

Digital Copyright / File Sharing / Data Retention

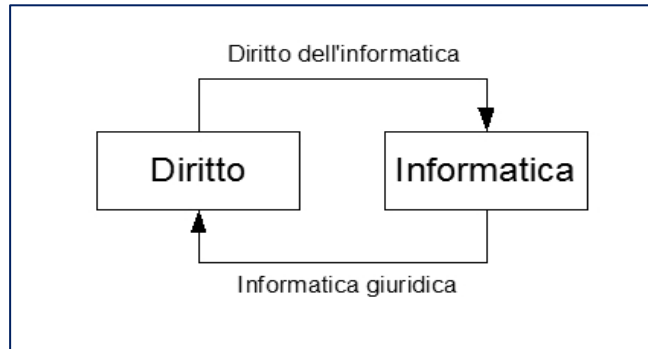
§. 1.- Premessa teorica	2
§. 1.1.- <i>Rapporto diritto / informatica</i>	2
§. 1.2.- <i>L'informazione come bene immateriale: Copyright e Digital Copyright.....</i>	2
§. 1.2.1.- <i>Fonti del diritto d'autore</i>	3
§. 1.2.2.- <i>Cenni alla disciplina tradizionale del diritto d'autore.....</i>	4
§. 1.2.3.- <i>La protezione tecnologica: il Digital Rights Management.....</i>	4
§. 1.2.3.1.- <i>Copyright Management Information.....</i>	5
§. 1.2.3.2.- <i>Misure Tecnologiche di Protezione.....</i>	6
§. 2.- La condivisione dell'informazione in Internet	7
§. 2.1.- <i>Struttura della comunicazione.....</i>	7
§. 2.2.- <i>Soggetti coinvolti.....</i>	7
§. 2.3.- <i>Il contenuto dell'informazione (e il suo controllo).....</i>	8
§. 3.- La responsabilità "verticale" del provider	8
§. 3.1.- <i>I modelli "analogici" di responsabilità</i>	8
§. 3.2.- <i>La discussione</i>	9
§. 3.3.- <i>La soluzione italiana.....</i>	9
§. 3.4.- <i>La normativa comunitaria sul "commercio elettronico".....</i>	9
§. 3.5.- <i>La condivisione "orizzontale": il peer to peer</i>	11
§. 3.5.1.- <i>Il Peer to Peer: reti "ibride" (Napster) e reti "pure" (Gnutella).....</i>	11
§. 3.5.2.- <i>The Pirate Bay come Google?</i>	11
§. 3.5.3.- <i>I precedenti: da Betamax a Grokster</i>	12
§. 4.- La responsabilità dell'utente: Data Retention sul traffico telematico	14
§. 4.1.- <i>Le sanzioni previste dalla legge sul diritto d'autore</i>	14
§. 4.2.- <i>Data Retention: evoluzione e prospettive</i>	17
§. 4.2.1.- <i>Il decreto "Pisanu".....</i>	17
§. 4.2.2.- <i>La giurisprudenza comunitaria: il caso "Promusicae".....</i>	19
§. 4.2.3.- <i>La proposta di direttiva "Pacchetto Telecom".....</i>	20
§. 5.- Conclusioni.....	21
§. 6.- Avvertenza	21



§. 1.- Premessa teorica

§. 1.1.- Rapporto diritto / informatica

In estrema sintesi, il rapporto tra Diritto e Informatica – che ai fini della presente sistemazione può essere considerata come la tecnologia per antonomasia – si può rappresentare come una relazione reciproca nei seguenti termini:



Per esempio, al **Diritto applicato all'informatica** si possono iscrivere le seguenti materie:

- (1) Nomi a dominio;
- (2) Commercio elettronico;
- (3) Protezione dati personali;
- (4) Diritto delle telecomunicazioni.

All'**informatizzazione del diritto**, invece, appartengono le seguenti tematiche:

- (1) Applicazione dell'informatica alla prassi giuridica e dunque:
 - a. Processo telematico;
 - b. Amministrazione digitale;
 - c. Legimatica.
- (2) Studi sulla teoria generale del diritto nella "Società dell'Informazione"¹;
- (3) Applicazione dell'intelligenza artificiale al diritto.

§. 1.2.- L'informazione come bene immateriale: Copyright e Digital Copyright

In estrema sintesi, nell'età dell'innovazione, il progresso è divenuto il "bene" supremo.

L'informazione è il più importante valore da difendere e da perseguire.

Di conseguenza, l'obiettivo essenziale del potere è il controllo sull'informazione.

Si distingue tradizionalmente tra brevetto e diritto d'autore.

	Brevetto	Diritto d'autore
Costituzione	Dal riconoscimento	Dalla creazione
Oggetto	Idea suscettibile di applicazione tecnica	Opera
Oneri	Costo mantenimento	Gratis

¹ A tal proposito pare opportuno menzionare almeno il tedesco Niklas Luhmann e gli italiani Vittorio Frosini, Enrico di Robilant, Mario G. Losano.



In questa sede si espongono alcune brevi considerazioni sul diritto d'autore, inteso come istituto giuridico dal quale si sviluppano un complesso di problematiche attinenti al controllo dei processi di elaborazione e diffusione delle creazioni intellettuali.

§. 1.2.1.- *Fonti del diritto d'autore*

È riconosciuto a livello internazionale, in particolare dall'art. 27 comma 2 della Dichiarazione dei Diritti dell'Uomo e dall'art. 17 comma 2 della Carta Fondamentale dell'Unione Europea².

In realtà gli attuali principi, risalenti alla Convenzione di Berna del 1886 (vedasi da ultimo la Legge 399/1978) devono essere ricondotti ad alcune convenzioni sottoscritte alla metà degli anni Novanta. In particolare meritano di essere ricordate anzitutto il discusso accordo TRIPS (*Trade Related Aspects of Intellectual Property Rights, TRIPS*) del 1994³, conclusivo dei negoziati relativi all'*Uruguay Round*, costitutivi del WTO; in secondo luogo i due trattati sottoscritti a Ginevra il 20 Dicembre 1996 presso l'Organizzazione mondiale per la protezione della proprietà intellettuale (OMPI, all'inglese WIPO)⁴.

La disciplina italiana, in passato riunita già in un testo unico nel 1881, fu rinnovata nella legge 633/1941 ed integrata nel 1942 da alcune disposizioni del Codice Civile. Su questo, che possiamo definire come il nucleo originario dell'attuale normativa, sono state operate numerose interpolazioni dovute ad alcune riforme di stampo pubblicistico – trattate di seguito – ma soprattutto date dall'adesione all'Unione Europea.

In tema di “nuovo diritto d'autore”, si citano in particolare il Libro Verde del 1988⁵, il Libro Verde del 1995⁶, la comunicazione del 1996⁷, la decisione del 1998⁸, la comunicazione del 28 maggio 2002 “e-Europe”⁹.

Di seguito si riportano gli estremi della disciplina europea e quelli dei corrispondenti provvedimenti di recepimento in Italia.

Unione Europea	-> Italia
Dir. 1991/250/CE	D. Lgs. 518/1992 in merito alla tutela dei programmi per elaboratore
Dir. 1992/100/CE	D. Lgs. 685/1994, in tema di noleggio e prestito
Dir. 1996/9/CE	D. Lgs. 169/1999, relativo alla tutela delle banche di dati
Dir. 1998/71/CE	D. Lgs. 95/2001, protezione giuridica di disegni e modelli
Dir. 2001/29/CE	D. Lgs. 68/2003, disciplina degli aspetti relativi alla Società dell'Informazione.
Dir. 2004/48/CE	D. Lgs. 140/2006, sul rispetto dei diritti di proprietà intellettuale

² Si ritiene che, pur in mancanza di espressa formulazione, la tutela del diritto d'autore rientri nella garanzia della libertà di espressione offerte dalla Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali.

³ Convenzione Generale sugli aspetti commerciali della proprietà intellettuale, recepita con L. 747/1994.

⁴ WIPO *Copyright Treaty* (WCT) “Trattato sul diritto d'autore” e WIPO *Performances and Phonograms Treaty* (WPPT), “Trattato sulle interpretazioni, le esecuzioni e i fonogrammi”.

⁵ COM (88) 172 def.

⁶ COM (95) 382 def.

⁷ 20 novembre 1996

⁸ Decisione 98/253/CE.

⁹ COM (2002) 263 def.



§. 1.2.2.- Cenni alla disciplina tradizionale del diritto d'autore

Oggetto:

- (1) Opere intellettuali;
- (2) *Software*¹⁰;
- (3) Banche dati (Diritto “*sui generis*”) ¹¹;
- (4) *Industrial design*.

Facoltà contenute:

Tradizionalmente all'autore sono collegati due generi di diritti, la cui caratteristica principale è l'*esclusività*, ossia il fatto che essi sono rivolti *erga omnes*:

- (1) *Diritti Morali*: l'autore ha il diritto di essere riconosciuto quale creatore dell'opera. Tale diritto è inalienabile. L'autore ha sulla sua creazione un potere talmente esteso da avere persino il diritto, personale e intrasmissibile, di ritirarla dal commercio, art. 2582 CC.
- (2) *Diritti Patrimoniali*: l'autore ha il diritto di sfruttare economicamente il prodotto del proprio lavoro intellettuale, art. 2577 CC¹².

