

DA ARPANET AL SOCIAL WEB*. ASPETTI INFORMATICO- GIURIDICI

PARTE 3

Dott. Gianluigi Fioriglio

Indice sommario

5.1 Il cloud computing.....	1
5.2 Il ruolo dell'utente nel social web.....	3
6.1 Il provider. Aspetti generali.....	4
6.2.1 Il d.lgs. 70/2003: premessa e aspetti generali.....	7
6.2.2 Il d.lgs. 70/2003: la responsabilità del provider.....	9
6.3 Il provider. alcuni casi giurisprudenziali.....	11

5.1 IL CLOUD COMPUTING

Il *cloud computing* costituisce un'espressione oramai entrata nell'uso comune, talvolta a sproposito. In linea generale, con essa si definiscono i servizi di rete forniti mediante server virtuali distribuiti (software distribuito su hardware "reale").



Figura 1 - Rappresentazione grafica semplificata del concetto di cloud computing

Si possono qui distinguere tre tipologie principali:

- IaaS (Infrastructure as a Service): utilizzo di una infrastruttura computazionale, il cui hardware viene generalmente riservato, in tutto o in parte, solo quando ciò è necessario (es. Amazon Web Services);
- PaaS (Platform as a Service): utilizzo di una piattaforma software (es. software applicativi *sub* Google App Engine o Microsoft Azure);
- SaaS (Software as a Service): utilizzo di uno o più programmi da remoto (es. Google Docs e Microsoft Office 365).

Si possono inoltre menzionare:

- DaaS (Data as a Service): utilizzo dati di varia tipologia (es. dati satellitari);
- NaaS (Network as a Service): fornitura di connettività (es. VPN, Virtual Private

* Parte della presente dispensa è stata estratta, con modificazioni e aggiornamenti, da G. Fioriglio, *Temi di informatica giuridica*, Aracne, Roma, 2004 (l'intero volume è liberamente scaricabile da www.dirittodellinformatica.it).

Network).

Come affermato dal Garante per la protezione dei dati personali, “L'utilizzo di servizi di *cloud computing* è un fenomeno in forte ascesa e determina un cambio di mentalità nelle modalità di utilizzo della rete Internet che, da strumento di condivisione documentale, diviene la porta di accesso alle risorse elaborative e di stoccaggio di fornitori di servizi remoti”¹.

Il *target* di ciascuna tipologia di servizi può essere vario: così, non è raro che sia professionisti sia consumatori usufruiscano di servizi di SaaS resi mediante tecnologie di cloud computing, mentre le IaaS sono tendenzialmente rivolte ai professionisti. La dottrina, con precipuo riferimento alle questioni sollevate in tema di diritto d'autore, ha altresì individuato i c.d. *cyberlockers* quali prestatori di servizi di cloud computing (dunque rivolti sostanzialmente ai consumatori)².

Al cloud computing si tende a ricorrere per i vari benefici offerti, fra cui si possono qui ricordare:

- Scalabilità;
- Abbattimento di costi;
- Spostamento di alcuni rischi hardware/software dall'utilizzatore al prestatore.

Si pongono, però, alcune problematiche:

- Disponibilità di adeguata connessione di rete;
- Necessità di pagamento di canone periodico;
- Limitazione nel tempo dei diritti di utilizzo;
- Ancora maggiore distanza dal concetto di proprietà³ che già di per sé non caratterizza il mondo del software, in cui ci si rifà solitamente al concetto di licenza d'uso e dunque della concessione della possibilità di utilizzare un software e non di diventarne proprietario.

In aggiunta a quanto accennato, è possibile individuare questioni giuridiche e informatiche di particolare rilevanza teorico-pratica. In particolare, come individuare la legge applicabile? Un primo importante elemento in tal senso può derivare dalla lettura del contratto di riferimento nonché dall'indicazione del luogo in cui i server sono materialmente collocati. L'internazionalità del fenomeno comporta un'ulteriore conseguenza: i costi per far valere i propri diritti possono essere molto elevati, poiché potrebbe essere necessario adire l'autorità giudiziaria di uno stato anche molto lontano (come, ad esempio, gli Stati Uniti) e magari caratterizzato da costi di giustizia molto più elevati di quelli italiani.

