifica dell'art. 156-*bis* L.d.A. Il testo, attualmente assegnato alla Commissione Giustizia in sede referente ma non ancora esaminato, è consultabile all'indirizzo *www.senato.it/leg/15/BGT/Schede/Ddliter/28379.htm*.

Sostenere che Peppermint abbia « *sorpreso* » la Telecom a fornire servizi utili alla violazione è come sostenere di aver sorpreso Autostrade S.p.a. a fornire servizi utili al traffico di stupefacenti con le sue strade!

Vista la terminologia usata, è difficile non pensare che il legislatore europeo abbia ritenuto riferirsi, quando parla di « controparte », esclusivamente all'autore della violazione o a soggetti terzi che abbiano concorso, agevolato o comunque partecipato scientemente alla violazione stessa.

Peraltro, anche volendo inquadrare la problematica sotto il profilo della responsabilità dei *provider* nei comportamenti abusivi o nelle comunicazioni illecite a mezzo di *internet*, va rilevato come gli ISP interessati dal caso « Peppermint » altro non siano che *provider mere conduit* nei cui confronti il D.Lgs. 9 aprile 2003, n. 70 non prevede alcuna forma di responsabilità per le informazioni trasmesse (art. 14), nessun obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza (art. 17, 1° co.), ma soprattutto nessun obbligo di fornire informazioni se non all'Autorità giudiziaria o a quella amministrativa aventi funzioni di vigilanza ovvero alle stesse Autorità (non certo a privati!) al fine di individuare e prevenire attività illecite (art. 17, 2° co, lett. *a*) e *b*))[9].

La questione non è di poco conto posto che l'utilizzo del ricorso *ex* 156-*bis* per fini meramente investigativi privati rischia di snaturare lo strumento di tutela previsto in sede comunitaria scardinando ulteriormente il delicato e già compromesso equilibrio del Diritto d'Autore.

Nell'ordinanza del 19 agosto 2006 il Tribunale afferma che il combinato disposto degli artt. 156 e 156-*bis*, L.d.A. deroga al principio di cui all'art. 210 c.p.c. secondo cui l'*actio exhibendum* non può avere ad oggetto documenti che non abbiano una originaria destinazione probatoria comune alle parti.

Con il termine « controparte » si deve intendere secondo il Tribunale il legittimato passivo nel giudizio di ostensione e cioè il possessore dei documenti, elementi o informazioni che confermano la fondatezza delle domande del titolare del diritto di utilizzazione economica che ritiene violato e non il supposto, o come nel caso l'ignoto, autore della violazione.

Nell'ordinanza del 1 marzo 2007, più articolata, si legge come l'introduzione della norma di cui all'art. 156-*bis*, L.d.A. debba ritenersi speciale rispetto a quanto previsto dall'art. 210 c.p.c. poiché la *ratio* della disposizione va individuata nel contesto comunitario di origine che ha voluto rafforzare le posizioni soggettive in materia di tutela della proprietà intellettuale al fine di opporre un sistema coordinato ed efficace di contrasto alle violazioni dei diritti d'autore.

Argomentazioni queste apparentemente accettabili a fronte della norma italiana ma in concreto viziate da un'interpretazione letterale che prescinde dal contesto normativo di riferimento e dai valori mediati sottostanti la complessa normativa del Diritto d'Autore.

Per altro, anche là dove il Tribunale prende a riferimento interpretativo la normativa europea, lo stesso estrapola parti dell'art. 8 della diret-

---

[9] In tema di responsabilità dei *provider*, cfr. l'interessante articolo di M. Gambuli, *La responsabilità penale del* provider *per i reati commessi in internet*, su *http://www.altalex.com/index.php?idnot=9965*, nonché la monografia di D. Petrini, *La responsabilità penale per i reati via internet*, Jovene, 2004.

tiva 2004/48/CE decontestualizzandoli ed omettendo così il costante richiamo alla « *scala commerciale* » posto scientemente a base del diritto di informazione.

La scala commerciale, che è a nostro parere addirittura qualche cosa di più del « fine di lucro » proprio della legislazione italiana, è discrimine fondamentale nella normativa a tutela del Diritto d'Autore a mediazione tra i diritti ivi protetti ed i diritti dei fruitori delle opere.

Come per il reato di « pirateria » punito dall'art. 171-*ter* L.d.A. il fine di lucro è contrassegno essenziale di punibilità per evitare di applicare la galera ai semplici fruitori delle opere ovvero a chi condivide a fini personali[10], così per il « diritto di informazione » di cui all'art. 8, Direttiva 2004/48/CE è richiesta una violazione su « scala commerciale », ovvero, si potrebbe dire, su scala imprenditoriale. Ma anche a voler tradurre « scala commerciale » con il fine di lucro, è certo che la condivisione in reti *peer-to peer* colpita dalla Peppermint è, potremmo dire ontologicamente, all'opposto della scala commerciale essendo la più avanzata forma di condivisione gratuita.