Strumenti giuridici di tutela

A prescindere dal regime sanzionatorio e dagli strumenti inibitori, attraverso la licenza – in particolare la *End User License Agreement* (EULA) per il *software* – il produttore determina le condizioni di distribuzione della sua opera. Il principio fondamentale si può riassumere nel ben noto brocardo: *nemo plus iuris transferre potest quam ipse habet*.

Strumenti tecnologici di tutela: il “nuovo diritto d'autore” o il *Digital Copyright*

La necessità di disciplinare la distribuzione e l'utilizzo di opere intellettuali in formato digitale costituisce il maggiore problema dell'attuale diritto d'autore. Le norme stabilite a tal fine sono denominate come *Digital Copyright* e si possono distinguere a seconda che riguardino accorgimenti tecnici o clausole contrattuali.

§. 1.2.3.- La protezione tecnologica: il *Digital Rights Management*

Occorre riconoscere le infinite possibilità concesse all'utente finale da parte delle tecnologie informatiche: non solo il contenuto può essere modificato (ad esempio, rielaborando un'immagine), ma anche e soprattutto l'opera stessa può essere duplicata per un numero infinito di volte. L'obiettivo principale

¹⁰ Definizione dell'OMPI del 1984: «*espressione di un sistema organizzato e strutturato di istruzioni (o simboli) contenute in qualsiasi forma o supporto (nastro, disco, film, circuito), capace direttamente o indirettamente, di far eseguire o far ottenere una funzione, un compito od un risultato particolare per mezzo di un sistema di elaborazione elettronica dell'informazione*». Il diritto il *software* costituisce un *bene immateriale* risultato di un processo intellettuale umano, *corpus mysticum*, che ha valore e consistenza autonoma, a prescindere dal supporto materiale, *corpus mechanicum*, in cui è fissato, TULLIO ASCARELLI. *Teoria della concorrenza e dei beni immateriali. Istituzioni di diritto industriale*, Milano 1960, p. 695. Direttiva 14 maggio 1991, n.250 riguardante «*Tutela giuridica dei programmi per elaboratore*», in G.U.C.E. L 122 del 17 maggio 1991, p. 42, modificata dalla Direttiva 29 ottobre 1993, n. 98 riguardante «*Armonizzazione della durata di protezione del diritto d'autore e di alcuni diritti connessi*», in G.U.C.E. L 290 del 24 novembre 1993, p. 9, recepita nel nostro ordinamento con Decreto Legislativo 29 dicembre 1992, n. 518 «*Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore*» in G.U. 31 dicembre 1992, n. 306.

¹¹ Si tratta di un diritto *sui generis*, dalla controversa collocazione dogmatica. Art. 2 L. 633/1941, punto 9) «*le banche di dati di cui al secondo comma dell'articolo 1, intese come raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo. La tutela delle banche di dati non si estende al loro contenuto e lascia impregiudicati diritti esistenti su tale contenuto*». Cfr. anche la direttiva n. 9 dell'11 marzo 1996, «*Tutela giuridica delle banche di dati*», in G.U.C.E. L 77 del 27 marzo 1996, p. 20.

¹² La durata dei diritti musicali è estesa dai precedenti 50 anni a 70 anni, termine ordinario previsto per i diritti patrimoniali d'autore, Proposta di direttiva del Parlamento Europeo e del Consiglio che modifica la direttiva 2006/116/CE del Parlamento Europeo e del Consiglio concernente la durata di protezione del diritto d'autore e di alcuni diritti connessi, COM/2008/0464 def. – COD 2008/0157.



della ricerca scientifica e dell'elaborazione giuridica è essenzialmente quello di individuare nuovi strumenti per controllare (e quindi limitare) le facoltà dell'utente.

Gli studi più recenti hanno concepito la Gestione digitale dei diritti d'autore (DRM, *Digital Rights Management*), che sono il vero e proprio nucleo di un nuovo sistema tecnologico molto complesso, teso a predeterminare le modalità stesse della fruizione dell'opera e quindi a permettere all'autore il controllo della condotta del destinatario della medesima. Esse, previste dagli accordi internazionali – art. 11 del WCT e art. 18 del WPPT – sono state accolte dalla legislazione sul *copyright* più recente, in U.S.A.¹³ e nell'Unione Europea¹⁴, di conseguenza anche nel nostro ordinamento. Sono, sì, un «*antifurto digitale*»¹⁵, ma anche molto di più. Il fatto che il distributore dell'opera possa mantenere un controllo sull'utilizzo della medesima implica enormi problemi, soprattutto relativamente alla tutela della *privacy* del consumatore (i cui gusti personali possono essere facilmente schedati dai titolari del sistema di protezione).

Si possono distinguere due strumenti nel DRM:

- (1) Le informazioni sul regime dei diritti (CMI, *Copyright Management Information*);
- (2) Le misure tecnologiche di protezione (d'ora in poi MTP).

§. 1.2.3.1.- *Copyright Management Information*

Ogni documento informatico contiene informazioni relative al suo autore, alla data di creazione, all'ultima modifica. Possono essere inseriti ulteriori dati relativi ad esempio ai diritti connessi alla distribuzione, alla registrazione dell'opera stessa, alle facoltà concesse o meno dal produttore al fruitore. Le CMI possono essere ricondotte soprattutto alla tutela dei diritti morali dell'autore: è evidente l'importanza di tali informazioni, nel momento in cui l'opera, in formato elettronico, può essere trasmessa a grande distanza, dove non è possibile controllarne l'autenticità. L'attribuzione delle informazioni sull'autore è detta *watermarking*, e deriva da *watermark*, particolare segno impresso sulla carta a garanzia di autenticità, visibile solamente con luce (come ad esempio nelle banconote).

Le CMI sono state prima previste a livello internazionale – all'art.12 del WCT e all'art. 19 del WPPT – e poi adottate dagli ordinamenti USA¹⁶ e UE¹⁷, quindi recepite dall'Italia come “informazioni elettroniche sul regime dei diritti”¹⁸.

¹³ *The Digital Millennium Copyright Act*, (DMCA) del 28 Ottobre 1998, Pubbl. L. No. 103 – 304.

¹⁴ Si citano, soltanto per quanto riguarda l'Unione Europea, il Libro Verde del 1988, il Libro Verde del 1995, la comunicazione del 1996, la decisione del 1998, la comunicazione del 28 maggio 2002 “eEurope”.

¹⁵ GIUSELLA FINOCCHIARO, *Banche dati al sicuro con lo scudo delle protezioni*, in “Guida al Diritto” (2002), n. 19, p. 55.

¹⁶ Il DMCA definisce le CMI come: «*identifying information about the work, the author, the copyright owner, and in certain cases, the performer, writer or director of the work, as well as the terms and conditions for use of the work, and such other information as the Register of Copyright may prescribe by regulation*» DMCA, section 1201 (c). Costituiscono reati due particolari condotte, relativamente alle informazioni sul copyright: (1) l'attribuzione di false informazioni, o la loro distribuzione «*if done with the intent to induce, enable, facilitate or conceal infringement*» sezione 1201 (a); (2) la rimozione o alterazione dei segni senza autorizzazione, o la loro distribuzione «*with reasonable ground to know that it will induce, enable, facilitate or conceal the infringement*», sezione 1201 (b).

¹⁷ La direttiva 29/2001 all'art. 7 comma 2 così definisce le “informazioni sul regime dei diritti”: «*qualunque informazione fornita dai titolari dei diritti che identifichi l'opera o i materiali protetti di cui alla presente direttiva o coperti dal diritto sui generis di cui al capitolo III della direttiva 96/9/CE, l'autore o qualsiasi altro titolare dei diritti, o qualunque informazione circa i termini e le condizioni di uso dell'opera o di altri materiali nonché qualunque numero o codice che rappresenti tali informazioni*». In sede UE sono proibite le seguenti condotte dall'art.7 comma 1: «*a) rimuovere o alterare qualsiasi informazione elettronica sul regime dei diritti; b) distribuire, importare a fini di distribuzione, diffondere per radio o televisione, comunicare o mettere a disposizione del pubblico opere o altri materiali protetti ai sensi della presente direttiva o del capitolo III della direttiva 96/9/CE, dalle quali siano state rimosse o alterate senza averne diritto le informazioni elettroniche sul regime dei diritti*».

¹⁸ Art. 102 *quinquies* comma 1 L. 633/1942, introdotto dal D. Lgs. 68/2003: «*identificano l'opera o il materiale protetto, nonché l'autore o qualsiasi altro titolare dei diritti. Tali informazioni possono altresì contenere indicazioni circa i termini o le condizioni d'uso dell'opera o dei materiali, nonché qualunque numero o codice che rappresenti le informazioni stesse o altri elementi di identificazione*». La violazione è pesantemente sanzionata ai sensi dell'art. 171-ter



§. 1.2.3.2.- Misure Tecnologiche di Protezione

Si possono distinguere due categorie di MTP a seconda dell'oggetto del controllo:

- (1) *Controllo sull'accesso alle informazioni* (esempio: la trasmissione criptata delle televisioni a pagamento, pay-per-view) c.d. "accesso condizionato" ai servizi della società dell'informazione¹⁹;
- (2) *Controllo sull'utilizzo delle informazioni* (ad esempio, dispositivi contro la duplicazione dei DVD, oppure attivazione di accorgimenti che impediscono la stampa di un documento, o la copia, o la manipolazione).