Inoltre, si pone la questione della tutela della privacy e della sicurezza dei dati memorizzati nella “nuvola”, anche in ordine alla collocazione fisica dei dispositivi presso cui i dati sono archiviati e trattati. Oltretutto, la normativa vigente è stata pensata in un momento storico in cui, fra l'altro, la tecnologia era meno pervasiva rispetto ad oggi, per cui soffre di un'impostazione “centralistica” e sarebbe forse opportuno un ripensamento effettivo (che vada anche oltre i meccanismi dello stesso GDPR, cui si accennerà nella sede opportuna). Bisogna comunque tenere presente che “l'utente, affidando i dati ai sistemi di un fornitore remoto, ne perde il controllo diretto ed esclusivo; la riservatezza e la disponibilità delle informazioni allocate sulla nuvola certamente dipendono anche dai

¹ Garante per la protezione dei dati personali, *Cloud computing: indicazioni per l'utilizzo consapevole dei servizi*, Roma, 2011, p. 11 (<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1819933>).

² M.L. Montagnani, *Primi orientamenti in materia di responsabilità dei fornitori di servizi cloud per violazione del diritto d'autore in rete*, in *Riv. Dir. Ind.*, 2014, 3. I cyberlockers forniscono, essenzialmente, un servizio di hosting di file che possono essere condivisi con una molteplicità di utenti; per ulteriori specificazioni si rinvia al materiale didattico sul diritto d'autore.

³ Cfr. anche su questo punto, con particolare riferimento ai diritti di proprietà intellettuale, G. Noto La Diega, *Il cloud computing. Alla ricerca del diritto perduto nel Web 3.0*, in *Eur. Dir. Priv.*, 2014, 2, p. 577.

meccanismi di sicurezza adottati dal *service provider*; [come se non bastasse], il servizio prescelto potrebbe essere il risultato finale di una catena di trasformazione di servizi acquisiti presso altri *service provider*, diversi dal fornitore con cui l'utente stipula il contratto di servizio; l'utente a fronte di filiere di responsabilità complesse potrebbe non sempre essere messo in grado di sapere chi, dei vari gestori dei servizi intermedi, può accedere a determinati dati⁴. In aggiunta, bisogna considerare che la sicurezza informatica di taluni servizi di cloud computing (e non solo di essi) può essere messa a rischio dalla interazione fra più servizi, per cui una falla in un sistema potrebbe essere utilizzata nei confronti di un altro; a mero titolo esemplificativo, si pensi alla comunicazione delle credenziali di autenticazione relative a un servizio non solo a chi lo fornisce ma anche a uno o più soggetti terzi che forniscono, a loro volta, altri servizi (in tal modo, aumentano le probabilità di un uso illecito di tali credenziali perché “custodite” da più soggetti).

La perdita del controllo o del possesso esclusivo non sono conseguenze di poco conto e tutt'altro che rare; basti pensare che determinati prestatori di servizi effettuano taluni trattamenti automatizzati sui file, al fine di ottimizzare le risorse. Ad esempio, se un medesimo file viene memorizzato da più utenti, è possibile che il provider faccia uso di un meccanismo per cui ne viene in realtà memorizzata una sola copia, ovviamente associata all'account di ciascun utente (per cui la cancellazione ad opera di uno non dovrebbe avere alcun effetto sugli altri). Ciò è reso possibile dalla immaterialità dei dati informatici, ma pone problematiche giuridiche anche in ordine alla effettiva conoscenza dei dati da parte del prestatore del servizio che si trova, dunque, ad effettuare operazioni di trattamento sui medesimi.

Infine, si può ricordare il ruolo del prestatore di servizi di cloud computing, che diviene hosting provider, con tutto ciò che ne consegue in ordine all'applicabilità della relativa disciplina, poiché la particolarità degli strumenti utilizzati non ne fa venire meno il ruolo sostanziale. Circa le soluzioni giuridiche prospettabili, si è osservato che “Le soluzioni [...] non sempre - o non solo - devono essere cercate nell'ambito della responsabilità dei fornitori di servizi cloud e nel tentativo di coinvolgere questi soggetti nella rimozione dei contenuti che circolano in maniera non autorizzata, o nella prevenzione della circolazione di contenuti non autorizzati tramite sistemi di filtraggio, o ancora nel blocco dei siti che forniscono l'accesso a materiale (anche) non autorizzato (a discapito peraltro del materiale invece lì conservato in maniera lecita). Tali soluzioni possono e devono passare anche per l'adeguamento non della rete alle norme, quanto delle norme alla rete, adeguamento che si realizza tramite il potenziamento della capacità includente del diritto d'autore, ossia ripensando le privative non solo in termini di diritto ad autorizzare, ma anche — e soprattutto in rete — in termini di diritto ad essere retribuito ogniqualvolta il contenuto su cui si vantano dei diritti venga fruito”⁵.