Valga ancora sottolineare come presupposto del diritto di informazione di cui all'art. 8 sia nella direttiva una violazione « in atto o imminente »: circostanza che nel caso « Peppermint » certamente non ricorreva trattandosi di presunte violazioni risalenti all'anno 2006.

Tali profili dovranno esser oggetto di attenta critica.

In ogni caso, il Tribunale, almeno nelle prime ordinanze, non si pone alcuno dei problemi sollevati e neppure affronta la fondamentale questione circa il rapporto e conseguente bilanciamento tra applicazione dell'art. 156-*bis*, L.d.A. per la tutela di interessi di carattere meramente patrimoniale e tutela di diritti di rango superiore, quale quello alla riservatezza che è valore fondamentale della persona.

Diversa, fortunatamente, l'interpretazione resa dal Tribunale di Roma con l'ordinanza 16 luglio 2007, in cui si legge come la corretta interpretazione dell'art. 156-*bis*, L. 633/1941 nella parte in cui prevede che il titolare di un diritto d'autore possa chiedere all'autorità giudiziaria, anche nei confronti di soggetti diversi dagli autori della violazione, un ordine di esibizione dei dati e delle informazioni necessarie all'individuazione degli autori delle violazioni stesse, debba essere necessariamente contemperata con la tutela di altri diritti coinvolti.

Ebbene, in questo caso, il Giudicante, con un'interpretazione sistematica, afferma che l'art. 156-*bis* non possa trovare applicazione con riferimento alla richiesta di esibizione di dati che attengono a comunicazioni elettroniche, né dei dati di traffico da queste prodotte, in quanto la tutela della segretezza (*rectius* della riservatezza) delle comunicazioni elettroniche e telematiche tra privati, quale valore fondamentale della persona, prevale, nel giudizio di bilanciamento dei due diritti, sulla tutela del Diritto d'Autore.

La tesi è semplice, chiara ed assolutamente incontestabile: sia il sistema normativo interno che quello comunitario impongono il divieto assoluto di

---

[10] Cfr. Cass., sez. III pen., 9 gennaio 2007, n. 149, su *http://www.altalex.com/index.php?idnot=10640* con nota di approfondimento di C. Blengino.

trattamento dei dati relativi a comunicazioni elettroniche e dunque la loro acquisizione, comunicazione e utilizzo.

A livello comunitario, il riferimento normativo è dato dagli artt. 8 e 9 della direttiva 2004/48/CE in materia di proprietà intellettuale i quali fanno salva, nella previsione di adozione da parte dei legislatori interni di norme che contemplino la possibilità di ottenere informazioni sulle opere violate dall'autore o da terzi che abbiano fornito servizi utilizzati per commettere la violazione stessa, la normativa relativa alla protezione dei dati personali.

A livello nazionale, invece, a parere del Tribunale, la tutela delle comunicazioni tra privati assurge a rango costituzionale ai sensi degli artt. 2 e 15 Cost. ed il divieto assoluto di trattamento può essere derogato solo per la tutela di valori di rango superiore e che attengano alla difesa di interessi della collettività ovvero alla protezione di sistemi informatici.

L'unica eccezione al divieto di trattamento è infatti rappresentata, secondo il Giudicante, dall'accertamento, dalla prevenzione e dalla repressione di illeciti penali di particolare gravità — art. 407, 2 co., lett. *a*), c.p.p. — e quelli in danno di sistemi informatici o telematici.

Dopo queste brevi considerazioni critiche circa la portata e la valenza dell'azione esperita *ex* art. 156-*bis* L.d.A., analizziamo, dunque, i diversi aspetti relativi alla tutela dei dati personali sottesi alla vicenda « Peppermint ».

3. Due questioni preliminari.

a) L'applicabilità del D.Lgs. 196/03.

b) La possibilità di considerare un indirizzo IP come dato personale.

3.a. Considerato che la Logistep AG ha sede legale a Steinhausen in Svizzera, si pone in prima battuta la questione dell'applicabilità della legge italiana in materia di tutela dei dati personali.

A tal proposito, il disposto dell'art. 5, D.Lgs. 196/03 è peraltro esaustivo e dirimente: il codice privacy disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato in un luogo comunque soggetto alla sovranità dello Stato.

La fattispecie in esame rientra dunque pienamente sotto la giurisdizione italiana in quanto, sebbene verosimilmente detenuti all'estero, i dati personali sono stati indiscutibilmente raccolti dalla Logistep AG, per conto della Peppermint, in Italia. È infatti indiscutibile che le informazioni assunte a mezzo del *software* antipirateria (indirizzo IP dell'utente, data e ora della connessione e nome del *file* condiviso) non possono che essere state estrapolate direttamente dai PC connessi in rete ma materialmente situati in Italia (in particolare punto di rete e cartella condivisa).