La tutela delle MTP – di cui agli art.11 del WCT e art.18 del WPPT - prevista dal DMCA²⁰ e dalla normativa europea²¹, è stata recepita dal nostro ordinamento²².

Per apprezzare la valenza delle "misure tecnologiche di protezione" occorre riferirsi alla disciplina della "riproduzione privata ad uso personale", in particolare, artt. 71 *quinqüies* e *sexies*:

L. 633/1942 «È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da cinque a trenta milioni di lire chiunque a fini di lucro».

¹⁹ Vedasi in tema la L. 22/2003, che estende la tutela penale di cui agli artt. 171 *bis* e *octies* della L.633/1941 alle ipotesi di "distribuzione illecita" di smart cards "piratate".

²⁰ Il DMCA ha inserito nella sezione 1201 del capitolo 12, titolo 17 U.S. Code, il reato di "*Circumvention of Technological Protection Measures*", con cui si punisce lo "sviamento" delle misure tecnologiche predisposte per prevenire l'accesso o la copia di opere protette dal diritto d'autore, nonché l'attività di distribuzione dei dispositivi aventi tale utilizzo. In merito è illuminante l'arresto del programmatore russo DMITRY SKLYAROV da parte dell'FBI, compiuto nel luglio 2001, per aver violato le MTP relative al formato PDF. Il caso scatenò censure da parte della comunità scientifica, l'informatico venne rilasciato ed assolto.

²¹ In sede UE, le MTP sono definite all'art. 6 della DIR 29/2001 come: «*tutte le tecnologie, i dispositivi o componenti che, nel normale corso del loro funzionamento, sono destinati a impedire o limitare atti, su opere o altri materiali protetti, non autorizzati dal titolare del diritto d'autore o del diritto connesso al diritto d'autore, così come previsto dalla legge o dal diritto sui generis previsto al capitolo III della direttiva 96/9/CE. Le misure tecnologiche sono considerate "efficaci" nel caso in cui l'uso dell'opera o di altro materiale protetto sia controllato dai titolari tramite l'applicazione di un controllo di accesso o di un procedimento di protezione, quale la cifratura, la distorsione o qualsiasi altra trasformazione dell'opera o di altro materiale protetto, o di un meccanismo di controllo delle copie, che realizza l'obiettivo di protezione*».

²² Art. 102 *quater* L. 633/1941, con il quale si definisce le MTP come: «*tutte le tecnologie, i dispositivi o i componenti che, nel normale corso del loro funzionamento, sono destinati ad impedire o limitare atti non autorizzati dai titolari dei diritti. Le misure tecnologiche di protezione sono considerate efficaci nel caso in cui l'uso dell'opera o del materiale protetto sia controllato dai titolari tramite l'applicazione di un dispositivo di accesso o di un procedimento di protezione, quali la cifratura, la distorsione o qualsiasi altra trasformazione dell'opera o del materiale protetto, ovvero sia limitato mediante un meccanismo di controllo delle copie che realizzi l'obiettivo di protezione*». Dal punto di vista dell'utente, è molto importante sottolineare che la tutela giuridica dell'opera intellettuale si estende a tali dispositivi, la cui elusione è sanzionata pesantemente. Con riferimento in particolare alle MTP che presiedono all'accesso, ai sensi dell'art. 171 *ter*, «È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da cinque a trenta milioni di lire chiunque a fini di lucro: [...] f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto». Da notare che tale previsione era già operante per effetto della L. 248/2000, la quale aveva anche inserito l'art. 171 *octies*, relativo alle trasmissioni ad accesso condizionato. In merito vedasi la sentenza Cassazione penale 2 luglio 2004, n. 28913, in "Il diritto industriale" (2005), n.3, p.325, con nota di Davide Sangiorgio. Riguardo alle MTP di controllo dell'utilizzo, alla stessa pena è soggetto, lettera f-bis), chi «*fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale*». La produzione o commercializzazione di dispositivi elusivi, invece, è reato ai sensi dell'art. 171 *ter* lett. f bis). L'utilizzo dei dispositivi di elusione delle MTP costituisce illecito amministrativo punito dall'art. 174 *ter*.



- (1) **L'interesse pubblico** (art.71 *quinquies* comma 1) impone all'autore la rimozione delle "misure" su richiesta dell'autorità competente, qualora si renda necessario l'accesso all'opera.
- (2) **L'interesse dell'utente** (art. 71 *sexies* comma 1) invece non può derogare le MTS, nemmeno per effettuare la "copia ad uso personale".

§. 2.- La condivisione dell'informazione in Internet

Ogni comunicazione notoriamente avviene tra un mittente e un destinatario.

Dal punto di vista giuridico, in Rete di solito il mittente è autore del messaggio e l'utente ne è il fruitore.

§. 2.1.- Struttura della comunicazione

Tipo di comunicazione	Qualificazione	Esempio "analogico"	Esempio "digitale"
1 -> 1	Comunicazione	Corrispondenza	Posta elettronica
1 -> Molti	Diffusione	Giornali, radio, TV	Sito web
Molti -> Molti	Condivisione	Bachecca informative (?)	Web 2.0 – social networking (myspace, facebook, twitter)

Proprio perché manca la disciplina– indicata per comodità come "analogica" – della condivisione di informazioni, la Corte di Pennsylvania nel caso *RENO / ACLU*²³ ha ritenuto per la prima volta espressamente che **Internet è un mezzo di comunicazione "diverso" dai precedenti.**

In realtà la decisione *RENO / ACLU* riguardava un antenato dell'attuale WEB 2.0, rappresentato dai sistemi di bacheche elettroniche (BBS) diffuse agli albori della Rete, poi evolutisi in *Newsgroup*, in cui un soggetto – il *provider* – metteva a disposizione degli utenti uno "spazio virtuale" in cui interagire: scambiarsi opinioni, consigli, discutere.

§. 2.2.- Soggetti coinvolti

Tra autore e utente vi è l'intermediazione di un terzo soggetto, il quale trasferisce il messaggio dal primo al secondo.

In realtà, i soggetti coinvolti sono ben quattro, ciascuno dei quali pretende il rispetto delle sue esigenze. Uno schema può aiutare anche in questo caso:

		Beneficiari di diritti			
Soggetti		UTENTE	PROVIDER	AUTORE	STATO
Destinatari di obblighi	UTENTE		Pagamento dei servizi	Pagamento delle opere DRM, MTP	Controllo traffico Ordine pubblico
	PROVIDER	Privacy		Pagamento dei diritti SIAE	Disciplina delle telecomunicazioni Ordine pubblico
	AUTORE	Autorizzazione all'uso	Pagamento dei servizi		Controllo sui contenuti
	STATO	Libertà di informazione Diritti del consumatore	Tutela della concorrenza	Libertà di informazione Diritto d'autore	

²³ Corte Federale degli Stati Uniti, Distretto Orientale della Pennsylvania, sentenza *Reno / American Civil Liberties Union*, 11 giugno 1997.



Per semplificare, si può sostenere che Internet consente due forme di comunicazione: una *verticale* – **1 -> molti**, come sopra si è accennato – e una *orizzontale* – **molti -> molti**, anch'essa già menzionata – e che dapprima si è tentato di disciplinare la Rete estendendo ad essa le forme di responsabilità già operanti per le comunicazioni “analogiche”, per poi giungere a costruire modelli “digitali” che possono essere considerati – almeno relativamente – “nuovi”.

In questa sede interessa considerare come lo Stato si ponga a difesa dell'autore e stabilisca in capo alle altre due figure – utente e provider – una precisa responsabilità.

§. 2.3.- Il contenuto dell'informazione (e il suo controllo)

Il problema non è, come si legge da più parti, soltanto una questione di “bilanciamento di interessi”, perché concerne esigenze incommensurabili. In altri termini, si tratta di *diritti di libertà* che si pongono in diversi piani. Se anche si può assimilare *libertà di informazione* – **cronaca** – e *libertà dall'informazione* – **riservatezza** – invece non si può negare che la **censura** possa essere concepita come una libertà di censurare da parte dello Stato.

In questo senso, si potrebbe forse discutere se vi sia un conflitto tra **due forme di sovranità**, quella tradizionale dello Stato, e quella più recente della Rete, intesa come organizzazione giuridica “autopoietica”, ossia in grado di generarsi da sé, darsi le proprie regole, difendersi.

§. 3.- La responsabilità “verticale” del provider

Qui non ci si interroga sull'eventuale responsabilità diretta del *provider*, ma su quella indiretta derivante dalla condotta illecita dell'utente che si avvale dei suoi servizi.

§. 3.1.- I modelli “analogici” di responsabilità

Tradizionalmente la responsabilità può essere soggettiva o oggettiva, a seconda che si richieda la colpevolezza.

Secondo l'art. 27 comma 1 Cost. «*la responsabilità penale è personale*», quindi ad un soggetto non può essere imputato un crimine commesso da altri.

