

# IL DIRITTO DELL'INFORMAZIONE E DELL'INFORMATICA

Anno XXVII Fasc. 2 - 2011

Pieremilio Sammarco

---

## **LA POSIZIONE DELL'INTERMEDIARIO TRA LA ESTRANEITÀ AI CONTENUTI TRASMESSI E L'EFFETTIVA CONOSCENZA DELL'ILLECITO: UN'ANALISI COMPARATA TRA SPAGNA, FRANCIA E REGOLAMENTAZIONE COMUNITARIA**

---

Virginia Raggi

---

## **BREVI NOTE SULL'ATTIVITÀ DI FILTRAGGIO DEI CONTENUTI INFORMATIVI VEICOLATI IN RETE**

---

Estratto



Milano • Giuffrè Editore

TRIBUNALE  
COMMERCIALE MADRID  
20 SETTEMBRE 2010

PARTI: GESTEVISION  
TELECINCO S.A.,  
TELECINCO CINEMA S.A.U.,  
YOUTUBE LLC

**Internet • Pubblicazione  
video • Attività editoriale  
• Inesistenza.**

*All'interno di una piattaforma informatica accessibile a chiunque, la messa disposizione in favore degli utenti di alcuni video ordinati attraverso una serie di parametri oggettivi e criteri definiti preliminarmente dagli stessi utenti, non comporta alcun lavoro editoriale di creazione o fornitura di contenuti da parte del soggetto intermediario.*

**Provider • Assenza  
preventivo obbligo  
supervisione contenuti  
informativi pubblicati.**

*L'art. 16 della Legge (spagnola) sui Servizi della Società dell'Informazione (LSSI), riproducendo il contenuto dell'art. 14 dalla Direttiva sul Commercio Elettronico, esonera dalla responsabilità i prestatori di servizi di memorizzazione quando: « a) non siano effettivamente a conoscenza del fatto che l'attività o l'informazione che memorizzano o alla quale rinviano è illecita ed è lesiva beni o diritti di terzi suscettibili di risarcimento; b) non appena a conoscenza di tali fatti, agiscano immediatamente per rimuovere le informazioni o per disabilitarne l'accesso ». Conformemente a tale norma, non appare possibile imporre ad alcun prestatore di servizi di*

*intermediazione un obbligo generale di supervisionare i dati che sono trasmessi o immagazzinati sui suoi server, né, ancora meno, di realizzare ricerche attive di fatti o circostanze relative ad attività illecite, atteso che il suo unico obbligo è precisamente quello di collaborare con i titolari dei diritti affinché, dopo aver riconosciuto l'infrazione, si proceda alla rimozione di tali contenuti.*

**Contenuti illeciti**

- Segnalazione
- conoscenza effettiva
- Obbligo di attivazione
- Rimozione.

*Conformemente alla Direttiva Europea in materia di Commercio elettronico ed alla Legge sui Servizi della Società dell'Informazione (LSSI) che in modo chiaro impediscono la previsione di un obbligo di controllo di carattere generale per coloro i quali prestano i servizi di intermediazione, l'assunzione di responsabilità per tali soggetti si configura in relazione ad un concetto giuridico di difficile determinazione come quello dell'« effettiva conoscenza ». Tale criterio implica che l'accertamento dell'illecito (violazione dei diritti di proprietà intellettuale sui contenuti trasmessi dal intermediario) sia effettuato caso per caso su segnalazione anche del soggetto leso, non essendo sufficiente il mero sospetto o la semplice indicazione.*

**M**OTIVI DI DIRITTO. — PRIMO. — In considerazione della singolare natura delle domande oggetto del presente giudizio, risulta opportuno analizzare le richieste delle parti per argomenti compiuti

\* Traduzione della sentenza a cura di Virginia Raggi e Pieremilio Sammarco.

ti che, nella loro concatenazione logica, unificano, senza rendere tuttavia omogenei, sia gli elementi fattuali che quelli propriamente giuridici che costituiscono il cuore della controversia.

La parte attrice, costituita da due società del gruppo Telecinco, ha proposto diverse domande per la asserita violazione dei diritti di proprietà intellettuale contro la società YouTube LLC, per far accertare e dichiarare che la diffusione mediante il sito *web* della convenuta di diverse registrazioni di programmi audiovisivi dei quali è titolare, costituisce violazione dei diritti di proprietà intellettuale ed ha provocato ingenti danni e pregiudizi la cui quantificazione esatta dovrà essere effettuata in un successivo giudizio.

La comparsa della convenuta si fonda su un insieme omogeneo di eccezioni che attengono sia alla natura dell'attività svolta, sia alla normativa applicabile e sia all'interpretazione giurisprudenziale che rinviano direttamente ai punti di seguito esposti.

In primo luogo, appare necessario accertare la natura dell'attività esercitata dalla convenuta in relazione alle registrazioni trasmesse e, in particolare, se tale attività si limiti a costituire un servizio di intermediazione per gli utenti della pagina *web* ovvero, al contrario, se agevoli e crei contenuti, rispetto ai quali si dovrà valutare la responsabilità ai sensi della normativa sulla proprietà intellettuale.

Inoltre, è necessario delimitare precisamente l'ambito di responsabilità della convenuta come mera prestatrice di servizi informatici in relazione ai contenuti diffusi a terzi, tramite la sua piattaforma informatica.

Infine, l'ultima parte delle argomentazioni avrà ad oggetto i danni ed i pregiudizi che parte attrice richiede e che, per la loro natura, sono subordinati all'analisi delle questioni precedenti.

#### **SECONDO. — L'attività di youtube. La prestazione dei servizi di intermediazione e la fornitura di contenuti.**

In considerazione dell'approccio della controversia, la natura dell'attività della società convenuta si configura come uno degli assi portanti sui quali si sviluppa il procedimento, in quanto sia l'insieme dei diritti e degli obblighi sia il regime delle responsabilità variano diametralmente al variare della tesi seguita. Parte attrice, infatti, sostiene che, a dispetto delle apparenze, la pagina *web* della convenuta non si limita a servire da piattaforma attraverso la quale terzi estranei diffondano i loro contenuti ma, al contrario, YouTube interviene direttamente o indirettamente nella loro creazione; diversamente, parte convenuta afferma che la sua attività si limita alla prestazione di servizi di intermediazione, come definito dalla Legge sui Servizi della Società dell'Informazione.

Al fine di procedere all'analisi delle questioni sopra indicate, seguirò, come filo logico, l'impostazione elaborata da parte attrice nell'atto di citazione anche per ragioni di carattere sistematico, atteso che l'esposizione ivi svolta, partendo dagli elementi o parametri che distorcono la natura dell'attività di YouTube come mera prestatrice di servizi, ci consentirà di esaminare l'essenza dell'attività stessa e raggiungere un criterio sufficientemente completo.

Secondo la tesi sostenuta nella domanda, YouTube si presenta come un mero prestatore di servizi di intermediazione, mentre, in realtà, agisce come fornitore di contenuti. A tal fine, ricorre ad una terminologia di matrice comunitaria utilizzando gli archetipi della direttiva, attribuendo agli utenti un artificioso ruolo determinante, camuffando il suo lavoro edito-

riale mediante l'asserita esistenza di procedimenti tecnici ed automatici di selezione, ecc. e tutto ciò al fine di violare i diritti di proprietà intellettuale che appartengono ai terzi, i quali non hanno prestato il loro consenso alla diffusione delle registrazioni.

Parte attrice evidenzia alcuni caratteri che, in tale quadro, consentirebbero di qualificare YouTube come fornitore di contenuti, come di seguito indicato.

Nella domanda viene affermato che YouTube sfrutta i video per il proprio beneficio, quale licenziataria degli utenti: in caso contrario, la società convenuta non avrebbe necessità di ottenere le licenze da parte dei titolari dei diritti per lo sfruttamento del sito *web*. La richiesta della licenza contenuta nella parte denominata « Condizioni di utilizzo » evidenzierebbe, secondo quanto sostiene parte attrice, che la società convenuta non si limita alla mera prestazione dei servizi di intermediazione.

Tuttavia, appare indubbio che l'esigenza di una licenza per gli utenti che caricano i contenuti risulta compatibile con l'esistenza di un mero servizio di intermediazione che può atteggiarsi in diversi modi: si prenda, ad esempio, il servizio di « *hosting 2.0* » il quale a differenza del servizio di « *hosting* » puro, consente agli utenti di caricare materiali per diffonderli e condividerli con altri utenti servizio. E tale è esattamente il servizio offerto da YouTube nel quale è frequente che il prestatore del servizio sia licenziatario dell'utente.

Il secondo carattere distintivo che confermerebbe la tesi di parte attrice consiste nel fatto che la società realizza un'attività dalla stessa denominata « lavoro editoriale », ossia un processo di selezione e controllo dei contenuti dei servizi che mostra nella pagina *web*. Tale attività sarebbe svolta per i c.d. « video in primo piano » che compaiono in una sezione speciale e sono scelti dal personale di YouTube ed anche nel controllo e nella scelta di determinati video che, pur non essendo illeciti, sono ritenuti incompatibili con la direzione editoriale che sostiene la convenuta.

Indipendentemente dal valore giuridico di siffatta tesi, è certo che la prova assunta non accredita, neanche in minima parte, la tesi che viene sostenuta nella domanda.

Come ha dichiarato la testimone Vittoria Grang in udienza, risulta materialmente impossibile attuare un controllo della totalità dei video che vengono messi a disposizione degli utenti perché attualmente vi sono oltre 500 milioni di video. I contenuti, di qualsiasi tipo siano, sono sempre identificati precedentemente dagli utenti che li catalogano e li segnalano affinché YouTube li rimuova.

Analogamente, la selezione di alcuni video per la sezione « video in primo piano » non implica alcun lavoro editoriale atteso che la loro identificazione avviene attraverso una serie di parametri di natura più o meno oggettiva quali, ad esempio, la popolarità del video tra gli utenti. In ogni modo, la selezione di determinati video, rispondendo ad alcuni criteri definiti preliminarmente dagli utenti, non comporta alcun lavoro editoriale di creazione o fornitura di contenuti.

Allo stesso modo, non sembra in contrasto con il carattere di prestazione di servizi di intermediazione il fatto che l'accesso ai video che la società convenuta mette a disposizione degli utenti all'interno del suo sito *web*, sia effettuato attraverso una pagina costruita da YouTube e contraddistinta dal suo marchio.

Parte attrice sostiene, inoltre, che la società convenuta realizzerebbe uno sfruttamento lucrativo e commerciale del suo sito *web* e, tuttavia, non ar-

riva a comprendere la relazione che intercorrerebbe tra questa circostanza e la natura della prestazione del servizio di intermediazione in quanto la stessa Legge dei Servizi della Società dell'Informazione (LSSI) considera che tutti i servizi prestati in relazione alla stessa sono normalmente effettuati a titolo oneroso. Tale tesi è, inoltre, confermata anche da una recente sentenza della Corte di Giustizia dell'Unione Europea ove si evidenzia che « *la semplice circostanza che il servizio di posizionamento sia a pagamento, che Google stabilisca le modalità di pagamento, o ancora che essa dia informazioni di ordine generale ai suoi clienti, non può avere come effetto di privare Google delle deroghe in materia di responsabilità previste dalla direttiva 2000/31* » (Corte di Giustizia Europea, 23 marzo 2010).

Di seguito, conviene ora descrivere dettagliatamente sia il processo di prestazione di servizi di memorizzazione [*hosting*] e il motore di ricerca offerto dalla società convenuta, sia il sistema che la stessa ha installato per verificare i contenuti, o più precisamente, per individuare i contenuti illeciti, atteso che tali attività rilevano sul piano della natura dell'attività della società convenuta e sull'estensione delle sue responsabilità.