Poiché la raccolta è una delle operazioni di trattamento previste dall'art. 4, 1° co., lett. *a*), D.Lgs. 196/03 e tale operazione è avvenuta materialmente in Italia, ne consegue che non può non trovare applicazione, quanto meno nella fase iniziale di trattamento, la legge italiana.

In ogni caso, il secondo comma del citato articolo 5 stabilisce che il codice si applica anche qualora il trattamento sia effettuato da un soggetto stabilito nel territorio di un Paese non appartenente all'Unione europea (nel caso di specie, la Svizzera) che impiega però strumenti situati nel territorio italiano anche diversi da quelli elettronici.

Orbene, è pacifico come nel caso di specie vi sia stata una seconda fase di trattamento, consistita nella comunicazione (art. 4, 1° co., lett. *a*), D.Lgs. 196/03) dei dati personali raccolti e registrati dalla Logistep AG verosimilmente alla Peppermint (e qui si aprirebbe un ulteriore profilo relativo all'applicabilità della legge tedesca) nonché allo studio legale di Bolzano, il quale studio li ha dapprima prodotti in giudizio avanti il Tribunale di Roma e poi, a seguito di un'operazione di *data matching*, utilizzati per inviare le diffide agli utenti.

È pertanto evidente ed innegabile come vi siano state più operazioni di trattamento, dalla raccolta alla consultazione, elaborazione, selezione, estrazione, comunicazione ed utilizzo, effettuate con strumenti situati in Italia.

3.b. Fornire la prova che l'indirizzo IP sia un dato personale potrebbe sembrare tautologico, visto che se non si trattasse di un'informazione relativa ad una persona identificabile[11] la Peppermint non sarebbe riuscita a diffidare ben 3.636 utenti italiani, tuttavia, vista la delicatezza della vicenda, non è superfluo ricordare che già nel parere n. 2 del 30 maggio 2002 il Gruppo per la tutela dei dati personali (Articolo 29) affermava che: « *Il Gruppo mette in evidenza che gli indirizzi IP attribuiti agli utenti Internet costituiscono dati personali e sono tutelati dalle direttiva 95/46/CEE e 97/66/CEE* »[12].

Più di recente, particolare attenzione al concetto di dato personale è stata manifestata dai Garanti europei i quali, sempre tramite il Gruppo di lavoro — Articolo 29, nel parere n. 4 del 20 giugno 2007, hanno ribadito che le informazioni apparentemente frammentarie costituiscono dato personale nella misura in cui il titolare le ha raccolte con l'intenzione di utilizzarle per identificare una determinata persona e viene fatto espresso riferimento ai titolari di diritti d'autore che raccolgono dati al fine di perseguire utenti di computer per violazioni della proprietà intellettuale[13].

4. La violazione dell'art. 23, D.Lgs. 196/03.

Premesso che nel caso di specie trova applicazione la legge italiana in materia di tutela dei dati personali e che gli indirizzi IP sono dati personali, pare pacifico che il trattamento effettuato dalla Peppermint, mediante l'attività svolta da Logistep AG, sia assolutamente illecito.

Le operazioni di raccolta degli indirizzi IP sono infatti state effettuate dalla Logistep AG, per conto della Peppermint, oltre che in assenza di

---

[11] Ai sensi dell'art. 4, 1° co., lett. *b*), D.Lgs. 196/03 si intende per dato personale « *qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi informazione, ivi compreso un numero di identificazione personale* ».

[12] Cfr. *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp58_it.pdf*.

[13] Cfr. Newsletter del Garante per la Protezione dei dati personali n. 293 del 26 luglio 2007 (*http://www.garanteprivacy.it/garante/doc.jsp?ID=1426830*) e più in dettaglio le argomentazioni del Gruppo di lavoro, sebbene ancora nella versione in lingua inglese, alle pagine 16-17 del documento al link *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf*.

qualsivoglia informativa, in assoluta violazione dell'art. 23, 1º co, D.Lgs. 196/03, il quale prescrive chiaramente che il consenso al trattamento di dati personali da parte di privati è ammesso solo con il consenso espresso dell'interessato[14].

L'ordinanza del 19 agosto 2006, invece, liquida la questione affermando che: « *Il modo in cui i suddetti dati sono stati recuperati dalla società incaricata dalla Peppermint appare dunque affidabile, accettabile e soprattutto lecito, posto 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* ».

La tesi pare però del tutto destituita di fondamento.

L'interpretazione del disposto di cui all'art. 23, D.Lgs. 196/03 da parte dell'Autorità Garante per la protezione dei dati personali è sempre stata assai rigorosa quanto univoca nell'affermare che i casi di deroga al consenso preventivo ed espresso dell'interessato di cui all'art. 24, D.Lgs. 196/03 sono tassativi e non possono essere dunque oggetto di estensione analogica.