Responsabilità	Soggettiva	Oggettiva
Diritto civile	Art. 2043 CC, illecito extracontrattuale	Art. 1218, inadempimento contrattuale
		Art. 2050, attività pericolosa
		Art. 2051, cose in custodia -> <i>privacy</i>
Diritto penale	<i>Di regola</i> Art. 43: dolo, colpa	<i>Eccezionale</i> Art. 57, responsabilità del direttore di testata giornalistica “a titolo di colpa”



§. 3.2.- *La discussione*

Nel tentativo di ricollegare una responsabilità indiretta al *provider*, di solito si utilizzano due argomenti, ciascuno dei quali si presta ad obiezioni:

Argomento	Obiezione
1.- art. 40 c. 2 CP: causalità omissiva impropria ²⁴ . Il provider ha contribuito causalmente all'evento dannoso.	1.- la legge non prevede un obbligo di sorvegliare gli utenti affinché non commettano reati. 2.- in ogni caso ciò determina causalità, ma non prova una colpa, che all'accusa è comunque necessario provare per imputare una responsabilità.
2.- (contro la prima obiezione) per analogia con art. 57: responsabilità oggettiva ²⁵ . Il provider avrebbe dovuto controllare le informazioni diffuse, quindi non serve dimostrare la colpa.	1.- nel diritto penale non si ammette analogia per le norme incriminatrici (art. 14 disp. Prel. C.C.) ²⁶ . 2.- la responsabilità oggettiva in diritto penale è un'eccezione.

§. 3.3.- *La soluzione italiana*

In base alla Legge 62/2001²⁷ alcuni sostennero che ogni provider fosse stato equiparato ad un editore. Di conseguenza, sussistendo la responsabilità oggettiva, vi era anche una sorta di legittimazione alla censura relativamente ad ogni forma di espressione in Rete (siti, blog, newsletter).

Con la "Legge comunitaria 2001"²⁸ si è chiarito l'equivoco negandosi una "posizione di garanzia" in capo all'operatore della Rete.

§. 3.4.- *La normativa comunitaria sul "commercio elettronico"*

Il principio fondamentale in tema di informatica non è l'elemento della colpevolezza o della omissione di controllo, ma quello della **disponibilità delle risorse**.

È evidente infatti che:

- (1) "controllare" un insieme di risorse equivale ad averne la "disponibilità", ma non sempre la "effettiva conoscenza";
- (2) l'"accesso" alle stesse significa averne "conoscibilità" senza necessariamente possederne il "controllo".

In realtà, a chiarire definitivamente la responsabilità del provider servì la Direttiva 31/2000²⁹ recepita in Italia con il D. Lgs. 70/2003³⁰, in cui si distinsero tre figure, delineando per ciascuno i requisiti per l'assenza di responsabilità:

²⁴ «Non impedire un evento, che si ha l'obbligo giuridico di impedire, equivale a cagionarlo».

²⁵ «Salva la responsabilità dell'autore della pubblicazione e fuori dei casi di concorso [110], il direttore o il vice-direttore responsabile, il quale omette di esercitare sul contenuto del periodico da lui diretto il controllo necessario ad impedire che col mezzo della pubblicazione siano commessi reati [528, 565, 596-bis, 683, 684, 685], è punito, a titolo di colpa [43], se un reato è commesso, con la pena stabilita per tale reato, diminuita in misura non eccedente un terzo [57-bis, 58-bis]».

²⁶ «Le leggi penali e quelle che fanno eccezione a regole generali o ad altre leggi non si applicano oltre i casi e i tempi in esse considerati [12; 1, 201 c.p.]».

²⁷ L. 7 marzo 2001, n. 62 (in Gazz. Uff., 21 marzo, n. 67). «Nuove norme sull'editoria e sui prodotti editoriali e modifiche alla legge 5 agosto 1981, n. 416».

²⁸ L. 1 marzo 2002, n. 39 (in Suppl. ordinario n. 54 alla Gazz. Uff., 26 marzo, n. 72). «Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee. Legge comunitaria 2001».

²⁹ Direttiva n. 31 del 8 giugno 2000 - 08/06/2000, n. 31 - 00/31/CE, G.U.C.E. 17/07/2000, n. 178.



- (1) chi compie mera attività di trasmissione “*mere conduit*” [art.14]³¹: poiché da egli non dipende la scelta di trasmettere o meno i dati all’utente;
- (2) chi le memorizza temporaneamente al fine di un nuovo inoltro “*caching*” [art.15]³²: la stessa modalità di erogazione dei servizi informatici non permette un controllo dei contenuti, in quanto “automatica, intermedia e temporanea”;
- (3) chi ospita presso di sé le informazioni create da altri “*hosting*” [art.16]³³: il contenuto delle informazioni è semplicemente determinato da altri soggetti.

L’assenza di un dovere di sorveglianza è stata espressamente stabilita con l’art. 17³⁴, ma ciò può correttamente operare solo per le comunicazioni fondate su una logica “verticale”, client / server.

³⁰ D. Lgs. 9 aprile 2003 n.70 (in Suppl. ordinario n. 61 alla Gazz. Uff., 14 aprile, n. 87) «Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell’informazione nel mercato interno, con particolare riferimento al commercio elettronico».

³¹ Art. 14: «1. Nella prestazione di un servizio della società dell’informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione, il prestatore non è responsabile delle informazioni trasmesse a condizione che: a) non dia origine alla trasmissione; b) non selezioni il destinatario della trasmissione; c) non selezioni né modifichi le informazioni trasmesse. 2. Le attività di trasmissione e di fornitura di accesso di cui al comma 1 includono la memorizzazione automatica, intermedia e transitoria delle informazioni trasmesse, a condizione che questa serva solo alla trasmissione sulla rete di comunicazione e che la sua durata non ecceda il tempo ragionevolmente necessario a tale scopo. 3. L’autorità giudiziaria o quella amministrativa, avente funzioni di vigilanza, può esigere, anche in via d’urgenza, che il prestatore, nell’esercizio delle attività di cui al comma 2, impedisca o ponga fine alle violazioni commesse».

³² Art.15: «1. Nella prestazione di un servizio della società dell’informazione, consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, il prestatore non è responsabile della memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta, a condizione che: a) non modifichi le informazioni; b) si conformi alle condizioni di accesso alle informazioni; c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del d) non interferisca con l’uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull’impiego delle informazioni; e) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l’accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l’accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un’ autorità amministrativa ne ha disposto la rimozione o la disabilitazione. 2. L’autorità giudiziaria o quella amministrativa aventi funzioni di vigilanza può esigere, anche in via d’urgenza, che il prestatore, nell’esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse».

³³ Art. 16: «1. Nella prestazione di un servizio della società dell’informazione, consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore: a) non sia effettivamente a conoscenza del fatto che l’attività o l’informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l’illiceità dell’attività o dell’informazione; b) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l’accesso. 2. Le disposizioni di cui al comma 1 non si applicano se il destinatario del servizio agisce sotto l’autorità o il controllo del prestatore. 3. L’autorità giudiziaria o quella amministrativa competente può esigere, anche in via d’urgenza, che il prestatore, nell’esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse».

³⁴ Art. 17 (Assenza dell’obbligo generale di sorveglianza) «1. Nella prestazione dei servizi di cui agli articoli 14, 15 e 16, il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, nè ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. 2. Fatte salve le disposizioni di cui agli articoli 14, 15 e 16, il prestatore è comunque tenuto: a) ad informare senza indugio l’autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell’informazione; b) a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l’identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite 3. Il prestatore è civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall’autorità giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l’accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l’accesso, non ha provveduto ad informarne l’autorità competente»



§. 3.5.- La condivisione “orizzontale”: il peer to peer

Quanto rilevato sinora riguarda ancora una logica “verticale”.

In realtà occorre spostarsi ad una dimensione ulteriore, quella che è propria della Rete e che era sconosciuta ai *mass media* precedenti.

In via preliminare occorre fornire alcuni cenni sul funzionamento delle reti di *file sharing*, per poter comprendere le ragioni della difficoltà di applicare ad esse la disciplina ordinaria.

§. 3.5.1.- Il Peer to Peer: reti “ibride” (Napster) e reti “pure” (Gnutella)

In realtà occorre distinguere almeno due tipi di reti *p2p*, quelle “ibride” e quelle “pure”.

In merito alle *prime*, occorre precisare che si tratta delle versioni più risalenti (si parla comunque di almeno cinque anni!), in cui vi è ancora traccia di una struttura *verticalistica*. **Napster**, per esempio, metteva a disposizione degli utenti i suoi server. In essi erano memorizzati gli indici delle opere disponibili alla condivisione. Dunque le informazioni venivano, sì, condivise tra i diversi client, ma le connessioni dirette erano instaurate sulla base delle indicazioni reperibili presso i server centrali. **EMule** funziona allo stesso modo.

Le *seconde*, invece, sono completamente orizzontali, dunque si realizza quella che è la vera e propria condivisione delle risorse. Ne sono esempio **Gnutella** e anche molti altri programmi di *file sharing* concepiti negli ultimi anni, alcuni dei quali caratterizzati dall'anonimato degli utenti (gli indirizzi IP sono mascherati) che generano traffico crittografato, relativamente inattaccabile dall'esterno.

Una forma intermedia tra i due sistemi è quella utilizzata da **BitTorrent**, in cui l'indice dei *files* disponibili in rete non è che un file, che può essere salvato in un qualunque *server*, anche all'insaputa del suo titolare, per poi essere elaborato da un apposito programma *client*.