In udienza, il Sig. Javier Arias ha fornito una descrizione dettagliata del procedimento che, in via generale, può essere descritto come segue: il procedimento inizia allorché un utente, che deve essersi preventivamente registrato ed ha un *account* attivo, decide di caricare un video sul sito di YouTube. L'utente deve attribuire [al video] un titolo ed anche alcune parole chiave, denominate « *tags* » che consentono di indicizzare il video. È importante rilevare che è proprio l'utente a prendere la decisione sull'utilizzo del video e ad assumersi la responsabilità sul contenuto.

Successivamente, YouTube converte il video attraverso il suo formato *Flash* mediante un procedimento di conversione completamente automatico e lo salva nei suoi *server*. Da quel momento, ogni persona che accede ad Internet può visualizzare i video che altri utenti hanno caricato nel sito *web*. Anche in tal caso, la decisione è integralmente rimessa all'utente.

Analogamente, deve essere segnalato che la società convenuta non fornisce né indica, agli utenti, gli strumenti o i programmi per scaricare i video. È indubbio che attraverso altre piattaforme si possa accedere a tali programmi ma si tratta di servizi che non hanno alcuna relazione con quelli offerti dalla società convenuta.

Inoltre, risulta opportuno descrivere, anche per sommi capi, i programmi che ha installato la società convenuta per la notificazione dell'avviso e l'eliminazione dei contenuti illeciti.

I titolari di diritti che si ritengano pregiudicati dalla diffusione di qualsiasi registrazione, possono richiedere l'eliminazione del contenuto illecito mediante l'identificazione dell'URL completo della pagina di riproduzione, unitamente ad una esposizione motivata del loro diritto. Una volta ricevuto tale avviso, il video viene ritirato automaticamente dal sito Internet di YouTube. Tale avviso viene trasmesso successivamente all'utente che può effettuare ciò che si chiama « *contro-notificazione* ».

L'identificazione del contenuto viene realizzata attraverso un programma che si chiama « *Video-ID* », che richiede la collaborazione del titolare del diritto affinché renda agevole per YouTube individuare gli archivi di riferimento di ciascun video del quale sia titolare e che intende rimuovere. Una volta identificato il video, il titolare può scegliere di bloccare automaticamente la suddetta registrazione in modo che non sia più pubblicata nel sito di YouTube, mediante il controllo dello stesso, ovvero cercare di ottenere un vantaggio mediante l'inserzione pubblicitaria associata al video.

È, tuttavia, indubbio che il sistema di indagine, di notifica degli avvisi e di verifica installato dalla società convenuta è risultato efficace in ogni occasione nella quale Telecinco ha richiesto la rimozione di contenuti dal sito *web* di YouTube. Così, il 14 febbraio 2007, la società attrice chiedeva alla convenuta di ritirare di alcuni contenuti illeciti in relazione ai vari video relativi a serie come i « *Serrano* » o « *Medico de Familia* ». In quello stesso giorno YouTube procedeva al ritiro di un episodio della serie « *Serrano* » e il video è stato immediatamente eliminato dalla pagina *web*. Tale condotta evidenzia che allorché vi è stata l'identificazione dei contenuti, attraverso l'URL, il sistema di protezione della proprietà installato dalla società convenuta è risultato efficace. Conseguentemente, non appare ragionevole affermare che si tratti di meri pretesti, scuse o sistemi ingannevoli, burocratici e farrinosi di impossibile funzionamento.

Tutto ciò evidenzia che la società convenuta offre un servizio di intermediazione nei termini definiti dalla LSSI come « *servizio della società dell'informazione attraverso il quale si agevola la prestazione o la fruizione degli altri servizi della società dell'informazione ovvero l'accesso all'informazione* ».

In tal modo, il regime di responsabilità di YouTube per la prestazione di servizi della società dell'informazione è disciplinato dagli artt. 14-17 della LSSI. Tali precetti stabiliscono un regime di esenzione parziale di responsabilità per i prestatori di servizi aventi ad oggetto i contenuti memorizzati all'interno dei loro siti *web*.

Secondo tale prospettiva, appare chiaro che conformemente con la Direttiva del Commercio Elettronico dell'8 giugno 2000, e con il contenuto della legge di recepimento spagnola, la LSSI, non appare possibile imporre ad alcun prestatore di servizi di intermediazione un obbligo generale di supervisionare i dati che sono trasmessi o immagazzinati, né, ancora meno, di realizzare ricerche attive di fatti o circostanze relative ad attività illecite.

YouTube non è un fornitore di contenuti e perciò non ha l'obbligo di controllare *ex ante* l'illiceità di ciò che viene caricato sul proprio sito *web*; il suo unico obbligo è precisamente quello di collaborare con i titolari dei diritti affinché, dopo aver identificato l'infrazione, si proceda al ritiro (o alla cancellazione) di tali contenuti. Tale dovere di collaborazione è quello che viene riconosciuto anche nella relazione accompagnatoria della LSSI e che è stato debitamente sollecitato dall'attrice mediante i sistemi di ricerca, notifica e verifica installati.

### TERZO. — La responsabilità dei prestatori di servizio. L'effettiva conoscenza.

La società attrice ha formulato anche un secondo gruppo di domande connesse alla qualifica di YouTube come società di servizi di intermediazione.

Nell'atto introduttivo viene sostenuto che, una volta ammesso che la riproduzione dei video nel sito *web* di YouTube non costituisce alcuna attività tipica di creazione di contenuti, bensì la prestazione di un servizio tecnico, la società convenuta sarebbe incorsa nella responsabilità generale prevista dalla LSSI dell'11 luglio 2002.

L'art. 12, 2° comma, della predetta legge prevede una eccezione al regime di responsabilità generale per i servizi di intermediazione ove afferma che « *al fine di determinare la responsabilità dei prestatori di ser-*

vizi per l'esercizio dell'attività di intermediazione, si vedano gli articoli seguenti ».

In tal modo, sotto la rubrica « *Responsabilità dei prestatori di servizio di memorizzazione [hosting]* » l'art. 16 della LSSI, riproducendo il contenuto dell'art. 14 della Direttiva sul Commercio Elettronico, esonera dalla responsabilità i prestatori di servizi di memorizzazione quando: « a) non siano effettivamente a conoscenza del fatto che l'attività o l'informazione che memorizzano o alla quale rinviano è illecita ed è lesiva beni o diritti di terzi suscettibili di risarcimento; b) non appena a conoscenza di tali fatti, agiscano immediatamente per rimuovere le informazioni o per disabilitarne l'accesso ».

Come evidenziano le disposizioni riportate, l'esenzione di responsabilità per i prestatori di servizi di intermediazione si configura in relazione ad un concetto giuridico di difficile determinazione come quello dell'« effettiva conoscenza ».

La legge spagnola sembra preferire un'interpretazione circoscritta e limitata dell'effettiva conoscenza dell'illiceità esigendo che questa sia dichiarata da un organo competente che abbia ordinato di ritirare i dati o che disabiliti l'accesso agli stessi. Secondo la LSSI per « *organo competente* » si devono intendere tutte le autorità giudiziarie o amministrative che agiscono nell'esercizio delle loro competenze istituzionali. Tuttavia, atteso che non esiste alcun organo amministrativo con competenze specifiche in questa materia, gli unici organi competenti per determinare la liceità o l'illiceità dell'informazione sono le autorità giudiziarie.

Secondo un'interpretazione ristretta e ortodossa della normativa, quindi, affinché YouTube abbia una « conoscenza effettiva » del carattere illecito dei contenuti ospitati sul proprio sito *web* e possa essere considerata responsabile, l'illiceità dovrebbe essere segnalata da un organo giudiziario. (In tal senso, si veda la sentenza del Tribunale Provinciale di Madrid del 19 febbraio 2010).

La società attrice favorisce un'interpretazione più flessibile di tale concetto, secondo la quale sarebbe ammissibile la conoscenza effettiva che proviene da un « organo competente » non giurisdizionale ovvero attraverso altre fonti di conoscenza, in conformità con i criteri stabiliti nella sentenza del Tribunale Supremo del 9 dicembre 2009, alla quale si rinvia.

Il primo punto che si può rilevare, tuttavia, è che la sentenza citata fa riferimento ad un presupposto di fatto certamente diverso, ove il nome a dominio registrato era manifestamente diffamatorio, circostanza che non ricorre nel caso che ci occupa.

Probabilmente, l'interpretazione più consolidata è quella in virtù della quale, senza arrivare all'interpretazione ortodossa che restringe il concetto sino a renderlo equivalente ad un accertamento giudiziale, si conformi ai principi che ispirano sia la Direttiva Europea sia la LSSI, che in modo chiaro impediscono la previsione di un obbligo di controllo di carattere generale per coloro i quali prestano i servizi di intermediazione.

Ciò significa che la conoscenza effettiva dovrà essere accertata caso per caso, non essendo sufficiente il mero sospetto o l'indicazione per provarla. La configurazione della conoscenza effettiva esige senza dubbio la collaborazione del soggetto leso. Tale conclusione è quella che si ricava dalla Sentenza del Tribunale de Grande Instance (TGI) di Parigi del 15 aprile 2008, che afferma che « *la conoscenza effettiva del carattere manifestamente*

*illecito di una violazione ai diritti patrimoniali morali degli autori o dei produttori, non implica alcuna conoscenza preventiva ma la collaborazione delle vittime di tali violazioni, le quali devono notificare alla società che memorizza i portali degli utenti, quali diritti assumono essere stati violati».*

Tutto ciò, riportato al caso di specie, significa che, partendo dal principio generale chiaramente stabilito in virtù del quale la società convenuta non ha alcun obbligo di monitorare o controllare preventivamente i contenuti ospitati all'interno del suo sito *web*, spetta alla società attrice portare ad «effettiva conoscenza» di YouTube quei contenuti che possono ledere o violare la titolarità dei suoi diritti di proprietà intellettuale. E ciò deve essere fatto non attraverso una modalità massiccia e incondizionata, bensì individualizzata e concreta perché, come correttamente ritiene la società convenuta, è possibile che molti dei video che gli utenti hanno caricato all'interno del sito *web* di YouTube siano parti di informazioni non tutelate dalla legge che disciplina il diritto d'autore, o mere parodie di programmi di Telecinco, per i quali neanche sussistono strumenti di tutela di tale protezione.

Per tale ragione, la società convenuta ha installato, come sopra esposto, un sistema di ricerca e verifica che consente il controllo da parte dei terzi che si ritengono lesi nei loro diritti di proprietà intellettuale. Sicuramente, possiamo convenire che non si tratta di uno strumento agevole e semplice per la società attrice, in particolare perché comporta l'ingrato compito di rintracciare e controllare i contenuti che sono ospitati sulla pagina *web* della società convenuta. Tuttavia, tale strumento risponde correttamente all'ordine di priorità che tanto il Legislatore comunitario, quanto quello nazionale, hanno stabilito.

Non neghiamo che esiste un ambito di sovrapposizione, carico di tensioni latenti, tra i titolari di diritti di proprietà intellettuale ed i prestatori di servizi di intermediazione nella Rete, che ospitano contenuti di terzi che, occasionalmente, possono violare tali diritti. Tuttavia, il cuore di tale tensione non si localizza nelle possibili incrinature della disciplina, perché le norme si limitano a replicare, come un'eco lontana, il suono che si può ascoltare al ritmo delle trasformazioni sociali che accadono nello strato profondo della struttura economica.

Probabilmente, vi è molta retorica e declamazione epica nei reiterati richiami della società convenuta a quel principio consacrato della libertà di espressione e alla pretesa funzione che in tale conteso afferma di svolgere. Sicuramente, oltre alle lodi, vi è una evidenza che non può essere disconosciuta e che tale processo esemplifica in modo paradigmatico: ossia che il valore dell'informazione è stato convertito nella merce più preziosa del mondo digitalizzato. La sfida delle imprese nella nuova economia non consiste tanto nel proteggere i diritti acquisiti quanto nel creare valore nella diffusione di quei contenuti perché l'evoluzione dei tempi ha evidenziato la sterilità di tutte le frontiere artificiali.