In particolare, l'interpretazione dell'esimente di cui all'art. 24, 1º co., lett. *c*), D.Lgs. 196/03, nella parte in cui parla di dati provenienti da « *pubblici registri, elenchi, atti o documenti conoscibili da chiunque* » è sempre stata nel senso di una pubblica conoscibilità basata su elementi normativi e non su mere circostanze di fatto, come sostenuto dal Tribunale di Roma.

Tra i tanti provvedimenti dell'Autorità Garante in materia, pare sintomatico il Provvedimento generale, emanato in data 29 maggio 2003, in materia di *spamming*, in cui viene affermato — con riferimento alla raccolta, considerata appunto illecita, di indirizzi di posta elettronica effettuata in rete tramite appositi software o motori di ricerca — il principio secondo cui non deroga alla necessità di acquisire il consenso preventivo ed espresso dell'interessato la circostanza che i dati personali siano, di fatto, conoscibili da chiunque atteso che la pubblicità (di registri, elenchi, atti o documenti) che scrimina il trattamento (senza consenso) ai sensi dell'art. 24, 1º co., lett. *c*), D.Lgs. 196/03, deve intendersi tassativamente subordinata ad una disciplina legislativa e/o regolamentare che ne consenta la conoscibilità indifferenziata da parte del pubblico e non anche quella che deriva da una conoscibilità diffusa per mere circostanze di fatto[15].

Sotto tale profilo, dunque, l'ordinanza 19 agosto 2006 del Tribunale di Roma non solo non è condivisibile ma adotta un principio in palese contrasto con la disciplina vigente.

---

[14] Cfr. per un interessante disamina delle problematiche giuridiche sottese alla raccolta occulta di dati di traffico internet, M. VIGGIANO, *« Navigazione » in internet e acquisizione occulta di dati personali*, in questa *Rivista*, 2007, 347.

[15] Cfr. Provvedimento generale 29 maggio 2003, su *www.garanteprivacy.it/garante/doc.jsp?ID=29840*; per un'attenta analisi sulle comunicazioni commerciali indesiderate cfr. M. BERLINGIERI, *L'informazione commerciale non desiderata e lo spamming*, disponibile su *www.privacy.it/berlingieri06.html*, nonché M.A. SENOR, *Comunicazioni indesiderate: tecniche commerciali, spamming e consenso dell'interessato*, in *Atti del convegno "I diversi aspetti del diritto alla protezione dei dati personali"*, Torino, 10 giugno 2004, al link *ww.ordineavvocatitorino.it/UserFiles/File/convegni/atti/RelazioneSenor.pdf*.

Ma il Tribunale va ben oltre: nella stessa ordinanza 19 agosto 2006 afferma infatti che il trattamento dei dati personali effettuato da Peppermint è scriminato ai sensi dell'art. 24, 1° co., lett. *f*), D.Lgs. 196/03 in quanto finalizzato a far valere o difendere un diritto in sede giudiziaria.

Orbene, in effetti il trattamento senza consenso da parte dello studio legale della casa discografica potrebbe apparire *prima facie* legittimo. Se non che, al limite, la scriminante potrebbe valere per il trattamento dei dati anagrafici così come ottenuti dai *provider* in esecuzione all'ordine di esibizione del Tribunale di Roma, ma non certo per i dati raccolti e registrati dalla Logistep AG (fase iniziale di raccolta e registrazione) ed ancor meno per quelli scaturiti dal *data matching* effettuato tra le anagrafiche acquisite grazie all'ordine di esibizione emanato dall'Autorità Giudiziaria e gli IP intercettati (fase finale di elaborazione, selezione, estrazione ed utilizzo).

Sotto tale profilo, l'ordinanza del 16 luglio 2007 è da salutare con entusiasmo atteso che ritiene, a nostro avviso correttamente, inapplicabile al caso « Peppermint » la scriminante di cui all'art. 24, lett. *f*), D.Lgs. 196/03 osservando come l'art. 24 possa trovare applicazione solo se il dato personale trattato senza il consenso dell'interessato sia previamente in possesso di chi intende utilizzarlo per far valere un diritto e tale possesso sia legittimo.

Nel caso di specie, osserva il Tribunale di Roma, le ricorrenti non solo non sono in possesso del dato personale che vorrebbero utilizzare per tutelare il loro diritto d'autore sui *file* oggetto di *file sharing*, ma anzi propongono ricorso proprio per acquisire i dati da utilizzare in un eventuale futuro giudizio e quindi « *si tratta di un ambito logicamente e temporalmente anteriore rispetto all'ipotesi contemplata dall'art. 24* ».