In sintesi:

Sistema	Napster	BitTorrent	Gnutella
qualificazione	P2p ibrido	P2p ibrido	P2p puro
funzionamento	Un server ha la specifica funzione di indicizzare i <i>files</i> condivisi	Un file contiene l'indice dei <i>files</i> condivisi, reindirizzando i pacchetti in cui essi sono suddivisi.	Gli utenti condividono anche gli indici.

È evidente la difficoltà di attribuire una qualche forma di responsabilità indiretta al provider sulla base dei concetti sviluppati precedentemente.

Che responsabilità può avere il fornitore di un tale servizio per i contenuti che sono scambiati o condivisi dagli utenti, anche in modo anonimo, visto che non può accedere alle informazioni o conoscere se il materiale che circola sia effettivamente protetto da copyright o meno?

§. 3.5.2.- The Pirate Bay come Google?

Il 17 aprile 2009, un tribunale svedese ha condannato al pagamento di una ingente somma di denaro i titolari³⁵ del sito <http://thepiratebay.org/> che ospita un motore di ricerca per files “.torrent”.

In Italia, il 10 agosto 2008 è avvenuto il blocco del DNS del sito svedese per ordine della Procura della Repubblica di Bergamo – nel corso di un'indagine relativa al sito “Columbo-BT.org”, seguito dall'attivazione di un analogo sito italiano <http://labaia.org> e subito dopo dal suo sequestro. Il 24 settembre 2008 il DNS è stato sbloccato.

La questione sulla liceità di tale iniziativa può essere così strutturata:

³⁵ Gottfrid Svartholm (anakata), Fredrik Neij (TiAMO) e Peter Sunde (brokep), oltre a Carl Lundstrm, semplice finanziatore.



Argomento a favore	Argomento contrario
1.- il sito non contiene materiale illecito come tale	1.- il materiale consente comunque di raggiungere materiale illecito
2.- in ogni caso, si tratta di un motore di ricerca, come ce ne sono tanti, in cui il contenuto non è filtrato.	2.- certo, ma il provider offre un insieme di contenuti idonei a suggerire agli utenti pratiche illecite e dunque facilita la violazione del copyright.
3.- il provider non ci guadagna niente dalla condotta illecita degli utenti.	3.- non è vero, perché comunque ci sono gli introiti pubblicitari (banners).
4.- il giudice che ha condannato The Pirate Bay, Tomas Norström, non era imparziale, perché membro di ben due associazioni a tutela del copyright: <i>Swedish Copyright Association</i> e alla <i>Swedish Association for the Protection of Intellectual Property</i>	4.- è una questione di forma (?)

In realtà la sentenza svedese è interessante perché dimostra come nell'Unione Europea si stia formando un orientamento giurisprudenziale uniforme che prescinde dalle disposizioni normative e che trae origine dai criteri adottati in alcune recenti decisioni statunitensi.

Occorre dunque richiamare queste ultime.

§. 3.5.3.- I precedenti: da *Betamax* a *Grokster*

Nel diritto americano si distinguono diverse forme di responsabilità:

1.- direct infringement

Violazione compiuta da parte di chi "materialmente" viola il copyright.

Egli è direttamente responsabile, per fatto proprio.

In realtà tale principio non si adatta al p2p, perché non si può indicare con certezza l'autore della violazione: chi mette a disposizione il materiale protetto oppure chi lo scarica?

2.- indirect (secondary) infringement:

Nel caso di apparati specificamente concepiti e distribuiti con lo scopo di violare il copyright, sono responsabili "indiretti" i produttori di tali sistemi.

In realtà, ci sono diverse figure comprese all'interno di questa categoria:

modello	Contributory liability	Vicarious liability	"Inducement theory"
Esempio "analogico"	vendita di un'arma da fuoco ad un soggetto che si sa commetterà un delitto.	Questo genere di responsabilità può essere ricollegato alla forma speciale di responsabilità del committente per l'attività compiuta dai commessi, art. 2049 CC, e per il conseguente beneficio economico ottenuto.	
Presupposto della condotta	1.- Direct Infringement: <i>There has been a direct infringement by someone.</i>	1.-Direct Infringement: <i>There has been a direct infringement by someone.</i>	1.- Direct Infringement: <i>There has been a direct infringement by someone.</i>
Elemento soggettivo	2.- Knowledge: <i>The accused contributory infringer knew of the underlying direct infringement. This element can be satisfied by showing either that the contributory infringer actually knew about the infringing activity, or that he reasonably should have known given all the facts and circumstances. At a minimum, however, the contributory infringer</i>	2.- Right and Ability to Control: <i>The accused vicarious infringer had the right and ability to control or supervise the underlying direct infringement. This element does not necessarily set a high hurdle. For example, the Napster court found that the ability to terminate user accounts or block user access to the system was enough to constitute "control."</i>	2.- Intent: <i>The accused inducer intended to promote copyright infringement. Courts generally allow intent to be shown by circumstantial evidence, which means that copyright owners will argue that almost anything could be relevant to establishing what the defendant intended. For example, copyright owners may point to how a company makes</i>



	<i>must have some specific information about infringing activity—the mere fact that the system is capable of being used for infringement, by itself, is not enough.</i>		<i>money, whether it could have modified its software to reduce infringing uses, and whether it was trying to attract infringers as users. As part of the litigation process known as “discovery,” copyright owners may be entitled to search through company and individual emails and other documents, as well as interview potential witnesses under oath, in order to develop evidence of intent.</i>
Condotta materiale	<p>3.- Material Contribution:</p> <p><i>The accused contributory infringer caused or materially contributed to the underlying direct infringement. Merely providing the “site and facilities” that make the direct infringement possible can be enough. Copyright owners have argued that simply providing software or a device that makes infringement possible is “material contribution”³⁶</i></p>	<p>3.- Direct Financial Benefit:</p> <p><i>The accused vicarious infringer derived a “direct financial benefit” from the underlying direct infringement. In applying this rule, however, the courts have not insisted that the benefit be especially “direct” or “financial”—almost any benefit seems to be enough. For example, the Napster court found that “financial benefit exists where the availability of infringing material acts as a draw for customers” and the growing user base, in turn, makes the company more attractive to investors³⁷</i></p>	<p>3.- Affirmative Act:</p> <p><i>The accused inducer has made statements or taken other active steps directed at encouraging infringing uses. Examples of affirmative steps may include advertising a product for infringing uses, instructing users how to infringe (including when providing customer support), or anything else that “entices or persuades” a user to commit infringement. It can also include promotional efforts aimed at deliberately attracting infringers to use your product (e.g., trying to attract the users of the old Napsterservice).</i></p>
Casi di riferimento	Betamax ³⁸ , Napster ³⁹ , Aimster ⁴⁰		Grokster ⁴¹

Come affermato nella sentenza **Betamax** – e perciò il principio fu definito “*Betamax rule*” o “*Sony safe Harbour*” – ad escludere la responsabilità del fornitore è sufficiente che il prodotto sia idoneo ad un utilizzo lecito: *«the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial non-infringing uses.»* (Sony 464 U.S. at 442).

La dottrina fondata su tale decisione è stata superata – per quanto riguarda la condivisione di *files* – prima con la sentenza **Napster** e poi con la sentenza **Aimster**.

Quanto a Napster, occorre tenere conto di due argomenti:

1.- i distributori del software avevano diretta e specifica conoscenza delle violazioni del copyright, date le modalità tecniche del suo funzionamento e avrebbero tecnicamente potuto, quindi avrebbero giuridicamente dovuto, rimuovere il materiale illecito dalle liste presenti sui loro *servers* con un efficace sistema di filtraggio automatico.

2.- ai fini della decisione, non si considerò il fatto che il servizio fosse offerto gratuitamente agli iscritti. In effetti il beneficio economico diretto diventa irrilevante in presenza di milioni di utenti affezionati.

Quanto ad Aimster, si affermò che:

³⁶ Requisiti tratti dallo Studio Di Fred Von Lohmann, reperibile presso il sito www.eff.org: “*What peer-to-peer developers need to know about copyright law*”, p. 4. L'autore è stato anche difensore di Grokster nella causa contro le *major*s.

³⁷ Studio di Von Lohmann, p. 5.

³⁸ Sony v. Universal City Studios, 464 U.S. 417 (1984)

³⁹ A&M Records v. Napster, 239 F.3d 1004 (9th Cir. 2001)

⁴⁰ In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003)

⁴¹ MGM v. Grokster, 125 S.Ct. 2764 (2005).



1.- è onere del convenuto quello di provare in giudizio l'idoneità del prodotto ad un utilizzo lecito.

2.- il fatto che le trasmissioni nella rete p2p fossero criptate venne considerato non una prova dell'impossibilità di conoscere da parte del *provider*, ma della volontà artificiosa di porsi fuori dalla legalità, eludendo il requisito della conoscibilità richiesto dalla *contributory liability*.

§. 4.- La responsabilità dell'utente: *Data Retention* sul traffico telematico

Con riferimento alla responsabilità diretta dell'utente, si è assistito ad un inasprimento delle sanzioni, amministrative e penali.

§. 4.1.- *Le sanzioni previste dalla legge sul diritto d'autore*

Il "Decreto Urbani"⁴² ha introdotto per la prima volta nel nostro ordinamento le sanzioni contro il *file sharing*.