#### **QUARTO. — La azione diretta di inibizione contro il fornitore di servizi di informazione.**

Infine, le società del gruppo Telecinco hanno esercitato un'azione inibitoria nei confronti della società convenuta nella sua qualità di fornitore di servizi di intermediazione alla luce dei precetti contenuti negli artt. 138 e 139 della Legge di Proprietà Intellettuale (Texto refundido de la Ley de



Propiedad Intelectual - TRLPI) integrato dalla legge 19/2006 del 5 giugno [2006] e dalla legge 23/2006 del 7 luglio [2006].

La parte attrice sostiene che alla luce della riforma operata nell'art. 138 della legge di proprietà intellettuale, appare perfettamente ammissibile articolare un'azione contro gli intermediari e prestatori di servizi, benché l'attività di tali intermediari non costituisca essa stessa una violazione.

Tale affermazione risulta solo parzialmente vera in quanto entrambe le norme che disciplinano le azioni inibitorie, stabiliscono una deroga nell'ultimo comma disponendo « *senza pregiudizio delle norme della legge n. 34/2002 dell'11 luglio 2002 sui Servizi della Società dell'Informazione e del Commercio Elettronico* ». Risulta, quindi, di tutta evidenza che la deroga configurata mediante l'espressione « senza pregiudizio » elimini *in nuce* la possibilità dell'esercizio di tale azione nei confronti degli intermediari dei servizi senza che, in tale senso, la legge di proprietà intellettuale aggiunga nulla alla deroga indicata nella LSSI.

In conclusione, atteso quanto sopra, la domanda deve essere rigettata.

QUINTO. — Conformemente a quanto stabilito nell'art. 394 del codice di procedura civile, le spese debbono essere poste a carico di parte attrice.

P.Q.M. — Sono integralmente respinte le richieste contenute nella domanda, e sono posti a carico di parte attrice i costi del presente giudizio.

Si notifichi la presente sentenza alle parti, comunicando loro che avverso la stessa, potrà essere proposto appello scritto.

TRIBUNALE CRETEIL

14 DICEMBRE 2010

PARTI: ISTITUTO NAZIONALE  
PER L'AUDIOVISIVO (INA)  
YOUTUBE LLC

**Provider • Assenza preventivo obbligo supervisione contenuti informativi pubblicati**

- **Contenuti illeciti**
- **Segnalazione**
- **conoscenza effettiva**
- **Obbligo di attivazione**
- **Rimozione**
- **Provider • Successiva pubblicazione medesimi contenuti informativi**
- **Obbligo di nuova notificazione**
- **Inesistenza**
- **Intermediario**
- **Pubblicazione contenuti informativi • Ordine installazione sistema filtraggio • Ammissibile.**

*Secondo l'art. 6-I-2 della legge sul commercio elettronico francese (LCEN), le persone fisiche o giuridiche che, anche a titolo gratuito, effettuano la memorizzazione dei segnali, di scritti, di immagini, di suoni o di messaggi di altra natura forniti dai destinatari dei servizi mettendoli a disposizione del pubblico su Internet, non possono essere ritenute civilmente responsabili per fatti relativi alle attività o alle informazioni memorizzate a richiesta dei destinatari, salvo che non fossero effettivamente a conoscenza del carattere illecito di tali materiali o dei fatti o delle circostanze relative e che, non appena conosciute tali circostanze, si siano prontamente attivate per rimuovere tali dati o per impedirne l'accesso. Tale regime di responsabilità limitato è integrato dall'art.*

*6-I-7 (LCEN) in virtù del quale i fornitori di accesso e di memorizzazione non sono tenuti ad un obbligo di verifica delle informazioni che trasmettono o memorizzano, né ad un obbligo generale di ricercare i fatti o le circostanze che rivelano l'esistenza di attività illecite.*

*Tuttavia, dal momento in cui l'hoster è a conoscenza del carattere illecito delle informazioni memorizzate, l'art. 6-2 (LCEN) lo obbliga ad agire prontamente per rimuovere tali dati o disabilitarne l'accesso.*

*Ogni successiva pubblicazione delle medesime informazioni da parte di terzi e già ritenute illecite, non costituisce un fatto nuovo tale da necessitare una ulteriore notificazione all'intermediario, dal momento che il contenuto ed il carattere di tali informazioni ed i relativi diritti di proprietà intellettuale sono identici.*

*L'intermediario, pertanto, non può richiamare l'esistenza di una generica impossibilità tecnica per esercitare tale attività di sorveglianza, atteso che vi è la capacità di adottare i mezzi e le misure necessarie a rimuovere i contenuti di tipo pedofilo, relativi all'apologia di reato contro l'umanità o all'incitamento all'odio razziale.*

*È ammissibile, nei confronti dell'intermediario, l'ordine di installazione di un sistema di filtraggio di verifica dei video in modo da impedire che i contenuti informativi illeciti non vengano più pubblicati.*

**M**OTIVI. — 1) SULLA RICEVIBILITÀ DELL'AZIONE DELL'INA.  
[omissis]

2) SULLE DOMANDE DELL'INA.

a) *Sullo statuto della società YouTube.*

L'INA afferma che la società YouTube non può essere considerata un *hoster* ai sensi della Legge 24 giugno 2004 che reca norme in tema di fiducia nell'economia digitale [commercio elettronico] (LCEN), poiché persegue una missione e un obiettivo diverso rispetto al fornitore di servizi tecnici definiti dalla legge. La società ricorrente precisa che la società YouTube non ha nulla di un semplice intermediario e non può, quindi, ricevere la qualifica di *hoster* e beneficiare del ben più leggero regime di responsabilità che, per tale posizione, è previsto dalla LCEN.

L'INA espone che, per la società YouTube, deve essere applicato lo statuto dell'editore atteso che la stessa rappresenta un vero e proprio *mass media* che sfrutta il proprio sito internet per mezzo dei video caricati dagli utenti, dei quali la stessa società assicura la valorizzazione attraverso una politica di manipolazione editoriale molto perfezionata, con lo scopo di massimizzare la frequentazione del suo sito e, conseguentemente, gli incassi derivanti dalla pubblicità. L'INA sostiene che la convenuta diffonde i contenuti ben sapendo che gli stessi sono oggetto di privativa intellettuale, al mero fine di attirare pubblico.

Al contrario, la società YouTube deduce di intervenire semplicemente in qualità di fornitore di servizi di intermediazione per i video caricati dagli utenti della sua piattaforma. La stessa ricorda che la legge del 21 giugno 2004 definisce il servizio di *hosting* come quello in virtù del quale il fornitore assicura, a richiesta dei terzi, la memorizzazione del contenuto da loro fornito, in vista di una ulteriore diffusione al pubblico.

La società YouTube sostiene di non avere alcun controllo sui contenuti caricati, ma che responsabilizza chiaramente gli utenti. La stessa, inoltre, deduce che l'INA avrebbe dovuto immediatamente adottare delle soluzioni idonee nei confronti degli utenti che caricavano contenuti controversi. La società YouTube precisa che gli strumenti messi a disposizione degli utenti non comportano in alcun modo [l'esecuzione di] un'attività di tipo editoriale e che la circostanza che la stessa sia remunerata attraverso le inserzioni pubblicitarie non consente di negare l'applicazione dell'art. 6 LCEN.

Secondo l'art. 6-I-2 della legge sul commercio elettronico francese (LCEN), le persone fisiche o giuridiche che, anche a titolo gratuito, effettuano la memorizzazione di segnali, di scritti, di immagini, di suoni o di messaggi di altra natura forniti dai destinatari dei servizi mettendoli a disposizione del pubblico su Internet, non possono essere ritenute civilmente responsabili per fatti relativi alle attività o alle informazioni memorizzate a richiesta dei destinatari, salvo che non fossero effettivamente a conoscenza del carattere illecito di tali materiali o dei fatti o delle circostanze relative e che, non appena conosciute tali circostanze, si siano prontamente attivate per rimuovere tali dati o per impedirne l'accesso.

---

\* Traduzione della sentenza a cura di Virginia Raggi e Pieremilio Sammarco.

Tale regime di responsabilità limitato è integrato dall'art. 6-I-7 (LCEN) in virtù del quale i fornitori di accesso e di memorizzazione non sono tenuti ad un obbligo di verifica delle informazioni che trasmettono o memorizzano, né ad un obbligo generale di ricercare i fatti o le circostanze che rivelano l'esistenza di attività illecite.

Inoltre, dalle condizioni di utilizzo del servizio di YouTube risulta che tale servizio consente agli utenti di ricercare, visionare in sola lettura o caricare video e risulta, altresì, che ogni utente, preventivamente iscritto può, una volta creato il suo *account* YouTube, trasferire su tale sito i contenuti audiovisivi (sui quali la società convenuta non esercita alcun controllo) al fine di metterli a disposizione del pubblico ovvero di un gruppo ristretto di utenti.

All'interno di tali condizioni, emerge che YouTube si limita a fornire una tecnologia di memorizzazione e di visualizzazione dei video, permettendo il loro caricamento a semplice richiesta degli utenti del sito, distinguendosi, così, in modo radicale da un servizio di tipo editoriale atteso che sugli stessi non viene effettuata alcuna scelta dei contenuti offerti al pubblico, né alcun intervento.

Le attività di controllo della presentazione delle pagine sul sito, la limitazione alla durata dei video diffusi, l'organizzazione e la gestione di una base di dati attraverso parole chiave che consentono la ricerca rapida dei video o, ancora, la fornitura di mezzi tecnici per repertoriare i predetti video sono di natura tecnica e non risultano incompatibili con la qualifica di *hoster*.

Inoltre, la commercializzazione di spazi pubblicitari svolta dalla società YouTube, non ne consente l'esclusione dal beneficio delle disposizioni sopra richiamate atteso che la LCEN non contiene alcuna norma che impedisce all'*hoster* di trarre profitto dal suo sito, anche in considerazione del fatto che tale sfruttamento permette agli utenti di accedere gratuitamente alla predetta piattaforma.

Pertanto, la società YouTube non può essere considerata come editore ai sensi della predetta Legge e deve, conseguentemente, vedersi applicato il regime di responsabilità destinato ai fornitori di servizi di intermediazione e memorizzazione.

b) *Sulla responsabilità della società YouTube in qualità di hoster.*

L'INA sostiene che la responsabilità della società YouTube nei suoi confronti è assimilabile a quella di un *hoster* poiché la società ha ritardato a rimuovere dal sito i programmi dell'INA o non li ha rimossi che parzialmente e conseguentemente ha fatto sì che gli stessi fossero ivi reperiti.

L'INA ricorda che l'*hoster*, ai sensi della LCEN, ha l'obbligo di ritirare prontamente i video allorché abbia la conoscenza effettiva del loro carattere illecito o di fatti e circostanze che lasciano presupporre tale carattere.

La società ricorrente aggiunge, inoltre, che la società YouTube non può pretendere che la sua responsabilità sia accertata solo dopo che sia stata negata giudizialmente l'assenza di responsabilità degli utenti che hanno caricato i video, atteso che non vi è alcun obbligo di legge che impone al titolare di diritti di agire secondo tale schema e che per l'*hoster* è previsto un regime di responsabilità specifico dal quale non può sottrarsi.

L'INA deduce che la società YouTube ha reso disponibili su suo sito dei video il cui carattere illecito gli era stato notificato secondo i termini indicati dalla legge, atteso che risulta chiaramente dalla giurisprudenza che gli *hoster* di dati debbono adoperarsi affinché i programmi dei quali sia stato notificato il carattere illecito non siano più diffusi attraverso il loro sito.

A sua difesa, la società YouTube sostiene di aver prontamente rimosso integralmente i video che gli erano stati segnalati dall'INA.