Ma chi sono gli autori della violazione? Contro chi agisce in sede giudiziaria la Peppermint utilizzando (il-legittimamente(?)) quei dati? Non contro gli autori ma contro soggetto terzo (ISP) al fine di trovarli. E per trovarli, con l'avvallo del Tribunale, si fa consegnare dati personali di cittadini che, in quanto intestatari delle linee telefoniche cui corrispondono gli indirizzi IP dell'*account*, potrebbero essere, ma non certamente sono, autori della violazione.

I dati forniti dai *provider* costituiscono al più ulteriore indizio per individuare, nella casa o nell'ufficio presso cui arriva la linea, il malandrino che condivideva la musica.

Ma ancora non esiste legalmente una « controparte » nei confronti della quale agire giudizialmente.

È pacifico, crediamo, che l'intestatario della linea telefonica cui corrisponde l'indirizzo IP « recuperato » (come scrive il Tribunale di Roma, sic!) non possa esser considerato *sic et simpliciter* l'autore della violazione.

Quale istituto giuridico potrebbe mai suffragare siffatta impostazione?

O si sostiene la sussistenza di una fantasiosa ipotesi di responsabilità oggettiva oppure il dato non consente alcuna legittima azione giudiziaria nei confronti del titolare.

Non si dimentichi che l'ipotetica azione civile della Peppermint sarebbe intentata per responsabilità extracontrattuale e dunque una responsabilità imputata per il sol fatto di esser l'intestatario rischierebbe di tradursi in responsabilità per fatto altrui.

Certamente non può allo stato sostenersi che il titolare di un accesso ad *internet* sia per ciò solo titolare di un'attività pericolosa con inversione

dell'onere probatorio in caso di utilizzo illecito delle informazioni trasmesse.

Valga ricordare invece agli autori dell'improvvida iniziativa stragiudiziale l'art. 15 che richiama espressamente l'art. 2050 c.c. per il trattamento dei dati personali!

Da queste considerazioni discendono forti dubbi circa la sussistenza, nel caso, della scriminante al consenso di cui all'art. 24, 1° co, lett. *f*), D.Lgs. 196/03 nel trattamento effettuato dallo studio legale nell'interesse della Peppermint.

Ad oggi, non c'è sede giudiziaria ove sia stato fatto valere qual si voglia diritto soggettivo.

Il ricorso *ex* art. 156-*bis* L.d.A. non è strumento deputato alla ricerca dell'autore della violazione, come erroneamente interpretato dal Tribunale di Roma nelle ordinanze in commento, ma è volto, crediamo, ad agevolare l'individuazione delle prove nell'ambito di un'azione inibitoria (art. 156 L.d.A.) per violazioni, temute o in atto, nei confronti dei responsabili.

In difetto, si autorizzerebbe chiunque a trattare qualsivoglia dato, di un'intera comunità, città o nazione, sol perché all'esito del trattamento, forse, potrebbe esser individuato un soggetto contro cui far valere un diritto in un possibile giudizio.

Sarebbe come consentire ed avallare l'intercettazione (illecita) di tutte le telefonate di una data comunità poiché, siccome qualcuno parla male di me e mi diffama in quell'ambito, individuerò le conversazioni lesive ed agirò in giudizio, prima contro il gestore della rete telefonica per sapere chi è l'intestatario della linea, poi contro costui per difendere la mia reputazione ed il mio buon nome, indipendentemente dal fatto che a proferir le male parole diffamanti sia l'ospite di casa, la moglie pettegola o il ribelle figliolo quindicenne!

Giova da ultimo ricordare che la violazione dell'art. 23, è sanzionata penalmente dall'art. 167, D.Lgs. 196/03[16].

5. La violazione dell'art. 122, D.Lgs. 196/03.

Sebbene il Tribunale di Roma non faccia riferimento esplicito ad alcuna determinata disposizione del codice per la protezione dei dati personali legislativa, l'ordinanza di rigetto del 16 luglio 2007 sottintende pacificamente la rilevanza nel caso « Peppermint » del disposto di cui all'art. 122, D.Lgs. 196/03.

L'art. 122, D.Lgs. 196/03, infatti, vieta espressamente l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente stesso.

Benché il disposto dell'art. 122 non sia sanzionato penalmente, va detto che ai sensi dell'art. 11, 2° co., del codice i dati personali trattati in violazione della disciplina in materia di trattamento dei dati personali non

[16] Cfr. G. Corrias Lucente, *La nuova normativa penale a tutela dei dati personali*, in AA.VV., *Il Codice dei dati personali*, Milano, 2004.

possono essere utilizzati ed il danno anche non patrimoniale che ne deriva è risarcibile ai sensi dell'art. 15, D.Lgs. 196/03.

L'unica deroga al disposto dell'art. 122 è stata introdotta dall'art. 7, 4º co., D.L. 144/05, recante misure urgenti per il contrasto al terrorismo, il quale prevede a carico dei titolari e dei gestori di pubblici esercizi o circoli privati misure *ad hoc* per monitorare ed archiviare le operazioni effettuate dagli utenti nonché misure specifiche per la preventiva acquisizione dei dati anagrafici (a mezzo documento di identità) dei soggetti che utilizzano postazioni pubbliche non vigilate per comunicazioni telematiche ovvero punti di accesso ad internet con tecnologia senza fili.