Ciò è testimoniato dalla sentenza Cassazione penale sez. III 22 novembre 2006 n. 149 di cui si riportano due massime:

«Il downloading di programmi per elaboratore e di altre opere dell'ingegno tutelati non è penalmente perseguibile (anno 1999) in assenza dello scopo di lucro poiché gli imputati non hanno tratto alcun profitto economico dalla predisposizione del server FTP, mentre dalla utilizzazione dello stesso traevano sostanzialmente vantaggio i soli utenti del server medesimo. Restano pertanto esclusi dall'applicazione degli art. 171 bis e 171 ter, così come vigenti all'epoca dei fatti, le condotte poste in essere, riconducibili alle ipotesi del conseguimento del fine di profitto, in quanto, finalizzate al prelievo di programmi - da parte degli utenti abilitati all'utilizzo del server - in cambio del conferimento di materiale informatico» (Diritto).

«Prima dell'entrata in vigore della l. n. 248 del 2000, che ha modificato la l. n. 633 del 1941, l'abusiva duplicazione di software era punita penalmente solo in presenza di "scopo di lucro" e non anche in caso di "scopo di profitto". Il fine di lucro deve concretizzarsi nel perseguimento di un vantaggio economicamente apprezzabile. Quindi, nella vigenza della precedente normativa, non poteva ritenersi reato lo scambio di software che avvenisse esclusivamente a titolo gratuito e non fosse connesso a forme di pubblicità o ad altra utilità economica tramite la realizzazione di un server Ftp ("File transfer protocol")»

Dal punto di vista tecnologico, la fattispecie non riguardava ancora il *peer to peer*, ma strumenti di condivisione client/server:

Alla luce delle recenti modifiche normative, la condotta dell'utente assume diversa rilevanza a seconda di come si manifesta e del suo scopo.

⁴² L. 21 maggio 2004 n. 128 (in Gazz. Uff., 22 maggio, n. 119). «Conversione in legge, con modificazioni, del decreto-legge 22 marzo 2004, n. 72, recante interventi per contrastare la diffusione telematica abusiva di materiale audiovisivo, nonché a sostegno delle attività cinematografiche e dello spettacolo».



	Upload (anche condivisione?)	Download (soltanto scaricamento)
Scopo di profitto o di lucro	<p>Art. 171 <i>ter</i> comma 2 lett. a bis)</p> <p>Condivisione + fine di lucro + uso non personale</p> <p><i>«È punito con la reclusione da uno a quattro anni e con la multa da cinque a trenta milioni di lire chiunque [...] in violazione dell'articolo 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa».</i></p> <p>Art. 171 <i>ter</i> comma 3</p> <p>Attenuante</p> <p><i>«La pena è diminuita se il fatto è di particolare tenuità».</i></p>	<p>Art. 171 <i>bis</i> comma 1</p> <p>Duplicazione abusiva + per trarne profitto⁴³</p> <p><i>«Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da lire cinque milioni a lire trenta milioni. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a lire trenta milioni se il fatto è di rilevante gravità».</i></p>
Senza scopo di profitto o di lucro	<p>Art. 171 lett. a bis)</p> <p>Sanzione penale</p> <p><i>«Salvo quanto previsto dall'art. 171-bis e dall'articolo 171-ter, è punito con la multa da lire 100.000 a lire 4.000.000 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma [...] mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa».</i></p>	<p>Art. 174 <i>ter</i></p> <p>Sanzione amministrativa</p> <p><i>«1. -Chiunque abusivamente utilizza, anche via etere o via cavo, duplica, riproduce, in tutto o in parte, con qualsiasi procedimento, anche avvalendosi di strumenti atti ad eludere le misure tecnologiche di protezione, opere o materiali protetti, oppure acquista o noleggia supporti audiovisivi, fonografici, informatici o multimediali non conformi alle prescrizioni della presente legge, ovvero attrezzature, prodotti o componenti atti ad eludere misure di protezione tecnologiche è punito, purché il fatto non concorra con i reati di cui agli articoli 171 , 171-bis , 171-ter , 171- quater , 171-quinquies , 171-septies e 171-octies , con la sanzione amministrativa pecuniaria di euro 154 e con le sanzioni accessorie della confisca del materiale e della pubblicazione del provvedimento su un giornale quotidiano a diffusione nazionale.</i></p> <p><i>2. In caso di recidiva o di fatto grave per la quantità delle violazioni o delle copie acquistate o nolleggiate, la sanzione amministrativa è aumentata sino ad euro 1032,00 ed il fatto è punito con la confisca degli strumenti e del materiale, con la pubblicazione del provvedimento su due o più giornali quotidiani a diffusione nazionale o su uno o più periodici specializzati nel settore dello spettacolo e, se si tratta di attività imprenditoriale, con la revoca della concessione o dell'autorizzazione di diffusione radiotelevisiva o dell' autorizzazione per l' esercizio dell' attività produttiva o commerciale».</i></p>

⁴³ Il *profitto* è un concetto più esteso del *lucro*, perché comprende una mancata spesa.



Sanzione comune	Art. 174 bis Sanzione amministrativa <i>«Ferma le sanzioni penali applicabili, la violazione delle disposizioni previste nella presente sezione è punita con la sanzione amministrativa pecuniaria pari al doppio del prezzo di mercato dell' opera o del supporto oggetto della violazione, in misura comunque non inferiore a euro 103,00. Se il prezzo non è facilmente determinabile, la violazione è punita con la sanzione amministrativa da euro 103,00 a euro 1032,00. La sanzione amministrativa si applica nella misura stabilita per ogni violazione e per ogni esemplare abusivamente duplicato o riprodotto»..</i>
-----------------	---

Il fatto di prevedere una sanzione penale per la condivisione di files è stato ritenuto eccessivo, pertanto la sanzione è stata mitigata di recente con un espediente processuale, poiché si prevede la possibilità di estinzione del reato con *oblazione*, art. 171 comma 2⁴⁴.

Se tuttavia la situazione si è mitigata dal punto di vista processuale, rimangono importanti poteri istruttori in capo alle Forze dell'Ordine. Infatti nel Decreto Urbani vi è l'affermazione di un principio relativo ai *provider*, ossia la sussistenza di un dovere, sanzionato amministrativamente, su richiesta dell'autorità giudiziaria, di comunicare informazioni utili alla repressione di condotte illecite e di inibire/rimuovere contenuti informativi dai sistemi amministrati, salva la disciplina in premessa (D. Lgs. 70/2003).

⁴⁴ «Chiunque commette la violazione di cui al primo comma, lettera a-bis), e' ammesso a pagare, prima dell'apertura del dibattimento, ovvero prima dell'emissione del decreto penale di condanna, una somma corrispondente alla meta' del massimo della pena stabilita dal primo comma per il reato commesso, oltre le spese del procedimento. Il pagamento estingue il reato». Le disposizioni originarie della Legge Urbani sono state mitigate dalla L. 31 marzo 2005 n. 43 (in Gazz. Uff., 1 aprile, n. 75). «Conversione in legge, con modificazioni, del decreto-legge 31 gennaio 2005, n. 7, recante disposizioni urgenti per l'università e la ricerca, per i beni e le attività culturali, per il completamento di grandi opere strategiche, per la mobilità dei pubblici dipendenti, nonché per semplificare gli adempimenti relativi a imposte di bollo e tasse di concessione. Sanatoria degli effetti dell'articolo 4, comma 1, del decreto-legge 29 novembre 2004, n. 280».



§. 4.2.- Data Retention: evoluzione e prospettive

In linea di principio, il Codice per la protezione dei dati personali⁴⁵ prevede termini molto rigorosi per la conservazione dei dati relativi alle connessioni⁴⁶.

§. 4.2.1.- Il decreto "Pisanu"

Per combattere il terrorismo internazionale, il Governo ha emanato il decreto legge 144/2005, poi convertito, che ha imposto al *provider* una serie di obblighi specificati in un successivo decreto ministeriale⁴⁷.

⁴⁵ D. Lgs. 30 giugno 2003, n.196 (in Suppl. ordinario n. 123 alla Gazz. Uff., 29 luglio, n. 174). «Codice in materia di protezione dei dati personali».

⁴⁶ In particolare, art. 123 (Dati relativi al traffico): «1. I dati relativi al traffico riguardanti abbonati ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica, fatte salve le disposizioni dei commi 2, 3 e 5. 2. Il trattamento dei dati relativi al traffico strettamente necessari a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione, è consentito al fornitore, a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale»; art. 132 (Conservazione di dati di traffico per altre finalità): «1. Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico inclusi quelli concernenti le chiamate senza risposta sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione. 1-bis. I dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per trenta giorni. 2. [abrogato] 3. Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto motivato del pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall' articolo 391-quater del codice di procedura penale , ferme restando le condizioni di cui all' articolo 8 , comma 2, lettera f). per il traffico entrante. 4. [abrogato] 4-bis [abrogato]. 4-ter. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi. 4-quater. Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-ter deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'articolo 326 del codice penale».

⁴⁷ L. 31 luglio 2005 n.155 (in Gazz. Uff., 1 luglio, n. 177) «Conversione in legge, con modificazioni, del decreto-legge 27 luglio 2005, n. 144, recante misure urgenti per il contrasto del terrorismo internazionale»; Decreto del Ministro dell'Interno 16 agosto 2005 «Misure di preventiva acquisizione di dati anagrafici dei soggetti che utilizzano postazioni pubbliche non vigilate per comunicazioni telematiche ovvero punti di accesso ad Internet utilizzando tecnologia senza fili, ai sensi dell'articolo 7, comma 4, del decreto-legge 27 luglio 2005, n. 144 convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155» (G.U. 17 agosto 2005, n. 190). Vedasi in merito T.A.R. Lazio, 21 aprile 2008, secondo il quale per l'irrogazione della sanzione amministrativa – in caso di inottemperanza all'obbligo da parte del provider – non è necessaria l'adozione del regolamento attuativo del D. L. 144/2005.