5.2 IL RUOLO DELL'UTENTE NEL SOCIAL WEB

Nella Società dell'informazione, in generale, e nel Social Web, in particolare, l'utente ha un ruolo fondamentale, come si è visto.

Quando l'utente è anche un consumatore, ossia non agisce nell'ambito della propria attività professionale, può contare su una normativa finalizzata a riequilibrare un rapporto contrattuale che lo vede in netto svantaggio rispetto al prestatore.

Così, in linea generale, si possono qui ricordare, senza pretesa alcuna di esaustività, talune normative che disciplinano il ruolo dell'utente “telematico”:

⁴ Garante per la protezione dei dati personali, *Cloud computing: indicazioni per l'utilizzo consapevole dei servizi*, cit., p. 12.

⁵ M.L. Montagnani, op. cit..

- D.lgs. 70/2003 (Commercio elettronico);
- D.lgs. 206/2005 (Codice del consumo);
- D.lgs. 196/2003 (Codice della privacy) e, dal 25 maggio 2018, il Regolamento UE 2016/679 (GDPR);
- D.P.R. 430/2001 (Manifestazioni a premio);
- D.lgs. 82/2005 (Codice dell'amministrazione digitale).

Inoltre, gli utenti possono rivolgersi a diverse Autorità, come:

- Autorità Garante della Concorrenza e del Mercato (Antitrust);
- Garante per la protezione dei dati personali (Garante privacy);⁹,
- Autorità per le Garanzie nelle Comunicazioni (AGCOM).

Le brevi elencazioni di cui sopra permettono di evidenziare i diversi ruoli che l'utente può avere nella Società dell'informazione:

- Fornitore di contenuti;
- Responsabile dei contenuti immessi da se medesimo;
- Oggetto di profilazione automatizzata;
- Utente-consumatore di beni e servizi, anche vittima di pubblicità ingannevoli⁶;
- Partecipante a concorsi e operazioni a premio on line;
- Cittadino "telematico".

In molti casi, il rapporto giuridico è regolamentato in primo luogo dai termini di servizio e dalle privacy policy e solo in secondo luogo dalla normativa, anche quando inderogabile. Ciò può avvenire poiché diviene spesso difficile, anche se magari non impossibile, far prevalere la normativa vigente sui termini di servizio anche quando essi la violano; spesso, infatti, le azioni che possono essere esercitate comportano un dispendio di tempo e denaro tali da indurre l'utente a desistere. In tal senso, dinanzi al crescente numero di micro-lesioni immateriali, è fondamentale l'operato delle predette Autorità per tentare di ridurlo.

In tale quadro, si pone altresì il paradosso dell'UGC (User Generated Content): esso viene creato dagli utenti (come suggerisce il nome stesso), cui dovrebbero spettare i diritti d'autore così come previsti dalla l. 633/1941 (legge sul diritto d'autore). Dal loro sfruttamento, seppur indiretto, trae di norma giovamento il provider che fornisce la piattaforma: sarebbe dunque necessario cercare una forma di indennizzo, quanto meno, che vada oltre l'attuale compensazione (per cui un servizio viene reso in forma apparentemente gratuita). Inoltre, sarebbe necessario trovare forme e standard per consentire la trasportabilità di dati e account, anche se ciò potrebbe risultare molto difficoltoso in virtù delle diverse piattaforme utilizzate da ciascun prestatore.

6.1 IL PROVIDER. ASPETTI GENERALI

Le tecnologie dell'informazione e della comunicazione (ICT) non eliminano la figura dell'intermediario, come spesso si tende a ritenere. Invero, nuovi intermediari controllano e possono cancellare le informazioni. A titolo esemplificativo, basti pensare ai seguenti prestatori di servizi:

- Motori di ricerca (ad es., Google: circa il 95% di utilizzo in Italia);
- Hosting e service provider (ad es., YouTube, Wordpress, Aruba);
- Social network (ad es., Facebook e Twitter);

⁶ Il Codice del consumo, in particolare, detta una serie di disposizioni che regolamentano il rapporto fra professionista e consumatore (e, in determinati casi, fra professionista e microimprese). Così, sono disciplinati i contratti negoziati fuori dei locali commerciali e a distanza, nonché il diritto di recesso e la garanzia per difetti di conformità. Sono inoltre regolamentate, e vietate, le pratiche commerciali scorrette (ingannevoli e aggressive), in merito a cui l'Antitrust può adottare gli opportuni provvedimenti.

- Riviste telematiche e siti di informazione; forum di discussione.