La convenuta riferisce, inoltre, che l'INA, talvolta, ha proceduto mediante notificazioni non valide, omettendo di comunicare il necessario indirizzo URL del video del quale veniva richiesta la rimozione; diversamente, quando gli estratti venivano chiaramente identificati, la società YouTube li ritirava prontamente, circostanza, peraltro, non contestata.

La società YouTube deduce che la sua responsabilità non sussisterebbe in relazione al caricamento di contenuti identici o simili a quelli precedentemente segnalati e rimossi, atteso che tale obbligo non risulta previsto né dalla legge né dalla successiva evoluzione giurisprudenziale tanto che, ai sensi della LCEN il ri-caricamento dei files deve essere considerato come un fatto nuovo che necessita di una nuova notifica.

La convenuta espone che la notifica di un contenuto manifestamente illecito non comporta per l'*hoster* alcun obbligo di procedere al monitoraggio e al filtro relativamente a quel contenuto per il futuro, salvo che vi sia un provvedimento dell'autorità giudiziaria che deve essere, in ogni modo, temporaneo e specifico.

In particolare, riconoscendo la qualità di *hoster* della società YouTube, occorre ricordare che in relazione a quanto previsto nella LCEN, la stessa non può essere considerata responsabile dei contenuti diffusi sul suo sito dagli utenti i quali ne sono i soli responsabili.

Salvo che per ciò che attiene al materiale con contenuti pedopornografici, relativi all'apologia di reati contro l'umanità e all'incitazione all'odio razziale, espressamente disciplinati dalla legge ed in relazione ai quali l'*hoster* deve attivarsi direttamente, senza attendere un provvedimento dell'Autorità giudiziaria, la sua responsabilità non può essere affermata tranne nel caso in cui vi sia una conoscenza effettiva del carattere manifestamente illecito delle informazioni memorizzate.

Analogamente, anche nell'ipotesi di lesioni di diritti morali e patrimoniali derivanti dalla contraffazione, è onere dei soggetti lesi portare a conoscenza dell'*hoster* i diritti che si ritengono violati.

L'art. 5-6 della LCEN dispone, infatti, che la presunzione di conoscenza relativamente a circostanze controverse si ritiene acquisita dagli *hoster* allorché gli vengano notificati i seguenti elementi: la data della notificazione, le coordinate del notificante, le coordinate del destinatario, la descrizione e la localizzazione precisa dei fatti controversi, i motivi per i quali il contenuto deve essere rimosso anche in relazione alle disposizioni di legge ed ai motivi di fatto. Il testo dispone, inoltre, che il precedente comma non pregiudica l'attività di monitoraggio mirato e temporaneo richiesto dall'Autorità giudiziaria.

Orbene, dal momento in cui l'*hoster* è a conoscenza del carattere illecito delle informazioni memorizzate, l'art. 6-2 della LCEN lo obbliga ad agire prontamente per rimuovere tali dati o disabilitarne l'accesso.

L'INA riconosce che 50 video contraffatti rilevati in data 31 marzo 2006, dei quali la società YouTube è stata informata il 19 aprile 2009, sono stati apparentemente rimossi lo stesso giorno. Aggiunge, inoltre, che 500 video rilevati in data 5 dicembre 2008, dei quali la società YouTube è stata informata in data 12 gennaio 2009, sono stati apparentemente rimossi il giorno successivo.

Al contrario, l'INA sostiene che 179 video contraffatti rilevati tra il 6 ed il 10 marzo 2008, dei quali la società YouTube è stata informata il 25 marzo 2008, sono stati rimossi solo quindici giorni dopo; analogamente,

per 547 video contraffatti rilevati tra il 28 ed il 30 luglio 2008, dei quali la società YouTube è stata informata il 28 agosto 2008, la rimozione è stata effettuata solo un mese dopo.

Ad ogni modo, il ritardo di quindici giorni e di un mese, che deve essere migliorato, non è sufficiente a far ritenere la responsabilità dell'*hoster*.

Al contrario, non risulta contestata la circostanza che 96 video ritenuti contraffatti come da atto depositato il 23 novembre 2006, sono stati rimossi dalla società YouTube solo in data 27 novembre 2007, ossia un anno più tardi, sul presupposto che vi erano trattative tra le parti: motivo che, tuttavia, non consente di giustificare che i video contraffatti fossero mantenuti sul sito della convenuta.

Inoltre, non vi è alcuna disposizione della legge 24 giugno 2004 che obblighi i titolari dei diritti ad agire preliminarmente nei confronti degli utenti che hanno caricato i video, atteso che l'*hoster* ha un regime di responsabilità specifico.

Infine, non risulta contestato il fatto che la società YouTube ha lasciato disponibili sul suo sito alcuni video il cui carattere illecito gli era già stato notificato, allorché era suo dovere intraprendere tutte le misure necessarie per evitare una nuova diffusione.

Infatti, il tema secondo il quale ogni ri-caricamento costituisce un fatto nuovo necessitando di una nuova notificazione deve essere rigettato nella misura in cui, benché le diffusioni successive siano imputabili ad utenti diversi dai primi, il loro contenuto ed i relativi diritti di proprietà intellettuale, sono identici.

La società YouTube pertanto, non può richiamare l'esistenza di una generica impossibilità tecnica per esercitare tale attività di sorveglianza, atteso che vi è la capacità di adottare i mezzi e le misure necessarie a rimuovere i contenuti di tipo pedofilo, relativi all'apologia di reato contro l'umanità o all'incitamento all'odio razziale.

Atteso che è dovere della stessa provare di aver adottato ogni cautela necessaria in vista dell'immediato ritiro di tutti i testi integrali segnalati come contraffatti e renderne impossibile il ri-caricamento, la società YouTube non può avvalersi della limitazione di responsabilità garantita dall'art. 6-1-2 della legge 24 giugno 2004 e la sua responsabilità è, dunque, rinvenibile nei confronti dell'INA ai sensi delle norme ordinarie sulla contraffazione, contenute agli artt. L 335-3 e L 335-4 del Codice della Proprietà intellettuale.

Diversamente, non è dimostrata in alcun modo l'esistenza di una responsabilità civile ulteriore e distinta rispetto a quella sopra indicata di talché la società YouTube non è responsabile ai sensi dell'art. 1382 del Codice Civile.

c) *Sull'installazione di un sistema di filtro efficace e immediato sul sito della società YouTube.*

L'INA chiede che sia ordinato alla società YouTube di installare sul suo sito un sistema di filtro efficace ed immediato per i video la cui diffusione è stata o sarà indicata dall'INA. La ricorrente precisa che la società YouTube dispone di una tecnologia che gli permette di impedire che un contenuto illecito non riappaia, ma non utilizza tale sistema che per proteggere i contenuti dei titolari di diritti che hanno concluso con la stessa un accordo di licenza e divisione dei ricavi.

A sua difesa, la società convenuta chiede il rigetto della domanda e precisa che l'INA ha sempre rifiutato di utilizzare dei mezzi di identificazione e prevenzione dei ri-caricamenti dei contenuti che la stessa ha

suggerito più volte alla società attrice (in particolare, si tratta di una tecnologia basata sul riconoscimento dei contenuti a partire dalla parte denominata « *content ID* »). La società convenuta afferma come sia di primaria importanza che la stessa ottenga l'autorizzazione espressa dei titolari dei diritti prima di adottare strumenti di tracciamento dei contenuti.

La società YouTube deduce che l'INA avrebbe preferito tentare di impiegare la propria tecnologia.

La società convenuta sostiene, infine, che ove il Tribunale disponga di adottare la misura di filtro richiesta, la stessa dovrebbe comunque soprassedere in attesa della decisione della Corte di Giustizia dell'Unione Europea, investita dal Tribunale di primo grado di Bruxelles in merito ad una questione pregiudiziale al fine di sapere se il giudice abbia solo il potere di imporre ad un fornitore di internet la cessazione degli atti che siano stati oggetto di condanna ovvero se, in modo più esteso ed eventualmente in che misura, potrebbe ingiungere a tale fornitore di prevenire ogni nuova ed ulteriore attività.

In particolare, la società YouTube spiega che la questione pregiudiziale è stata posta alla Corte di Giustizia dell'Unione Europea il 28 giugno 2010, affinché venga stabilito se un giudice nazionale, adito all'interno di un procedimento, possa ordinare ad un fornitore di servizi di adottare, nei confronti di tutti i suoi utenti, in astratto ed a titolo preventivo, a proprie spese e senza limiti temporali, un sistema di filtro della maggior parte delle informazioni memorizzate sui suoi server, allo scopo di identificare i *files* che contengono opere sulle quali terzi pretendano avere diritti, al fine di bloccare successivamente tali *files*.

Occorre, alla fine, constatare che la questione pregiudiziale conduce ad una domanda generale relativa all'adozione di un sistema di filtro in astratto e a titolo preventivo, mentre la domanda formulata dall'INA è precisa e concerne le opere già segnalate dalla stessa alla società YouTube.

La domanda di sospendere il giudizio sarà, quindi, rigettata.

Conseguentemente, viene ordinato alla società YouTube di installare sul proprio sito un sistema di filtro efficace ed immediato per i video la cui diffusione è stata o sarà contestata dall'INA.

d) *Sul risarcimento dei danni.*

[*omissis*]

3) SULLE DOMANDE RICONVENZIONALI DELLA SOCIETÀ YOUTUBE.

[*omissis*]

4) SULLE ALTRE DOMANDE.

[*omissis*]

**P.Q.M. — Il Tribunale, in pubblica udienza ed esperito il contraddittorio, in prima istanza,**

Ritiene ricevibile il ricorso dell'INA.

Ritiene applicabile alla società YouTube il regime di responsabilità previsto per gli *hoster* dalla legge 21 giugno 2004 per la fiducia nell'economia digitale (LCEN).

Ritiene che la diffusione ed il mantenimento, ad opera della società YouTube, di estratti di programmi audiovisivi appartenenti al catalogo

dell'INA, senza la sua autorizzazione, dopo che la loro illiceità era stata segnalata e atteso che, ciò nonostante, non ne è stato impedito il ri-caricamento, costituisce contraffazione ai sensi degli artt. L 122-4 e L 215-1 del Codice della Proprietà Intellettuale.

Conseguentemente, ordina alla società YouTube di installare sul suo sito un sistema di filtro efficace ed immediato per i video la cui diffusione è stata o sarà contestata dall'INA.

[omissis]

---

**LA POSIZIONE  
DELL'INTERMEDIARIO  
TRA LA ESTRANEITÀ AI  
CONTENUTI TRASMESSI E  
L'EFFETTIVA CONOSCENZA  
DELL'ILLECITO:  
UN'ANALISI COMPARATA  
TRA SPAGNA, FRANCIA  
E REGOLAMENTAZIONE  
COMUNITARIA**

---

**1. I CASI GIUDIZIARI.**

**I**l ruolo di *YouTube* e la questione inerente alla violazione del diritto di autore sui contenuti audiovisivi pubblicati dagli utenti investe, come accaduto in molti paesi europei, anche la giurisprudenza spagnola e francese. La vicenda giudiziaria è sempre la stessa: il titolare esclusivo dei diritti di sfruttamento di un'opera audiovisiva lamenta la violazione dei propri diritti attraverso la piattaforma informatica allestita da *YouTube* ed il giudice è chiamato a valutare tale condotta alla luce della direttiva comunitaria sul commercio elettronico e della legge interna di recepimento.

L'interpretazione resa dal Tribunale spagnolo si fonda su queste argomentazioni:

1) per l'attività espletata e le modalità del servizio reso, il ruolo di *YouTube* non può essere qualificato come fornitore di contenuti, ma di mero intermediario;

2) la messa disposizione in favore degli utenti di alcuni video ordinati attraverso una serie di parametri oggettivi e criteri definiti preliminarmente dagli stessi utenti, non comporta alcun lavoro editoriale di creazione o fornitura di contenuti da parte del soggetto intermediario;

3) in virtù di tale posizione, non è possibile imporre al prestatore di servizi di intermediazione un obbligo generale di supervisionare preventivamente i dati e le informazioni che sono immagazzinati sui propri *server* e successivamente trasmessi in rete, né, ancora meno, di attivarsi per ricercare fatti o circostanze relative ad attività illecite, atteso che il suo unico obbligo è precisamente quello di collaborare con i titolari dei diritti affinché, dopo aver riconosciuto l'infrazione, si proceda alla rimozione di tali contenuti.