Detta deroga, a ben guardare, non solo non scalfisce l'applicabilità del disposto di cui all'art. 122 al caso « Peppermint », ma, anzi, rafforza la correttezza dell'interpretazione data alla prevalenza del diritto alla riservatezza su diritti di rango inferiore.

La possibilità di monitorare ed archiviare le operazioni effettuate dagli utenti a mezzo *internet* in deroga all'art. 122, D.Lgs. 196/03 può essere dunque giustificata solo da ragioni di sicurezza (lotta contro il terrorismo) ed è limitata ai gestori di pubblici esercizi. *Tertium non datur*.

6. Il bilanciamento tra diritti connessi al diritto d'autore ed il diritto alla tutela dei dati personali.

La domanda fondamentale diviene allora la seguente: la tutela dei diritti connessi al Diritto d'Autore di una casa discografica su di una canzone (la maggior parte dei cittadini colpiti è rea di aver condiviso un solo brano musicale in formato mp3!), prevale, nel giudizio di bilanciamento, sul diritto alla tutela dei dati personali del singolo utente?

Ovvero è legittimo violare norme a tutela del diritto alla riservatezza per tutelare il diritto connesso al Diritto d'Autore?

Il Diritto d'Autore, nelle sue diverse componenti, e nella sua complessa titolarità, non è un diritto assoluto, ma il frutto della mediazione tra il diritto alla libera circolazione delle idee e della cultura e la giusta remunerazione della creazione dell'ingegno.

Basti pensare che nella Dichiarazione Universale dei Diritti dell'Uomo all'art. 27 si legge:

1. *Ogni individuo ha diritto di prendere parte liberamente alla vita culturale della comunità, di godere delle arti e di partecipare al progresso scientifico ed ai suoi benefici.*

2. *Ogni individuo ha diritto alla protezione degli interessi morali e materiali derivanti da ogni produzione scientifica, letteraria e artistica di cui egli sia autore.*

Crediamo che la formulazione e l'ordine gerarchico dei principi espressi non sia casuale.

Per contro, il diritto alla riservatezza è un diritto primario costituzionalmente garantito[17].

[17] Tale diritto è stato formulato dalla dottrina italiana sulla scorta del diritto anglosassone « *right to be alone* ». Il concetto ha subito, peraltro, ulteriori evoluzioni come si evince dall'elaborazione del « diritto di essere lasciati in pace » formulato da M. Atelli,

Ma vi è di più.

Il diritto alla protezione dei propri dati personali è sino ad oggi sempre stato fatto salvo anche a fronte di ipotesi e/o tentativi di compressione giustificate da esigenze di lotta alla criminalità (salve le eccezioni legate alla legislazione d'urgenza per ragioni di anti-terrorismo).

In particolare, pare opportuno richiamare il Parere n. 9 del 5 novembre 2001 del Gruppo sulla tutela dei dati personali (Articolo 29) secondo cui: « *Le misure adottate per soddisfare gli interessi legittimi della lotta alla criminalità informatica devono infatti essere conformi agli imperativi relativi alla tutela dei diritti e delle libertà fondamentali. Qualsiasi limitazione di tali diritti e libertà va debitamente giustificata e deve essere necessaria e commisurata all'obiettivo perseguito. La maggiore considerazione del fenomeno della criminalità informatica non deve fornire l'occasione per istituire tecniche di sorveglianza importante dei cittadini, senza che siano state esaminate accuratamente le alternative per lottare contro la criminalità informatica* ».

Se tale principio è adottato per la lotta istituzionale alla criminalità, è evidente che finalità di « lotta privata » non possono che porsi ancor più in subordine in guisa tale da non elidere in alcun modo i diritti e le libertà fondamentali dei cittadini.

Più di recente ed a livello nazionale si pone la recente sentenza[18] con cui la Corte Costituzionale ha dichiarato inammissibili e non fondate alcune questioni di legittimità costituzionale sull'art. 132, D.Lgs. 196/03, nella parte in cui pone modalità e limiti all'acquisizione di tabulati telefonici nel corso di indagini di polizia giudiziaria, affermando che tale norma esprime scelte di politica criminale e di ragionevole bilanciamento fra diritto individuale alla riservatezza e interesse collettivo alla repressione dei reati.