In particolare:

- (1) l'adozione di misure tecnologiche di protezione contro l'accesso abusivo alla connessione;
- (2) l'identificazione degli utenti che accedono alla Rete da postazioni in "luoghi aperti al pubblico", anche wi-fi;
- (3) il monitoraggio dell'attività *on line*;
- (4) la conservazione obbligatoria dei dati "estrinseci" delle comunicazioni per accesso su autorizzazione dell'Autorità Giudiziaria:
 - a. dati telefonici:
 - i. 24 mesi per l'accertamento di reati
 - ii. proroga fino a 48 mesi per delitti:
 1. di cui all'art. 407 comma 2 lett. a) C.P.P.⁴⁸
 2. in danno di sistemi informatici e telematici.
 - b. dati telematici (obbligo introdotto con L. 155/2005):
 - i. 6 mesi
 - ii. proroga fino a 12 mesi per delitti:
 1. di cui all'art. 407 comma 2 lett. a) C.P.P.⁴⁹
 2. in danno di sistemi informatici e telematici.

⁴⁸ «1) delitti di cui agli articoli 285, 286, 416-bis e 422 del codice penale, 291-ter, limitatamente alle ipotesi aggravate previste dalle lettere a), d) ed e) del comma 2, e 291-quater, comma 4, del testo unico approvato con decreto del Presidente della Repubblica 23 gennaio 1973, n. 43; 2) delitti consumati o tentati di cui agli articoli 575, 628, terzo comma, 629, secondo comma, e 630 dello stesso codice penale; 3) delitti commessi avvalendosi delle condizioni previste dall'articolo 416-bis del codice penale ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo; 4) delitti commessi per finalità di terrorismo o di eversione dell'ordinamento costituzionale per i quali la legge stabilisce la pena della reclusione non inferiore nel minimo a cinque anni o nel massimo a dieci anni, nonché delitti di cui agli articoli 270, terzo comma, e 306, secondo comma, del codice penale; 5) delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo, escluse quelle previste dall'articolo 2, terzo comma, della legge 18 aprile 1975, n. 110; 6) delitti di cui agli articoli 73, limitatamente alle ipotesi aggravate ai sensi dell'articolo 80, comma 2, e 74 del testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza approvato con decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, e successive modificazioni; 7) delitto di cui all'articolo 416 del codice penale nei casi in cui è obbligatorio l'arresto in flagranza [380]; 7-bis) dei delitti previsti dagli articoli 600, 600-bis, primo comma, 600-ter, primo comma, 601, 602, 609-bis nelle ipotesi aggravate previste dall'articolo 609-ter, 609-quater, 609-octies del codice penale»;

⁴⁹ «1) delitti di cui agli articoli 285, 286, 416-bis e 422 del codice penale, 291-ter, limitatamente alle ipotesi aggravate previste dalle lettere a), d) ed e) del comma 2, e 291-quater, comma 4, del testo unico approvato con decreto del Presidente della Repubblica 23 gennaio 1973, n. 43; 2) delitti consumati o tentati di cui agli articoli 575, 628, terzo comma, 629, secondo comma, e 630 dello stesso codice penale; 3) delitti commessi avvalendosi delle condizioni previste dall'articolo 416-bis del codice penale ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo; 4) delitti commessi per finalità di terrorismo o di eversione dell'ordinamento costituzionale per i quali la legge stabilisce la pena della reclusione non inferiore nel minimo a cinque anni o nel massimo a dieci anni, nonché delitti di cui agli articoli 270, terzo comma, e 306, secondo comma, del codice penale; 5) delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo, escluse quelle previste dall'articolo 2, terzo comma, della legge 18 aprile 1975, n. 110; 6) delitti di cui agli articoli 73, limitatamente alle ipotesi aggravate ai sensi dell'articolo 80, comma 2, e 74 del testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza approvato con decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, e successive modificazioni; 7) delitto di cui all'articolo 416 del codice penale nei casi in cui è obbligatorio l'arresto in flagranza [380]; 7-bis) dei delitti previsti dagli articoli 600, 600-bis, primo comma, 600-ter, primo comma, 601, 602, 609-bis nelle ipotesi aggravate previste dall'articolo 609-ter, 609-quater, 609-octies del codice penale»;



§. 4.2.2.- *La giurisprudenza comunitaria: il caso "Promusicae"*

Si consideri la sentenza resa a sezioni unite dalla CCGE del 29 gennaio 2008⁵⁰, di cui si trascrive il dispositivo.

«La direttiva del Parlamento europeo e del Consiglio 8 giugno 2000, 2000/31/CE, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("direttiva sul commercio elettronico"), la direttiva del Parlamento europeo e del Consiglio 22 maggio 2001, 2001/29/CE, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, la direttiva del Parlamento europeo e del Consiglio 29 aprile 2004, 2004/48/CE, sul rispetto dei diritti di proprietà intellettuale, e la direttiva del Parlamento europeo e del Consiglio 12 luglio 2002, 2002/58/CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), non impongono agli Stati membri, in una situazione come quella oggetto della causa principale, di istituire un obbligo di comunicare dati personali per garantire l'effettiva tutela del diritto d'autore nel contesto di un procedimento civile. Tuttavia, il diritto comunitario richiede che i detti Stati, in occasione della trasposizione di tali direttive, abbiano cura di fondarsi su un'interpretazione delle medesime tale da garantire un giusto equilibrio tra i diversi diritti fondamentali tutelati dall'ordinamento giuridico comunitario. Inoltre, in sede di attuazione delle misure di recepimento delle dette direttive, le autorità e i giudici degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme a tali direttive, ma anche evitare di fondarsi su un'interpretazione di esse che entri in conflitto con i detti diritti fondamentali o con gli altri principi generali del diritto comunitario, come, ad esempio, il principio di proporzionalità».

In massima sintesi, gli Stati membri dell'Unione Europea hanno facoltà – non obbligo, come per i reati – di prevedere la comunicazione dei dati relativi al traffico telefonico all'interno di procedimenti civili.

Tribunale di Roma, 17 marzo 2008:

«L'acquisizione gratuita, tramite il "file-sharing", di opere protette dai diritti di proprietà intellettuale, consentita agli utenti da determinati siti internet, non giustifica l'obbligo di "discovery" al "provider", consistente nella rivelazione dei dati idonei ad identificare i consumatori utenti del servizio informatico ed utilizzatori dei programmi di file-sharing, anche alla luce della vigente normativa comunitaria, in quanto nel bilanciamento tra il diritto di proprietà intellettuale e il diritto alla riservatezza la prevalenza del primo sul secondo è giustificata unicamente se unita alla lesione di interessi della collettività protetti da diritto penale.

La domanda tesa all'ottenimento dei dati personali degli utenti della rete Internet per verificare l'identità di chi abbia commesso illeciti in tema di proprietà intellettuale non è ammessa, risultando prevalente il diritto alla riservatezza dei dati.

L'ordine di discovery, pur essendo ammesso dal d.lg. 140/2006, con cui si è data attuazione alla "direttiva enforcement" non può essere emesso laddove sussista un ragionevole rischio di violare il diritto alla riservatezza degli utenti della rete Internet».

Al contrario, vi sono altre pronunce secondo le quali il diritto alla riservatezza degli utenti cede di fronte al *copyright*, anche in sede di provvedimenti d'urgenza:

Tribunale di Roma, ord. 18 agosto 2006.

Tribunale di Roma, sez. marchi, ord. 9 febbraio 2007

⁵⁰ Sentenza della Corte (Grande Sezione) 29 gennaio 2008 (domanda di pronuncia pregiudiziale proposta dal Juzgado de lo Mercantil n. 5 de Madrid - Spagna) - Productores de Música de España (Promusicae) / Telefónica de España SAU (Causa C-275/06), in G.U.U.E. C 212 del 2 settembre 2006.



Tribunale di Roma, sez. marchi, ord. 5 aprile 2007
 Tribunale di Roma, sez. marchi, ord. 20 aprile 2007
 Tribunale di Roma, sez. marchi, ord. 26 aprile 2007
 Tribunale di Roma, sez. marchi, ord. 14 luglio 2007

In conclusione, è vero che di regola il *provider* non ha l'obbligo di "censurare" le informazioni, ma è altrettanto vero che gli si impone comunque di "registrare" l'attività degli utenti per esigenze di ordine pubblico⁵¹.

§. 4.2.3.- *La proposta di direttiva "Pacchetto Telecom"*

In sede di Unione Europea è in discussione il c.d. "pacchetto Telecom"⁵² che modifica le precedenti direttive: la Direttiva 2002/21/CE, la Direttiva 2002/19/CE, la Direttiva 2002/20/CE.

Ad ora non si possono fornire osservazioni conclusive, ma soltanto alcune indicazioni di massima.