Attraverso questo percorso logico, il Tribunale spagnolo giunge ad escludere la responsabilità dell'intermediario per la veicolazione e la messa a disposizione di contenuti video in violazione della legge sul diritto d'autore, perché privi delle necessarie autorizzazioni rilasciate da-



gli aventi diritto. La soluzione offerta, a parere del giudice iberico, si ispira ai principi della direttiva europea 2000/31/CE, che stabilisce l'inesistenza di un preventivo obbligo di controllo di carattere generale per i soggetti che prestano servizi di intermediazione nella società dell'informazione<sup>1</sup>.

Diversamente, il Tribunale francese, chiamato a valutare la liceità dell'attività dell'intermediario *YouTube* nella messa a disposizione degli utenti della rete di frammenti di programmi televisivi andati in onda sui canali pubblici della tv francese, i cui diritti esclusivi di utilizzazione competono all'*Institut National de l'Audiovisuel (INA)*, ha affermato che la ricezione di una comunicazione di notifica da parte del soggetto leso, corredata delle informazioni necessarie, fa sorgere in capo all'intermediario l'obbligo di attivarsi per la rimozione delle opere protette, pena l'attribuzione di responsabilità.

Si tratta di una decisione, su fattispecie pressoché identica, che si contrappone a quella resa dal Tribunale spagnolo, in virtù di una diversa interpretazione della direttiva comunitaria e della non omogeneità delle normative interne di recepimento.

La corte francese fonda la propria decisione sul fatto che l'intermediario non può, a propria giustificazione, far valere una obiettiva impossibilità tecnica di esercitare un'attività di sorveglianza o controllo sui contenuti immessi nella rete Internet dai propri utenti, né che non dispone dei mezzi adeguati per eliminare le opere che violano il diritto d'autore, dal momento che interviene sui contenuti ospitati, disabilitando o cancellando quelli a carattere pedofilo, o che incitano all'odio, o che sono un'apologia del crimine.

Inoltre, il Tribunale francese, applicando in modo assai rigoroso il principio di presunzione di conoscenza, ha stabilito che l'intermediario va ritenuto responsabile anche per ogni successiva nuova pubblicazione dei contenuti informativi lesivi, anche se essa avviene per opera di utenti diversi da quelli precedentemente coinvolti<sup>2</sup>. E precisa il giudice francese che, in questo caso, non si è in presenza di un fatto nuovo tale da richiedere una ulteriore notifica, perché i diritti di proprietà intellettuale sono i medesimi.

Nel condannare *YouTube*, per la consumata contraffazione, al pagamento dell'importo di € 150.000,00 il giudice francese, ed è questo a nostro avviso l'elemento di maggiore novità, accogliendo la specifica domanda avanzata dall'*INA*, ordina all'intermediario di installare sui propri server un sistema di filtraggio dei video che sia efficace e che immediatamente impedisca la pubblicazione di opere protette prive delle necessarie autorizzazioni rilasciate dagli aventi diritto e dispone che la stessa parte lesa abbia la possibilità di constatare la funzionalità del dispositivo tecnico anzidetto.

<sup>1</sup> Principio, come è noto, sancito nel 47° considerando e nell'art. 15 della direttiva 2000/31/CE.

<sup>2</sup> Nella vicenda sottoposta al Tribunale francese, il numero dei contenuti informativi oggetto della controversia era consi-

derevole: 50 video rilevati in data 31 marzo 2006, 179 video rilevati tra il 6 e il 10 marzo 2008, 500 video rilevati il 5 dicembre 2008, 547 video rilevati tra il 28 e il 30 luglio 2008 e 96 video indicati nel ricorso depositato il 23 novembre 2006.

## 2. LA NORMATIVA SPAGNOLA.

Come è noto, la direttiva europea 2000/31/CE non sanziona l'intermediario dei servizi della società dell'informazione a condizione che questi non sia effettivamente a conoscenza dell'attività illecita posta in essere e non si adoperi per porre rimedio, rimuovendo le informazioni illecite o disabilitandone l'accesso. Secondo la linea di indirizzo scelta dal Tribunale spagnolo, in armonia con quanto disposto dalla direttiva, non sussistono obblighi preventivi di sorta per il *provider*, ma solo obblighi che possono essergli imposti successivamente e solamente una volta che l'intermediario abbia avuto conoscenza dell'illecito.

La stessa direttiva europea 2000/31/CE che stabilisce il principio dell'assenza di un preciso obbligo di sorveglianza a carico dell'intermediario non offre indicazioni all'interprete per accertare quali siano gli elementi discriminanti per ritenere quando e al verificarsi di quali condizioni sia possibile presumere la conoscenza dell'illecito, così da imporre l'obbligo di pronta attivazione.

Si tratta di un vuoto normativo contenuto nella direttiva che ha rimesso alle decisioni dei singoli Stati membri come contemplare la questione della conoscenza effettiva dell'illecito da parte dell'intermediario.

Il legislatore spagnolo, con la legge di recepimento della direttiva comunitaria (*Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*), all'art. 16 ha statuito che sussiste la effettiva conoscenza (*conocimiento efectivo*) quando un organismo competente ha preventivamente dichiarato la natura illegittima di tali dati, o ne ha ordinato la disabilitazione all'accesso o la loro rimozione e l'intermediario ne era al corrente, fatte comunque salve le procedure di rilevamento del carattere illecito approntate dagli stessi fornitori di contenuti e quelle frutto di accordi in autoregolamentazione e gli altri mezzi di efficace conoscenza che potranno in futuro essere individuati<sup>3</sup>.

Dunque, la legge spagnola sembra preferire un'interpretazione restrittiva dell'effettiva conoscenza dell'illiceità, esigendo che questa sia dichiarata preventivamente da un organo competente. E per « *organo competente* » si devono intendere tutte le autorità giudiziarie o amministrative che agiscono nell'esercizio delle loro competenze istituzionali. Tuttavia, dal momento che non esiste in Spagna alcun organo amministrativo con competenze specifiche in questa materia, l'unico organo competente per determinare la liceità o meno dell'informazione è l'autorità giudiziaria.

Nello stesso tracciato, il legislatore italiano, nel recepire la direttiva europea, ha cercato di colmare la suddescritta lacuna normativa scegliendo

<sup>3</sup> Testualmente, l'art. 16 della Ley 34/2002, al suo secondo comma stabilisce che « *se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hu-*

*biera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse* ».

di presumere la conoscenza effettiva (che fa scattare l'obbligo di attivazione) dell'intermediario alla ricezione di una specifica comunicazione o di una richiesta proveniente da parte delle autorità competenti.

Nell'importazione in sede di regolamentazione europea del modello statunitense relativo alla responsabilità dell'intermediario, il legislatore comunitario ha preferito affermare con vigore il principio dell'assenza dell'obbligo generale di sorveglianza, tralasciando la trattazione sulla rilevante questione dell'effettiva conoscenza. Si tratta di una scelta di politica del diritto che ha determinato le incertezze interpretative sul punto, aprendo la strada alle diverse soluzioni giurisprudenziali che, come nel caso in esame, si vanno contrapponendo all'interno degli stati membri<sup>4</sup>.

Anche il legislatore d'oltreoceano, nel *Digital Millennium Act* del 1998 (o *rectius*, della sua parte *Online Copyright Infringement Liability Act*), in linea con il *Communications Decency Act* che stabilisce l'inapplicabilità della responsabilità editoriale, ha escluso forme di responsabilità oggettiva, imputando la colpa al *provider* nei casi di *contributory infringement*; viene, tuttavia, attribuita all'intermediario la responsabilità quando questi non si attivi in caso di palese illiceità, o quando riceva specifica comunicazione (*notification*) redatta per iscritto dal soggetto titolare del diritto che si assume essere stato leso, purché sia idonea ad identificare con sufficiente certezza la fonte della violazione e si dimostri l'esistenza in buona fede del diritto<sup>5</sup>.

Pertanto, nel sistema statunitense, a differenza di quanto previsto nel quadro di riferimento comunitario, non è necessario, ai fini dell'esistenza dell'obbligo della pronta attivazione dell'intermediario, uno specifico ordine o una precisa richiesta da parte delle autorità competenti, essendo

<sup>4</sup> Lo stesso caso (cfr. *RTI S.p.A. v. YouTube LLC, Google Inc., Google UK Ltd*) è stato affrontato dal giudice italiano (Trib. Roma, ord. 11 febbraio 2010, in questa *Rivista*, 2010, 275), per il quale è ammissibile l'emissione di un provvedimento cautelare con cui si ordini la rimozione dei frammenti audiovisivi di un'opera protetta abusivamente diffusi via Internet nel caso in cui l'intermediario, nonostante la ricezione di ripetute diffide da parte del titolare dei diritti di utilizzazione e sfruttamento dell'opera, non si sia immediatamente attivato per rimuovere il materiale segnalatogli come illecito. Infatti, secondo il giudice italiano, la disciplina interna di recepimento della direttiva comunitaria, pur non richiedendo all'*host provider* di svolgere un'attività preventiva di controllo e di accertamento sull'eventuale carattere illecito delle informazioni caricate dagli utenti, pone a suo carico l'obbligo di rimuoverle immediatamente non appena avuto conoscenza di tale illiceità, anche se comunicazione ricevuta dal titolare dei diritti, non essendo necessario a tal fine un apposito ordine dell'autorità giudiziaria.

Peraltro, il giudice italiano, con il suo orientamento, non si è distanziato dall'interpretazione della nozione di effettiva conoscenza resa dalla sentenza della Corte di Giustizia del 23 marzo 2010 (caso *Google France Sarl*), in questa *Rivista*, 2010, 707, laddove al punto n. 109, si precisa che « la limitazione della responsabilità di cui all'art. 14 si applica in caso di prestazione di un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio e significa che il prestatore di un tale servizio non può essere ritenuto responsabile per i dati che ha memorizzato su richiesta di un destinatario del servizio in parola, salvo che tale prestatore, dopo aver preso conoscenza, mediante un'informazione fornita dalla persona lesa o in altro modo, della natura illecita di tali dati o di attività di detto destinatario, abbia omissis di prontamente rimuovere tali dati o disabilitare l'accesso agli stessi ».

<sup>5</sup> Cfr. *US Digital Millennium Copyright Act (DMCA)* H.R. 2281, Sec. 202, § 512.

sufficiente la notificazione a cura del soggetto interessato dell'illecito perpetrato ai suoi danni<sup>6</sup>. Tutto ciò perché, a differenza del modello comunitario, si prevede con maggiore determinatezza la nozione di conoscenza effettiva (*actual knowledge*) dell'illecito, sulla quale ruota il principio della responsabilità dell'intermediario<sup>7</sup>.

### 3. LA NORMATIVA FRANCESE.

A conclusioni difformi dall'interpretazione resa dal Tribunale di Madrid, giunge il giudice francese del *Tribunal de Grande Instance de Creteil* con la sentenza del 14 dicembre 2010 relativa all'iniziativa giudiziaria promossa dall'*Institut National de l'Audiovisuel (INA)* contro YouTube per la pubblicazione sulla piattaforma di quest'ultima di frammenti di opere audiovisive coperte dal diritto d'autore.