Quanto all'art. 132, D.Lgs. 196/03 (il cui titolo « *Conservazione di dati di traffico per altre finalità* » è di per sé sintomatico della limitata utilizzabilità di tali dati) pare doveroso sottolineare come la regola sia che i dati di traffico telefonico e telematico possono essere conservati (e dunque esibiti) solo per finalità di accertamento e repressione di reati rispettivamente per ventiquattro e sei mesi, mentre l'ulteriore conservazione per ventiquattro o sei mesi rappresenta un'eccezione ed è motivata da esclusive finalità di accertamento e repressione dei reati di cui all'art. 407, 2° co., lett. *a*), c.p.p. e dei delitti in danno di sistemi informatici o telematici.

Nel caso di specie, dunque, la richiesta *ex* art. 156-*bis*, L. 633/41 finalizzata alla salvaguardia del Diritto d'Autore di una casa discografica non può costituire una valida ragione per derogare al divieto di trattamento imposto dal titolo X del codice privacy.

Chiamate indesiderate. Commento, in AA. VV., *Privacy e telecomunicazioni. Commentario al D.Lgs. n. 171/1998*, a cura di M. Atelli, Napoli, 1999, 201 e ss, nonché del « diritto alla tranquillità personale » formulato da S. Vigliar, *Privacy e comunicazioni elettroniche: la direttiva 2002/58/CE*, in questa *Rivista*, 2003, 419-420. Per un'analisi del diritto alla protezione dei dati personali inteso come « nuovo diritto della personalità », cfr. Cardarelli, Sica, Zeno Zencovich, *Il Codice dei dati personali*, Milano, 2004, 23 e ss.

[18] Cfr. Corte Cost., 14 novembre 2006, n. 372, in questa *Rivista*, 2007, 133.

Se il diritto alla riservatezza non può essere compresso, limitato e/o derogato neppure a favore delle indagini giudiziarie svolte sotto il controllo della magistratura, come può essere del tutto eliso da un soggetto privato, con indagini private al fine di a far valere un presunto (e dubbio!) diritto patrimoniale[19]?

7. Le modalità di trattamento e la mancata notificazione all'Autorità Garante.

Va poi preso in considerazione l'ulteriore profilo relativo alle modalità con cui è effettuato il trattamento dei dati personali delle persone « intercettate » da parte della Peppermint, della Logistep AG e dello studio legale di Bolzano, l'ambito di comunicazione e di conoscenza dei dati stessi.

Sul punto gli interessati nulla sanno.

Ad onor del vero, anche la titolarità del trattamento in capo alla Peppermint è frutto di una deduzione logica, sicuramente attendibile, ma pur sempre e solo logica.

Se non fossero sufficienti le argomentazioni sopra esposte, questa sarebbe comunque la prova dell'illiceità del trattamento!

Le uniche informazioni che gli interessati hanno in ordine al trattamento dei loro dati personali effettuato dalla Peppermint emergono dal contenuto della raccomandata; in assenza di informativa e consenso nulla è dato conosce in particolare circa le modalità del trattamento, l'ambito di comunicazione dei dati e quali siano le persone che possono venire a conoscenza dei dati stessi.

Tali informazioni concernono la c.d. struttura privacy adottata dalla casa discografica tedesca: dall'organigramma delle funzioni attribuite ai vari soggetti che effettuano operazioni di trattamento (nomine de responsabili interni e/o esterni e degli incaricati) alle misure di sicurezza adottate.

Da ultimo, pare doveroso un richiamo al disposto dell'art. 37, D.Lgs. 196/03 in materia di notificazioni.

In particolare, il riferimento è all'obbligo di notificazione (che deve essere presentata al Garante prima dell'inizio del trattamento stesso) quando i dati sono trattati con l'ausilio di strumenti elettronici e siano volti a monitorare l'utilizzo di servizi di comunicazione elettronica.

Ovviamente la norma parla di monitoraggio e non di raccolta proprio perché quest'ultima, concretizzandosi di fatto in una intercettazione illegale, è espressamente vietata dall'art. 122, D.Lgs. 196/03, nonché sanzionata penalmente dall'art. 617-*bis*, c.p.

In ogni caso, per il solo monitoraggio è appunto prescritta la notifica al Garante, cosa che nel caso di specie, non risulta essere stata effettuata.

La Peppermint Jam risulta pertanto inadempiente anche sotto tale profilo ed il Tribunale di Roma nell'ordinanza 16 luglio 2007 correttamente sostiene che il possesso dei dati parziali dei presunti responsabili della vio-

[19] Per un attento esame dei delicati rapporti tra tecnologia e riservatezza, cfr. Plantamura, *Moderne Tecnologie, riservatezza e sistema penale: quali equilibri?*, in questa *Rivista*, 2006, 417.

lazione dell'art. 16, L. 633/1941, ovverosia l'indirizzo IP ed il codice GUID, che le ricorrenti adducono come « seri elementi » indiziari della violazione del diritto d'autore, sono stati acquisiti illecitamente in violazione dell'art. 37, D.Lgs. 196/03.