In particolare, dal testo approvato dal Parlamento Europeo:

- (1) Si afferma che *«l'aspetto più importante da affrontare è la persistente mancanza di un mercato unico delle comunicazioni elettroniche»* (considerando 2): ciò significa che ogni ulteriore valore vi è subordinato;
- (2) Si introduce un'affermazione di principio alquanto equivoca: *«Riconoscendo che Internet è essenziale per l'istruzione e l'esercizio pratico della libertà di espressione e l'accesso all'informazione, qualsiasi restrizione imposta all'esercizio di tali diritti fondamentali dovrebbe essere conforme alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Per quanto riguarda tali temi, la Commissione dovrebbe avviare un'ampia consultazione pubblica»* (considerando 3 bis): ne deriva che non si nega in astratto l'ammissibilità delle restrizioni, quasi che la C.E.D.U. fosse un regolamento dei vincoli e non il fondamento convenzionale delle libertà;
- (3) Si istituisce il BEREC (*Body of European Regulators for Electronic Communications*, ossia Organismo dei regolatori europei delle comunicazioni elettroniche), con il compito di amministrare lo spettro radio e le reti telematiche: da esso dipenderà ciascuna autorità nazionale;
- (4) Si ritiene inderogabile il principio secondo cui: *«non possono essere imposte limitazioni ai diritti e alle libertà fondamentali degli utenti finali, in assenza di una decisione preliminare da parte dell'autorità giudiziaria, in particolare a norma dell'articolo 11 della Carta dei diritti fondamentali dell'Unione europea, sulla libertà di espressione e di informazione, ad eccezione del caso in cui vi sia una minaccia per la sicurezza pubblica e l'intervento dell'autorità giudiziaria sia successivo»* (art. 2 comma 2, lett. f bis), delineando un meccanismo di intervento urgente che prevede l'azione dell'Autorità di Pubblica Sicurezza e successivamente l'interpello dell'Autorità Giudiziaria: ciò esclude, almeno per ora, che l'utente possa essere disconnesso direttamente dal *provider*.

⁵¹ In merito, deve essere menzionata la Convenzione del Consiglio d'Europa presentata a Budapest il 23 novembre 2001 contro la criminalità informatica.

⁵² Proposta di direttiva del Parlamento europeo e del Consiglio recante modifica delle direttive 2002/21/CE che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, 2002/19/CE relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime e 2002/20/CE relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica {SEC(2007) 1472} {SEC(2007) 1473} /* COM/2007/0697 def. - COD 2007/0247 */



§. 5.- Conclusioni

Si possono delineare almeno quattro tendenze:

- (1) Estensione del controllo tecnologico sul *copyright*
- (2) Uniformazione degli strumenti giuridici di tutela della proprietà intellettuale
- (3) Estensione del controllo dei *providers* sull'attività degli utenti
- (4) Deriva "ideologica" della violazione del *copyright*: dopo "il mezzo è il messaggio" di McLuhann, "la violazione del mezzo è il messaggio"?⁵³

§. 6.- Avvertenza

Il presente scritto, di cui le note a piè di pagina sono parte integrante, non costituisce testo scientifico ma vale soltanto ai fini della preparazione dell'esame universitario, quale breve introduzione al tema trattato, esposta giovedì 14 maggio 2009 all'interno del modulo di Informatica insegnamento di Filosofia del Diritto, presso la Facoltà di Giurisprudenza dell'Università degli Studi di Udine.

I testi normativi più rilevanti sono citati per esteso ai fini di maggiore sintesi espositiva. Ai fini della preparazione si considerano presupposte le nozioni fondamentali di diritto civile in tema di diritto d'autore, nonché le informazioni contenute ai seguenti link:

Sui sistemi *peer to peer*:

- ~ <http://it.wikipedia.org/wiki/Napster>
- ~ <http://it.wikipedia.org/wiki/Gnutella>
- ~ <http://it.wikipedia.org/wiki/BitTorrent>
- ~ <http://en.wikipedia.org/wiki/Grokster>
- ~ http://it.wikipedia.org/wiki/Pirate_Bay
- ~ http://it.wikinews.org/wiki/L%27Italia_blocca_The_Pirate_Bay
<http://www.ifpi.org/content/library/Pirate-Bay-verdict-English-translation.pdf>
traduzione NON UFFICIALE della sentenza di condanna ai creatori di "The Pirate Bay".
- ~ <http://embassyofpiracy.org/>
sito legato a "The Pirate Bay", in cui si da appuntamento alla prossima Biennale di Venezia.

Si segnalano inoltre alcune pubblicazioni ulteriori per gli studenti più diligenti.

Sulla responsabilità dei provider:

⁵³ Citazione da <http://embassyofpiracy.org/about/> (consultato il 14 maggio 2009): «*Time is epic, the ecosystem of the Internet is tested and we are here to defend it. Old regimes are passing new laws and new regulations to uphold a failing system that nobody really wants. An internet today is not some virtual entity, but a network that can materialize in everything from court systems, parliaments and phone networks to memes, music and art systems. Internet is a methodology, not a place. The idea of an Embassy of Piracy came up when Piratbyrån and The Pirate Bay got invited to contribute to first Internet Pavilion that will be part of this years Venice Biennial. As an Embassy our task is to represent the freedom of Internet and pirates of Internet and to promote the Kopimi way of life. The Embassy The Embassy has multipliable and modifiable form in shape of a pyramid. By downloading and printing out the foldable paper model you can make the Embassy materialize anywhere; in public spaces, in the forest, at work, school or on your dinner table or for your pets. Remember, when you form an Embassy, you are legally within internet territory. Together we will multiply a growing number of Embassies all over the world. Share your photos of The Embassy on the <http://embassyofpiracy.org> We are all the Embassy, we are all Ambassadors of the freedom of Internet. This adventure is ours to swarm, modify and share*».



- ~ *RENO / ACLU*: Corte Federale degli Stati Uniti, Distretto Orientale della Pennsylvania, sentenza 19 marzo 1997 - 11 giugno 1997, con nota di Vincenzo Zeno Zencovich, in “Diritto dell'informazione e dell'informatica” (1996), n. 4, pag. 604.
- ~ <http://www.senat.fr/dossierleg/pjl07-405.html> recente legge francese
- ~ <http://www.europarl.europa.eu/oeil/file.jsp?id=5563972&fromfiche=1388&mailer=> informazioni sulla procedura COD/2007/0247 “pacchetto Telecom”
- ~ <http://www.europarl.europa.eu/oeil/file.jsp?id=5667672> informazioni sulla procedura COD/2008/0157 “estensione durata copyright”
- ~ SIMONA LAVAGNINI, *La proprietà intellettuale in Internet*, in “AIDA” (2008), pag. 396.

Sugli aspetti penali del Copyright

- ~ DAVID D'AGOSTINI, SABRINA D'ANGELO, LUCA VIOLINO, *Diritto penale dell'informatica. Dai Computer crimes alla digital forensic*, Forlì: Experta 2007.
- ~ GIOVANNI LUCA PERDONÒ, *Le responsabilità penali collegate all'uso di Internet fra comparazione e prospettive di riforma*, in “Diritto dell'informazione e dell'informatica” (2007), p. 323.
- ~ Cassazione penale sez. III 22 novembre 2006 n. 149, in “Diritto d'Autore” (2007), 2, p. 279 con nota di L. Cimenti; in “Guida al diritto” (2007), n. 5, pag. 38 con nota di A. Sirotti Gaudenzi) e in “Rivista di Diritto Industriale” (2008), II, pag. 17, con nota di P. Corbello.
- ~ Convenzione di Budapest
<http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=1&CL=ITA>

Sul DRM:

- ~ La sezione dedicata al DRM sul sito <http://www.eff.org>;
- ~ Il rapporto del marzo 2005 della commissione “Vigevano” reperibile presso il sito del nostro Ministero per l'Innovazione e le Tecnologie (<http://www.innovazione.gov.it>)

Sulla Data Retention:

- ~ CHIARA FATTA, *La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo*, in “Diritto dell'informazione e dell'informatica” (2008), p. 395.
- ~ Tribunale di Roma, 17 marzo 2008, in “Diritto dell'informazione e dell'informatica” (2008), p. 384.
- ~ T.A.R. Lazio, 21 aprile 2008, in “Diritto dell'informazione e dell'informatica” (2008), p. 856 con nota di Antonio Tolone.
- ~ Sentenza della Corte (Grande Sezione) 29 gennaio 2008 (domanda di pronuncia pregiudiziale proposta dal Juzgado de lo Mercantil n. 5 de Madrid - Spagna) - Productores de Música de España (Promusicae) / Telefónica de España SAU (Causa C-275/06), in G.U.U.E. C 64 08.03.2008 pag.9, in “Il diritto industriale” (2009) n. 1 con nota di Alfredo Trotta, e in “Rivista di Diritto Industriale” (2008), II, pag. 328, con nota di Marcello De Cata.
- ~ Tribunale di Roma, ord. 18 agosto 2006, Tribunale di Roma, sez. marchi, ord. 9 febbraio 2007, Tribunale di Roma, sez. marchi, ord. 5 aprile 2007, Tribunale di Roma, sez. marchi, ord. 20 aprile 2007, Tribunale di Roma, sez. marchi, ord. 26 aprile 2007, Tribunale di Roma, sez. marchi, ord. 14 luglio 2007, in “Rivista di Diritto Industriale” (2008), II, pag. 328, con nota di Marcello De Cata.