Come sottolinea Manuel Castells, poi, i principali servizi online (ad es., YouTube e Facebook) possono essere punti critici tra:

- media;
- reti di auto-comunicazione di massa;
- portatori di interessi commerciali (ad es., servizi di *advertising*);
- attori politici (che vogliono filtrare o introdurre contenuti in tutti questi network)⁷.

È evidente, dunque, l'importanza di difendere la neutralità della Rete e degli strumenti tecnologici per garantire la libertà: tale esigenza diventa sempre più pressante in una società tanto pervasa dalla tecnologia quanto quella contemporanea.

Ciò non deve però far dimenticare che Internet è meno decentralizzata di quanto sembri: (relativamente) pochi siti sono enormemente visitati, mentre la maggior parte passa inosservata, come osserva Benkler⁸.

La figura che segue mostra i dieci siti più visitati al mondo (dati aggiornati a ottobre 2014):

1	Google.com Enables users to search the world's information, including webpages, images, and videos. Offers... More
2	Facebook.com A social utility that connects people, to keep up with friends, upload photos, share links and ... More
3	Youtube.com YouTube is a way to get your videos to the people who matter to you. Upload, tag and share your... More
4	Yahoo.com A major internet portal and service provider offering search results, customizable content, cha... More
5	Baidu.com The leading Chinese language search engine, provides "simple and reliable" search exp... More
6	Wikipedia.org A free encyclopedia built collaboratively using wiki software. (Creative Commons Attribution-Sh... More
7	Amazon.com Amazon.com seeks to be Earth's most customer-centric company, where customers can find and disc... More
8	Twitter.com Social networking and microblogging service utilising instant messaging, SMS or a web interface.
9	Qq.com China's largest and most used Internet service portal owned by Tencent, Inc founded in Nov... More
10	Taobao.com Launched in May 2003, Taobao Marketplace (www.taobao.com) is the online shopping destination of... More

Figura 2 – Siti più visitati (dati Alexa.com, ottobre 2014)

Quanto qui brevemente esposto, corroborato ulteriormente dalla figura 2, consente di evidenziare come vi sia una sempre crescente centralità dei provider e degli utenti. I primi forniscono la piattaforma tecnologica per l'accesso alle informazioni, i secondi i contenuti. Insieme essi sono le chiavi per comprendere il web 2.0 e la sua evoluzione “social”⁹. Analizziamo, dunque, il quadro normativo *in subiecta materia*, partendo proprio dai provider, in merito a cui si possono effettuare le seguenti distinzioni di base:

- Internet access provider / Internet service provider; e
- Provider attivo / provider passivo (v. *infra*); e
- mere conduit provider / caching provider / hosting provider (rilevanti, in particolare,

⁷ M. Castells, *Communication Power*, New York 2009.

⁸ Y. Benkler, *The Wealth of Networks. How Social Production Transforms Markets and Freedom*, New Haven and London 2006.

⁹ *Ibidem*.

ai fini del d.lgs. 70/2003: v. *infra*).

Una prima distinzione, come si è detto, deve essere effettuata fra *Internet access provider (IAP)* e *Internet service provider (ISP)*, che, rispettivamente, forniscono accesso alla rete Internet e servizi della Società dell'informazione. Pertanto, qualsiasi attività posta in essere su Internet, come la semplice visione di un sito *web* o l'invio di un messaggio di posta elettronica, lo è sempre per mezzo del *provider*, dal momento che tutti i dati da e verso i computer dei suoi clienti passano tramite i suoi elaboratori. Quando l'ISP fornisce uno spazio *web* alla propria clientela può semplicemente mettere a disposizione un determinato spazio o creare e gestire il sito secondo i desideri della clientela stessa, ma comunque con un'attività propria. Nel primo caso si parla di *hosting provider*, nel secondo di *content provider*.

Queste distinzioni sono di importanza fondamentale per la ricostruzione del regime di responsabilità applicabile all'ipotesi di comportamenti illeciti effettuati via Internet attraverso gli elaboratori del *provider*. Difatti, nel caso in cui l'autore dell'illecito risulti anonimo¹⁰, per consentire il risarcimento al danneggiato è necessario configurare la responsabilità del *provider*. Nella maggior parte dei casi è possibile risalire al nome dell'utente che ha commesso la violazione: ciò è realizzabile tramite l'utilizzo dei *file di log*¹¹, anche se al riguardo si pone l'ulteriore problema dell'utilizzo abusivo di credenziali altrui (*user ID* e *password*)¹². Il primo caso europeo rilevante si è verificato in Francia ed è stato deciso dalla Corte d'appello di Parigi il 10 febbraio 1999¹³: i giudici d'oltralpe hanno stabilito che il *provider* che offre ospitalità anonima e senza restrizioni di accesso, consentendo la diffusione di segni, scritti, immagini, suoni e messaggi, estranei alla corrispondenza privata, eccede il ruolo tecnico di semplice trasmettitore di informazioni ed è direttamente responsabile nei confronti dei terzi del compimento di atti illeciti all'interno dei siti che gestisce. Un altro caso straniero molto celebre (*Godfrey v. Demon*) è stato originato dalla diffamazione nei confronti del dott. Laurence Godfrey, avvenuta in un *newsgroup*: in questa occasione, è stata riconosciuta la responsabilità in capo al *provider* per l'immissione di dichiarazioni diffamatorie da parte di un soggetto rimasto anonimo¹⁴.