Il Tribunale d'oltralpe, nel ribadire che l'attività in questione non può essere assimilata a quella esercitata da un editore, ma è propria dei soggetti che offrono servizi della società dell'informazione, stabilisce che all'intermediario deve applicarsi il regime di responsabilità stabilito dalla *loi du 21 juin 2004 n. 575 pour la confiance dans l'économie numérique (LCEN)* che recepisce la direttiva europea 2000/31/CE e che la diffusione di frammenti di opere protette senza l'autorizzazione del titolare dei diritti, dopo che l'attività illecita era stata debitamente segnalata, costituisce contraffazione ai sensi degli artt. L 122-4 e L-215-1 del *Code de la propriété intellectuelle*.

La decisione resa dal Tribunale francese si fonda sull'interpretazione dell'art. 6-2 *LCEN*, che impone all'intermediario l'obbligo di attivazione diretto alla rimozione dell'illecito dal momento della sua conoscenza<sup>8</sup> e la presunzione di effettiva conoscenza (*effectivement connaissance*), secondo quanto disposto dall'art. 6-5 *LCEN*, si ha una volta ricevuta una notifica contenente tutti i dati necessari ad identificare i soggetti coinvolti e le ragioni atte a dimostrare l'illecito perpetrato.

Nello specifico, secondo la legislazione francese, la conoscenza dei fatti illeciti si presume per l'intermediario quando la notifica inviata a quest'ultimo è corredata dei seguenti elementi: la data, le generalità complete della persona fisica o giuridica notificante e l'indicazione del legale rap-

<sup>6</sup> Sul sistema della *notification* negli Stati Uniti, su tutti, si veda G.M. RICCIO, *La responsabilità civile degli internet providers*, Torino, 2002, 178 e ss.. Peraltro, il sistema « *notice and takedown* » statunitense è stato adottato anche in Australia, Cina, Nuova Zelanda, Singapore e Corea del Sud.

<sup>7</sup> La legislazione statunitense, oltre al principio della conoscenza effettiva (*actual knowledge*), prevede l'attribuzione della responsabilità all'intermediario nei casi in cui l'attività illecita è immediatamente riconoscibile [*DMCA*, § 512 (c) (1) (A) (ii), « *facts or circumstances from which infringing activity is apparent* »].

<sup>8</sup> Testualmente, l'art. 6-2 *LCEN*: « *les personnes physiques ou morales qui assu-*

*rent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible* ».

presentante, se trattasi di ente; il nome ed il domicilio o sede legale del destinatario della notifica; una descrizione dei fatti contestati e la loro precisa localizzazione nella rete; le ragioni di diritto in base alle quali il contenuto informativo deve essere rimosso; la copia della corrispondenza inviata che documenti la questione controversa e che contenga la domanda di rimozione o di modificazione del contenuto informativo pubblicato, o i motivi per i quali non è stato possibile inviare la corrispondenza (art. 6-5 *LCEN*)<sup>9</sup>.

Come accennato, la corte francese ha imposto all'intermediario di dotarsi di un sistema o dispositivo tecnico di filtraggio che impedisca la pubblicazione *on-line* dei contenuti protetti, attribuendo alla parte lesa dalla contraffazione subita, la facoltà di controllo in ordine alla efficacia di tale mezzo. Si tratta, senza dubbio, di un elemento di novità nel panorama delle decisioni sinora emesse, dal momento che, qualora tale dispositivo effettivamente funzionasse, determinerebbe in capo all'intermediario, un potere di controllo preventivo su ogni contenuto informativo veicolato<sup>10</sup>.

Questo tipo di misura era in qualche modo prevista dalla c.d legge Hadopi (*loi favorisant la diffusion e la protection de la création sur Internet*) che ha stabilito la creazione di un'autorità amministrativa indipendente (*Haute Autorité pour la Diffusion des œuvres et la Protection des Droits sur Internet*)<sup>11</sup> che poteva ordinare a carico dell'intermediario l'installazione di dispositivi *software* in grado di monitorare i flussi informativi in entrata ed in uscita, così da scongiurare il pericolo di violazioni della legge sul diritto d'autore<sup>12</sup>. Come è noto, il *Conseil Constitutionnel*, con la de-

<sup>9</sup> L'art. 6-5 *LCEN*, testualmente, recita: « *la connaissance des faits litigieux est présumée acquise par les personnes désignées au 2 lorsqu'il leur est notifié les éléments suivants: — la date de la notification; — si le notifiant est une personne physique: ses nom, prénoms, profession, domicile, nationalité, date et lieu de naissance; si le requérant est une personne morale: sa forme, sa dénomination, son siège social et l'organe qui la représente légalement; — les nom et domicile du destinataire ou, s'il s'agit d'une personne morale, sa dénomination et son siège social; — la description des faits litigieux, ou la localisation précise; — les motifs pour lesquels le contenu doit être retiré, comprenant la mention des dispositions légales et des justifications de faits; — la copie de la correspondance adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification de ce que l'auteur ou l'éditeur n'a pu être contacté* ».

<sup>10</sup> In un'altra pronuncia della giurisprudenza francese, (*Tribunal de grande instance de Paris, Ordonnance de référé* del 5 marzo 2009, *Magdane et autres v. Youtube*), all'intermediario veniva impo-

sto un dispositivo tecnico di blocco (*mesure de blocage*) della diffusione di opere audiovisive contenute in due Dvd. In dottrina, sul rapporto tra i dispositivi tecnici che impediscono la pubblicazione di contenuti informativi e le libertà fondamentali dell'individuo, cfr. il documento dell'11 maggio 2010, redatto sotto l'egida dell'*Open Society*, da C. CALLANAN-M. GERCKE-E. DE MARCO-H. DRIES-ZIEKENHEINER, *Filterage d'Internet: Equilibrer les réponses à la cybercriminalité dans une société démocratique*, disponibile *on-line*. Per l'Italia, G. FINOCCHIARO, *Filtering e responsabilità del provider*, in *AIDA*, 2010, 340. In generale, sul dibattito inerente all'accesso alla rete ed alla conoscenza intesa come libertà fondamentale dell'individuo, A. KAPZCYNski, *The access to knowledge mobilization and the new politics of intellectual property*, 117 *Yale L.J.*, 304 (2008).

<sup>11</sup> Questa autorità sostituisce l'*Autorité de régulation des mesures techniques (ARMT)* introdotta dalla legge n. 2006-961 del 1° agosto 2006 relativa *au droit d'auteur et aux droits voisins dans la société de l'information* (conosciuta come *loi « Dadvs »*).

<sup>12</sup> Va osservato che l'introduzione di dispositivi tecnici di prevenzione a carico

cisione del 10 giugno 2009, ha censurato l'imposizione di tali programmi, riservando all'autorità soltanto la facoltà di consigliarne l'uso, ma non anche di imporlo<sup>13</sup>.

Peraltro, al di là della valutazione sulla costituzionalità della norma, una siffatta attribuzione di poteri in capo all'intermediario, sembrerebbe in contrasto con il principio declamato nella direttiva comunitaria in base al quale non sussiste in capo al fornitore di servizi della società dell'informazione un obbligo generale di sorveglianza, o di ricercare fatti o circostanze delle attività illecite.

Per completezza sul tema, però, ad onor del vero, va anche osservato che nel 40° considerando della direttiva 2000/31/CE, si rinviene l'invito del legislatore comunitario agli stati membri a sviluppare sistemi tecnici, concordati tra tutte le parti interessate, che siano efficaci nel rimuovere le attività illecite nell'ambito dei servizi della società dell'informazione, ma, ad oggi, fatta eccezione per quanto verificatosi in Francia, questa esortazione non ha sortito effetto<sup>14</sup>.

Forse, le ragioni di questo mancato accoglimento dell'invito, sono da ricercarsi nella trasformazione della rete Internet (e dei servizi ad essa collegati) che si è verificata negli ultimi anni, che vede ora un numero esiguo di soggetti dominare l'erogazione dei servizi, contrapposto ad un nu-

degli intermediari non è un fatto nuovo nel panorama normativo, dal momento che, nella legislazione del Giappone sui *services provider* (legge n. 137 del 2001, art. 3), è stabilito che questi ultimi non sono responsabili per le attività contraffattorie qualora abbiano impiegato misure tecniche atte a prevenire gli illeciti.

<sup>13</sup> Sulla questione della legittimità costituzionale della legge Hadopi, cfr. L. COSTES, *La loi « Creation et Internet » partiellement censurée par le Conseil constitutionnel*, in 50 *Rev. Lamy Dr. Immatériel*, 3 (2009); A. GAUTRON, *La réponse graduée (à nouveau) épinglée par le Conseil constitutionnel. Ou la délicate adéquation des moyens aux fins*, in 51, *Rev. Lamy Dr. Immatériel*, 63 (2009); D. ROUSSEAU, *Hado-pirate la Constitution: le Conseil sanctionne*, in 51, *Rev. Lamy Dr. Immatériel*, 103 (2009); I. BOUBEKERUR, *De la loi Hadopi à la loi Hadopi 2. Analyse de la décision du Conseil Constitutionnel 2009-580 DC et de ses conséquences*, in 51 *Rev. Lamy Dr. Immatériel*, 107 (2009); N. LUCCHI, *Access to network services and protection of constitutional rights: recognizing the essential role of Internet access for the freedom of expression*, in 19 *Cardozo J. Int'l & Comp. Law*, (2011); nel panorama della dottrina italiana, G. VOTANO, *Internet fra diritto d'autore e libertà di comunicazione: il modello francese*, in questa *Rivista*, 2009, 538; P. PASSAGLIA, *L'accesso ad Internet è un diritto (il conseil constitutionnel france-*

*se dichiara l'incostituzionalità di parte della c.d. « legge anti file sharing »*, in *Fo-ro it.*, 2009, IV, 474.

<sup>14</sup> Si legge, testualmente, nel 40° considerando della direttiva 2000/31/CE che « *le attuali o emergenti divergenze tra le normative e le giurisprudenze nazionali, nel campo della responsabilità dei prestatori di servizi che agiscono come intermediari, impediscono il buon funzionamento del mercato interno, soprattutto ostacolando lo sviluppo dei servizi transnazionali e introducendo distorsioni delle concorrenze. In taluni casi, i prestatori di servizi hanno il dovere di agire per evitare o per porre fine alle attività illegali. La presente direttiva dovrebbe costituire la base adeguata per elaborare sistemi rapidi e affidabili idonei a rimuovere le informazioni illecite e disabilitare l'accesso alle medesime. Tali sistemi potrebbero essere concordati tra tutte le parti interessate e andrebbero incoraggiati dagli Stati membri. È nell'interesse di tutte le parti attive nella prestazione di servizi della società dell'informazione istituire e applicare tali sistemi. Le disposizioni della presente direttiva sulla responsabilità non dovrebbero impedire ai vari interessati di sviluppare e usare effettivamente sistemi tecnici di protezione e di identificazione, nonché strumenti tecnici di sorveglianza resi possibili dalla tecnologia digitale, entro i limiti fissati dalle direttive 97/46/CE e 97/66/CE* ».

mero elevatissimo e sempre più crescente relativo alla pubblicazione di contenuti informativi che provengono dagli stessi utenti<sup>15</sup>.

Ma, comunque, al di là delle concrete ragioni connesse alla mancata adozione da parte degli stati membri dei dispositivi tecnici di filtraggio, in questo vuoto di regolamentazione sul punto e nonostante il pronunciamento del *Conseil Constitutionnel*, il giudice francese, con il suo intervento, ha colmato tale lacuna, dando di nuovo corpo a quella parte della legge Hadopi che contempla, come ausilio alla lotta contro le violazioni del diritto d'autore, l'impiego di mezzi coercitivi di tipo tecnico<sup>16</sup>.

E, in questa direzione, oltre a domandarsi se l'intervento giurisprudenziale possa in qualche modo sacrificare o quanto meno intaccare il principio della neutralità della rete, imponendo una intromissione nei contenuti informativi veicolati<sup>17</sup>, occorre ancora di più chiedersi se tali iniziative giurisprudenziali o di carattere regolamentare si pongano in contrasto con i valori costituzionali — anche europei — della persona, quali la segretezza delle comunicazioni e le libertà fondamentali dell'individuo.