8. Conclusioni.

Concludevamo una nostra prima nota sul caso « Peppermint »[20] auspicando che il principio del *male captum, bene retentum*, che Cordero paragonava all'albero dai frutti velenosi[21], di fatto applicato dal Tribunale di Roma nelle ordinanze di accoglimento dei ricorsi Peppermint non trovasse cittadinanza in Italia.

Oggi riteniamo che le argomentazione addotte dal Tribunale di Roma nell'ordinanza 16 luglio 2007 sicuramente saranno di conforto a quei 4.000 cittadini che dopo la ricezione delle raccomandate simil-estorsive basate sulle precedenti ordinanze romane avevano denunciato il grave rischio sotteso ad un'interpretazione scorretta dell'art. 156-*bis*, L.633/1941 ed al conseguente squarcio prodotto nel tessuto ordinamentale laddove fosse concesso a soggetti privati di derogare per fini personali (e forse solo di lucro!) a regole fondamentali poste a protezione dell'intera collettività.

Ma, come si accennava inizialmente, quel che più conforta, non solo i cittadini ma anche gli operatori del diritto, è l'intervento nel giudizio in esame del Garante per la protezione del dati personali.

La sua assenza nei precedenti procedimenti aveva certamente influito negativamente, quanto meno sulla corretta interpretazione della normativa privacy.

La decisione di costituirsi nel presente ricorso è dunque da salutare con favore sia in considerazione delle ampiamente condivisibili ed attente ragioni addotte a sostegno dell'intervento, sia in prospettiva, atteso che l'Autorità Garante sarà chiamata ad emettere a breve il suo giudizio sui reclami ad essa presentati in relazione al caso « Peppermint ».

Siamo certi che il Garante provvederà al più presto alla sua decisione in senso positivo per gli utenti interessati dall'incresciosa vicenda, conformemente a quanto dichiarato agli organi di stampa dal Segretario generale[22] nonché dalle argomentazioni addotte dall'avvocatura erariale nell'intervento per conto del Garante nell'ordinanza in commento.

Il Diritto d'Autore è uno dei più nobili diritti, poiché fondato sul titolo della creazione.

I diritti ad esso connessi di sfruttamento economico dei produttori, ci sia consentito, un poco meno nobili sono.

---

[20] Cfr. C. Blengino e M.A. Senor, *Caso Peppermint:* file sharing *e utilizzo di dati personali illecitamente trattati*, su *http://www.altalex.com/index.php?idnot=2541*.

[21] Per un interessante parallelo tra il principio *de quo*, sequestri e intercettazioni, cfr. Cordero, *Piccole apocalissi a buon mercato*, su *www.libertaegiustizia.it/primopiano/pp_leggi_articolo.php?id=687&id_titoli_primo_piano=1*.

[22] Cfr. G. Buttarelli, *Il Caso « Peppermint » banco di prova dei diritti*, ne *Il Sole-24 Ore*, 31 maggio 2007.

Entrambi debbono però flettere, senza resistenza, davanti al diritto costituzionalmente garantito alla protezione dei dati personali.

Gli strumenti e le modalità di tutela dei diritti previsti dalla L.d.A. dopo l'attuazione della direttiva 2004/48/CE sono già oggetto di aspra critica per l'intollerabile compressione del diritto costituzionalmente garantito all'accesso ed alla fruizione della cultura e delle idee da parte di tutti[23]. E ciò non a beneficio degli autori ma di imprese commerciali che con la creazione e l'ingegno hanno poco a che fare.

Del resto, dopo queste parole pronunciate dal prof. Pizzetti nella Relazione annuale lo scorso 12 luglio, non si può non esser ottimisti:

« *È certamente vero che non c'è libertà senza sicurezza, ma è ancora più vero che non c'è sicurezza che valga la perdita di ogni libertà. Ripetiamo che la protezione dati non è e non sarà mai "antagonista" al bisogno di sicurezza, ma riaffermiamo che essa è un elemento essenziale di un sistema democratico di tutele* »[24].

E ci sia consentito rimarcare come, nei pretesi diritti dei titolari di diritti connessi al Diritto d'Autore, vi è ben poca sicurezza e vi è molto privilegio commerciale: se il diritto costituzionalmente garantito alla riservatezza dovesse ceder ancora a fronte dei particolari interessi economici di una piccola casa discografica, bhè, crediamo sarebbe davvero difficile parlare di tutela della privacy e dunque di libertà.

Carlo Blengino
Monica Alessia Senor

[23] Sul complesso rapporto tra libertà e tecnologie informatiche, cfr. G. Corasaniti, *Diritti nella rete. Valori umani, regole, interazione tecnologica globale*, Angeli, 2006.

[24] Cfr. Discorso del Presidente dell'Autorità Garante per la protezione dei dati personali, prof. Francesco Pizzetti - Relazione 2006 - 12 luglio 2007, al link *http://www.garanteprivacy.it/garante/doc.jsp?ID=1419791*.