PIEREMILIO SAMMARCO

---

**BREVI NOTE**  
**SULL'ATTIVITÀ DI**  
**FILTRAGGIO DEI**  
**CONTENUTI INFORMATIVI**  
**VEICOLATI IN RETE**

con il preciso scopo di filtrare, inibire o bloccare determinati contenuti informatici, sia aventi carattere tecnicamente insidioso (c.d. *malware*, ossia *software* che tendono a danneggiare i computer nei quali si installano), o

**L**a sentenza resa dal Tribunale di Creteil offre l'occasione per svolgere alcune osservazioni in merito ai servizi di filtraggio dei contenuti informativi veicolati per il tramite di Internet, attività comunemente denominata *filtering*.

Tale espressione è utilizzata per indicare una serie di pratiche, dispositivi informatici, *software* o altri mezzi, predisposti ed organizzati

---

<sup>15</sup> L'*Organization for Economic Co-operation and Development (OECD)* ha coniato la definizione di «*user-created content*» per i contenuti informativi che presentano tre caratteristiche: (i) sono messi a disposizione del pubblico, (ii) sono dotati di un minimo di creatività e (iii) sono stati creati al di fuori di attività professionali, cfr. documento *OECD, Participative web and user-created content* (2007).

<sup>16</sup> Seguendo il tracciato segnato dalla c.d. legge Hadopi, va segnalato che la Francia, successivamente alla pubblicazione della sentenza del *Tribunal de Grande Instance de Creteil* in commento, ha ema-

nato un provvedimento normativo (*Décret n° 2010-1630 du 23 décembre 2010 relatif à la procédure d'évaluation et de labellisation des moyens de sécurisation destinés à prévenir l'utilisation illicite de l'accès à un service de communication au public en ligne*) che, modificando il *code de la propriété intellectuelle*, contempla l'impiego di mezzi e strumenti tecnici di filtraggio e controllo dei contenuti informativi da pubblicare *on-line*.

<sup>17</sup> J. DE BEER-C.D. CLEMMER, *Global trends in online copyright enforcement: a non neutral role for network intermediaries?*, in 49 *Jurimetrics J.* 375 (2009).

semplicemente che abbiano particolari caratteristiche antiggiuridiche (illeciti, pornografici, violenti, ecc.)<sup>1</sup>.

In via generale, si può affermare che i sistemi di filtraggio possono essere installati sia dai singoli utenti sui loro personali dispositivi, o dai *provider*, od anche da enti o persone giuridiche per regolare le modalità di accesso alla loro rete interna (intranet). Nel primo caso, ciascun utente può decidere quali contenuti escludere (non consentendone il caricamento sul proprio computer, la visualizzazione dal motore di ricerca, ovvero la ricezione sulla posta elettronica, ecc.) secondo le proprie prescrizioni; diversamente, nel secondo caso, sono il *provider* o i singoli utenti a decidere quali contenuti debbano essere inibiti e ciò, naturalmente, ha effetto per tutti gli utenti che utilizzano i servizi offerti da quel *provider*, o accedono a quella particolare rete chiusa. Tra l'altro, mentre il controllo effettuato all'interno di una rete chiusa implica la scelta decisionale in ordine a quali contenuti rendere indisponibili in relazione ad una determinata direttiva o ad un preciso orientamento, il filtro attivato dal *provider* (inteso specificamente come fornitore d'accesso alla rete) non rispecchia necessariamente una scelta politica né, tanto meno, può essere considerato rappresentativo delle scelte dei propri utenti<sup>2</sup>.

Tecnicamente, i sistemi di filtraggio vengono impostati per riconoscere la presenza di determinati elementi all'interno dei *files* che transitano nella rete ed attivare, conseguentemente, il blocco o l'inibizione del relativo contenuto informativo. Tali elementi possono essere rappresentati dalle parole chiave attinenti ad una determinata area semantica i cui contenuti sono ritenuti sgraditi (si pensi ai vocaboli attinenti al sesso, o alla razza, ecc.), ovvero dalla c.d. «impronta elettronica» del contenuto, come risultante dalla funzione di *hash*. In particolare, tale funzione è costituita da una sequenza alfanumerica che, secondo un preciso algoritmo, viene determinata univocamente a partire da una stringa di *bit* (siano essi contenuti in un *file* di testo, un'immagine, un video o, anche, un intero *hard disk*). In tal modo, se il sistema viene impostato per riconoscere e bloccare alcune funzioni, ne impedirà automaticamente l'accesso qualunque sia la forma o il formato sotto i quali esse si presentano, ovvero la denominazione attribuita al *file*<sup>3</sup>.

<sup>1</sup> Per un approfondimento, si veda anche il Rapporto redatto da C. CALLANAN, M. GERCKE, E. DE MARCO e H. DRIES-ZIEKENHEINER, *Filtrage d'Internet - Equilibrer les réponses à la cybercriminalité dans une société démocratique*, commissionato dall'*Open Society* e disponibile on-line: <http://www.juriscom.net/documents/lib20100520.pdf>.

<sup>2</sup> In tale caso, infatti, l'*access provider* non può certamente essere portatore delle istanze dei propri utenti e, così, si potrebbe affermare che i sistemi di filtraggio adottati da tali operatori dovrebbero mantenere una sorta di neutralità rispetto ai contenuti filtrati, non implicando alcuna scelta politica ma rispondendo unicamente alla necessità di offrire un servizio al pubblico il quale, come noto, è composto dalla

comunità di utenti le cui scelte, in relazione a ciò che si ritiene appropriato, possono essere molto diverse tra loro. Diversamente, appare ammissibile riconoscere che il *service provider* o il *content provider* possano operare scelte significative in relazione ai contenuti filtrati e ciò perché, diversamente dal mero fornitore d'accesso, esplicano un'attività specificamente orientata nei confronti di determinate categorie di utenti.

<sup>3</sup> Tale sistema viene ritenuto abbastanza sicuro in quanto si considera estremamente remota la possibilità che due *files* generino un valore di *hash* identico (e ciò anche se la complessità di *files* di origine esistenti, video, immagini o altro, supera enormemente il numero di valori di *hash* che possono essere generati). La caratteri-



Mediante la selezione e la combinazione dei sopra indicati elementi, viene quindi creata una lista di dati che il sistema di filtro dovrà riconoscere al fine di attuare le misure di volta in volta richieste. In particolare, qualora sia creata una c.d. «*block-list*», il dispositivo tecnico fermerà tutti i *files* all'interno dei quali avrà rinvenuto uno o più elementi appartenenti alla predetta lista. Diversamente, qualora il sistema venga impostato su una c.d. «*allow-list*» o «*white-list*», ossia una lista contenente tutti gli elementi ritenuti appropriati (per una determinata fascia d'età, per gli impiegati di una determinata azienda, ecc.), saranno i *files* che non contengono gli elementi selezionati ad essere bloccati<sup>4</sup>. Entrambi tali sistemi, inoltre, possono prevedere un ulteriore controllo «manuale» sui contenuti, effettuato da personale specializzato. Infine, è possibile impostare il sistema di filtro sul c.d. *rating*, ossia una classificazione dei contenuti o dei siti, effettuata direttamente dagli utenti o da soggetti terzi: in base a tale sistema, ogni risorsa viene catalogata in relazione alla sussistenza di determinati elementi (presenza di materiale pornografico, violento, razzista, parole volgari, ecc.) che indicano con sufficiente precisione l'affidabilità della risorsa stessa.

Nella realtà, accade sovente che il filtraggio venga effettuato mediante la combinazione di tutti i sistemi descritti, al fine di ottenere la maggiore sicurezza del contenuto caricato e visionato sul computer dall'utente finale. Tuttavia, ciò nonostante, si possono sempre verificare casi di c.d. «falsi positivi» o falsi negativi», ossia contenuti che vengono bloccati pur non corrispondendo ai parametri di ricerca o, al contrario, che non vengono filtrati pur in presenza di materiale ritenuto non idoneo.

Tali ipotesi risultano di agevole comprensione se si considera la costante tensione tra due contrapposte istanze: quella di alcuni operatori volte a creare filtri sempre più sicuri ed a «maglie», potremmo dire, sempre più strette e quella, opposta, rappresentata dagli altri soggetti che creano contenuti o *software* in grado di aggirare e superare i filtri stessi. Tale contrapposizione non sembra definitivamente superabile da nessuna delle due parti, stante la tendenziale inarrestabilità dello sviluppo informatico e, così, appare inevitabile la corsa continua per aggiornare e migliorare i sistemi di filtraggio in relazione alla sempre maggiore insidiosità dei contenuti.

---

stica della funzione di *hash*, inoltre è quella di non consentire di risalire al *file* di origine e, pertanto, viene definita «a senso unico». La tecnologia posta alla base della firma digitale si giova proprio di tale principio, noto anche come crittografia asimmetrica, in virtù del quale un utente che voglia inviare un messaggio riservato, può cifrarlo utilizzando la propria chiave privata (in tal modo, gli attribuisce una «impronta» unica) da inviare unitamente alla firma stessa, che sarà decifrata solo dal destinatario il quale potrà controllarne l'autenticità e la non avvenuta manipolazione de messaggio utilizzando un'altra chiave (quella pubblica) del mittente: in tal modo,

se le due «impronte» coincidono, si può affermare che il messaggio non ha subito alcuna modificazione successiva alla sua sottoscrizione da parte dell'autore.

<sup>4</sup> Nella realtà esistono numerose tipologie di liste in relazione alle diverse esigenze che emergono in seno alle comunità: si pensi alle liste che impediscono l'accesso a determinati *link*, o a liste che impediscono la ricerca di contenuti provenienti da determinate fonti, liste basate sull'attendibilità degli URL, ecc. Conseguentemente, i sistemi saranno impostati per riconoscere determinati *link*, determinati URL, determinati siti che vengono aggiornati o, diversamente che non vengono mai aggiornati.

Ad uno sguardo d'insieme si potrebbe ritenere che tali dispositivi abbiano, come fine ultimo, quello di limitare la diffusione di contenuti anche illeciti e tuttavia, qualora si ritenga di approfondire maggiormente il tema non si può negare che non sia certo l'illiceità (che peraltro dovrebbe essere oggetto di uno specifico accertamento giudiziale) o la presunta illiceità, l'elemento che determina l'inclusione del contenuto all'interno di una lista.

Tali premesse appaiono sufficienti ad illustrare la complessità della tematica in esame che necessita di essere approfondita in relazione ai tanti profili controversi<sup>5</sup>.

Un primo aspetto di particolare rilievo concerne l'identità e la legittimazione dei soggetti preposti alla creazione delle liste (siano esse strutturate come *block-list*, come *white-list* o come sistemi di *rating*) necessarie al funzionamento dei sistemi di filtro. Occorrerà, in altri termini, stabilire chi ha la facoltà di determinare i criteri di selezione dei contenuti informativi e dunque cosa, diversamente, debba essere filtrato<sup>6</sup>. Non va sottovalutato, poi che all'interno di un ordinamento, l'effettiva valutazione sulla natura illecita dei contenuti è demandata all'Autorità Giudiziaria la quale, in via esclusiva, dovrebbe poter decidere ed irrogare le sanzioni conseguenti a tale carattere. Lo stesso potere potrebbe essere demandato, in virtù di un espresso indirizzo dato da una fonte normativa, ad altri soggetti, quali ad esempio, le autorità amministrative indipendenti.

Diversamente, nel caso in cui le misure particolarmente gravose (quali il divieto di caricamento e apertura del *file* o la restrizione alla loro circolazione) vengano adottate da soggetti privati, quali sono gli intermediari dei servizi della società dell'informazione senza l'autorizzazione degli stessi utenti destinatari dei servizi medesimi, si potrebbe determinare una illecita intromissione nella corrispondenza privata<sup>7</sup> la cui segretezza

<sup>5</sup> Sul tema, per una prima sistemazione, cfr. G. FINOCCHIARO, *Filternig e responsabilità del provider*, in *AIDA*, Milano, 2010, 340.

<sup>6</sup> Tale riflessione, non di poco conto, comporta la necessità di attribuire ad un'organizzazione nazionale o internazionale, accreditata e riconosciuta, l'autorità e la legittimazione ad effettuare tale scelta che, in ogni modo, appare fortemente discrezionale. Ad esempio, sul tema della sicurezza delle reti per i minori, la Commissione Europea ha varato il programma denominato *Safer Internet* che si articola prevalentemente in quattro direzioni: contrastare la diffusione di contenuti illegali (es. pedopornografia) in particolare su internet e cellulari; contrastare la diffusione di contenuti potenzialmente dannosi per i minori; promuovere la diffusione della consapevolezza dell'importanza di navigare in un ambiente sicuro per bambini e adolescenti; incoraggiare azioni di sensibilizzazione a un utilizzo sicuro di Internet rivolte a giovani e adulti (Informazioni tratte dal sito internet del Ministero delle Pari Op-

portunità all'indirizzo: <http://www.pariopportunita.gov.it/index.php/quinsonsitocca/1946-inhope-e-insafe>). A tal fine ha promosso la creazione di due reti europee INHOPE e INSAFE: il primo è un *network* che offre la possibilità a chi naviga in Rete di segnalare contenuti illegali o potenzialmente dannosi per bambini e adolescenti, così da contrastarne la diffusione e limitarne l'accessibilità (per maggiori informazioni cfr. il sito <http://www.inhope.org/gns/home.aspx>); il secondo è un *network* che ha lo scopo di agevolare lo scambio di buone prassi tra i diversi membri e di offrire occasioni di formazione in linea con la continua evoluzione di Internet e cellulari (per approfondimenti v. il sito: <http://www.saferinternet.org/web/guest/home>).

<sup>7</sup> Si pensi, in proposito, ai numerosi filtri anti-*spam* e anti-*pishing* che normalmente vengono installati nelle caselle di posta elettronica e ciò sia automaticamente dal fornitore del servizio sia, a seguito di personalizzazione svolta direttamente dall'utente della casella.

è garantita come diritto inviolabile dell'individuo, in relazione alla quale ogni eventuale limitazione è soggetta alla duplice riserva di giurisdizione e di legge<sup>8</sup>.

Tuttavia, anche il semplice inserimento di un URL, di un contenuto informativo o di un *file* all'interno di una *block-list*, oltre a porre problemi di qualificazione ai sensi della normativa sul trattamento di dati personali<sup>9</sup>, potrebbe rappresentare un'indebita compressione del diritto alla libertà dell'individuo ed alla libera espressione e manifestazione del pensiero, tanto più nelle ipotesi di *over-blocking*.

In proposito, occorre anche ricordare che per talune categorie di utenti (si pensi alle persone con disabilità grave tale da non consentire libertà di movimento) l'utilizzo della rete costituisce il più significativo, se non l'unico, modo per comunicare all'esterno. In tali casi, quindi, ogni misura volta perfezionare tali sistemi di filtraggio per renderli sempre più efficienti, potrebbe risultare ancora più insidiosa.

Inoltre, è indubbio che l'effetto immediato di tali sistemi di filtraggio è, comunque, quello di limitare la libera circolazione dei contenuti e, con

<sup>8</sup> Come precisa il Rapporto cit., 179 e ss., occorre, inoltre, considerare che il concetto di posta implica « una comunicazione personale e temporanea, suscettibile di interattività, indirizzata a soggetti individualmente determinati » che, nel complesso panorama della Rete, può coincidere solo parzialmente con i messaggi elettronici effettivamente trasmessi tramite caselle di posta. Infatti, secondo la richiamata definizione, i caratteri distintivi della posta sono costituiti dalla personalità del messaggio, ossia dalla circostanza che lo stesso sia specificamente indirizzato nel destinatario anche nel contenuto (in altri termini, un messaggio commerciale non può costituire un messaggio personale, salvo che anche il contenuto contenga riferimenti precisamente individuati al destinatario sfruttando, ad esempio, le sue scelte in fatto di consumi) e dalla temporalità dello stesso, ossia dalla circostanza che il messaggio sia temporalmente circoscrivibile e connesso a determinati avvenimenti (in tal modo, non sarebbe ritenuta temporanea una comunicazione che può ben adattarsi a tutte le epoche). Inoltre, sempre secondo la definizione riportata, occorre che il messaggio stesso sia indirizzato a destinatari individualmente determinati, circostanza che lo rende (o dovrebbe renderlo) non visionabile dai terzi. Alla luce di tale enunciazione, pertanto, ogni mezzo di comunicazione che permetta l'interattività, la personalità e la temporaneità del messaggio, nonché la possibilità di escludere i terzi, può effettivamente costituire supporto per la corrispondenza. Si pensi, oltre all'*e-mail*, ad aree private messe a disposizione sul *web* per scambiare informa-

zioni (come un *forum* privato, una *chat* privata). È, quindi, evidente come la penetrazione del controllo effettuato dai sistemi di filtraggio sia potenzialmente idonea ad interferire non solo con le *e-mail*, ma anche con altre tipologie di messaggi che normalmente vengono scambiati tra gli utenti.

<sup>9</sup> Il tema dei dati personali risulta di estremo rilievo atteso che, a seguito della direttiva comunitaria 95/46/CE, tutti gli Stati membri si sono dotati di una legislazione che, conformemente al testo di riferimento, tutela anche la confidenzialità di tali dati. Ai sensi dell'art. 2, comma 1, lett. a) della direttiva, recepito dall'art. 4, comma 1, lett. b), della legge 30 giugno 2003, n. 196, sono considerati dati personali « toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ». Alla luce di tale enunciazione, sembrerebbero assimilabili ai dati personali anche gli indirizzi IP, atteso che identificherebbero univocamente il titolare di un accesso a Internet e, conseguentemente, la loro registrazione all'interno di una banca di dati dovrebbe avvenire solo a seguito del consenso del titolare. Tale problematica è stata oggetto del noto caso c.d. *Peppermint*, in questa *Rivista*, 2007, 828, con nota di C. BLENGINO e M.A. SENOR alla quale si rinvia per maggiori approfondimenti.

essi, delle idee e delle informazioni che ne sono alla base, in relazione alla contrapposta esigenza di « ripulire » la rete da contenuti ritenuti inappropriati. Secondo tale logica, quindi, un diritto inviolabile costituzionalmente garantito viene, contrapposto e persino compresso non da un ordine dell'Autorità Giudiziaria o da una disposizione di legge, o, eventualmente, da un diritto di pari rango, bensì da un'istanza (che può essere più o meno condivisa dalla generalità degli utenti), che può essere comunque priva di riconoscimento costituzionale. Appare, quindi, in tutta la sua criticità il rapporto tra tali diritti di libertà costituzionalmente garantiti da un lato e le contrapposte richieste, provenienti dagli utenti della rete o dai titolari di diritti di proprietà intellettuale, che tuttavia non possono essere ignorate.

Alla luce di alcuni provvedimenti normativi tendenti a proteggere con maggior vigore alcune situazioni giuridiche soggettive, si potrebbe anche ritenere che la tutela degli interessi ivi considerati possa giustificare la creazione di filtri: si tratta delle norme in tema di tutela dei minori<sup>10</sup>, discriminazione razziale<sup>11</sup> e protezione della proprietà intellettuale<sup>12</sup>.

Sembra anche fondato ammettere che mentre l'installazione di un sistema di filtro da parte del singolo utente (ovvero da parte di una comunità di utenti che condivide i medesimi valori in merito a cosa sia appropriato e cosa, invece, sia preferibile bloccare) possa essere considerata come l'esplicazione della libertà di autodeterminazione dell'individuo, in relazione, ad esempio, alla scelta in merito alla tipologia di contenuti da ricevere o ai quali poter accedere, quando tale installazione sia effettuata dai *provider* di accesso, la tendenziale neutralità del sistema rispetto ai contenuti potrebbe determinare una significativa restrizione alla libertà di circolazione delle informazioni ed alla libera manifestazione del pensiero.

Per altro verso, occorre anche considerare che qualora il *provider* effettui un controllo mirato o che, comunque, possa essere ritenuto non-neutrale, sarebbe sottoposto al regime di responsabilità delineato dalla direttiva comunitaria 2000/31/CE. Ma, come affermato dalla pronuncia resa dal Tribunale dei Creteil, una volta riconosciuta la responsabilità del *provider* per l'illiceità di determinati contenuti immessi in

<sup>10</sup> Si fa riferimento, in particolare, alla Convenzione Internazionale dei Diritti dell'Infanzia approvata dall'Assemblea generale delle Nazioni Unite il 20 novembre 1989 e ratificata dall'Italia con legge del 27 maggio 1991, n. 176 all'interno della quale viene prescritto il diritto dei fanciulli di essere tutelati da « ogni forma di violenza, di oltraggio o di brutalità fisiche o mentali, di abbandono o di negligenza, di maltrattamenti o di sfruttamento, compresa la violenza sessuale » (art. 19), ogni forma di « sfruttamento economico » (art. 32), « sessuale e di violenza sessuale » (art. 34) e « ogni altra forma di sfruttamento pregiudizievole al suo benessere in ogni suo aspetto » (art. 36). Per approfondimenti, v. il sito: <http://www.unicef.it/doc/599/il->

[testo-della-convenzione-sui-diritti-dell'infanzia.htm](http://www.unicef.it/doc/599/il-testo-della-convenzione-sui-diritti-dell'infanzia.htm).

<sup>11</sup> Si fa riferimento, in particolare, alla Convenzione Internazionale per l'eliminazione di ogni forma di discriminazione razziale, Adottata dall'Assemblea Generale delle Nazioni Unite il 21 dicembre 1965, entrata in vigore il 4 gennaio 1969 e resa esecutiva in Italia con la legge n. 654 del 13 ottobre 1975, entrando in vigore per l'Italia il 4 febbraio 1976. Per approfondimenti v. il sito: <http://www.conflicti-dimenticati.it/cd/docs/1225.pdf>.

<sup>12</sup> Si fa riferimento alle numerose convenzioni internazionali sulla tutela del diritto d'autore per le quali consulta il sito: <http://www.wipo.int/treaties/fr/ip/wct/index.html>.

rete e subordinatamente alla rimozione degli stessi, l'attività di controllo preventivo mirata diviene non solo lecita, ma obbligatoria, allorché sia finalizzata ad impedire la reiterazione dell'illecito giudizialmente accertato<sup>13</sup>.

VIRGINIA RAGGI

---

<sup>13</sup> Tale principio, affermato dalla sentenza francese, non affronta, tuttavia, alcuni profili critici che l'adozione di siffatta misura di filtraggio potrebbe determinare. In primo luogo, una volta affermato l'obbligo del controllo preventivo a seguito di una precedente segnalazione, occorrerà valutare se la responsabilità del *provider* risulti accresciuta e ciò anche in relazione alla possibilità pratica che il sistema di filtraggio installato sia costantemente aggiornato ed in relazione alla possibilità, di andare incontro a fenomeni di *overblocking* (che si determina allorché il

sistema blocchi anche contenuti che non corrispondevano a quanto segnalato, e si verifica, dunque, un eccesso di blocco di dati) o *underblocking* (che si realizza, all'opposto, quando il filtro tralasci di bloccare alcuni contenuti che, diversamente, non avrebbero dovuto essere caricati). Inoltre, occorrerà determinare con precisione il significato dell'espressione « *remise in ligne* » utilizzata dal Giudice, in relazione a quelle fattispecie ove il materiale nuovamente caricato da terzi coincida solo in parte con quello oggetto della precedente segnalazione.