Si è mossa sostanzialmente nello stesso senso anche la Corte europea dei diritti dell'uomo nella decisione sul caso *Delfi AS c. Estonia* del 10 ottobre 2013, confermata il 16 giugno 2015 a seguito del ricorso di Delfi¹⁵. Più specificatamente, il gestore di un portale (Delfi) è stato condannato per i commenti diffamatori posti in calce a un articolo, poiché, avendo concesso la

¹⁰ "L'anonimato, infatti, può essere usato per violare la *privacy* altrui"; così S. Rodotà, *Tecnopolitica*, Roma-Bari 1997, p. 145; tuttavia "la possibilità di rimanere anonimi è indispensabile per garantire nel cyberspazio il rispetto dei diritti fondamentali alla riservatezza e alla libertà di espressione" (G. Santaniello, *Privacy telematica e utilizzo di Internet, reti e servizi di telecomunicazioni*, in <http://www.privacy.it/convirisant.html>); B. Donato, *La responsabilità dell'operatore di sistemi telematici*, in *Dir. inf.*, 1996, 1, p. 146, da un lato considera che "l'anonimato della connessione costituisce un incentivo al reato informatico", dall'altro esprime la preoccupazione che estendendo il regime della responsabilità oggettiva nei confronti del *provider*, venga giustificata l'intrusione di questi finanche nelle caselle di posta elettronica.

¹¹ Il *log file* memorizza lo *user ID* (o *login*, o nome di accesso), la *password* e tutte le azioni compiute da un determinato soggetto per mezzo dell'elaboratore elettronico con cui questi si collega alla Rete.

¹² Si pensi al caso, tutt'altro di scuola, del tecnico che apprende le suddette informazioni durante la sua opera di configurazione o di riparazione di un determinato *computer* (anche se in tal caso sussiste la colpa del cliente, il quale dovrebbe subito cambiare la *password* o in ogni modo non comunicarla); in tal caso, comunque, troverebbe applicazione l'art. 615-ter cod. pen.

¹³ In *Danno e resp.*, 1999, 7, p. 754, con nota di F. Di Ciommo, *Internet, diritti della personalità e responsabilità aquiliana del provider*, pp. 756–765, e in *Dir. inf.*, 1999, 4–5, p. 926, con nota di G. M. Riccio, *La responsabilità del provider nell'esperienza francese: il caso Hallyday*, pp. 929–941. Il caso riguardava la pubblicazione, sul sito <http://altern.org/silversurfer>, di fotografie di nudo ritraenti la sig.ra Estelle Hallyday, senza il suo consenso.

¹⁴ Per una analisi più dettagliata del caso v. Y. Akdeniz, *Case Analysis: Laurence Godfrey v. Demon Internet Limited*, in *Journal of Civil liberties*, 1999, 4 (2).

¹⁵ Le decisioni possono essere reperite al seguente indirizzo: <http://hudoc.echr.coe.int>.

possibilità di ospitare commenti anonimi e avendo comunque interesse a ricevere visite e commenti, non ha adottato misure sufficienti per evitare di essere considerato responsabile (così, il filtraggio automatico preventivo di alcune parole e il sistema di *notice and take down* sono stati ritenuti insufficienti), anche alla luce del fatto che il contenuto stesso dell'articolo fosse per sua natura idoneo a suscitare reazioni negative. Come anticipato, il 16 giugno 2015 la Corte (con quindici voti a favore e due contrari) ha confermato questa decisione (sulla base della natura “estrema” dei commenti, della natura commerciale del portale, dell'insufficienza delle misure adottate da Delfi dopo la pubblicazione dei commenti, nonché del modesto ammontare della sanzione imposta dai giudici estoni al prestatore). In particolare, ha rigettato la tesi, avanzata da Delfi, della violazione dell'art. 10 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali¹⁶.

Fermo restando quanto premesso, nel corso degli anni il dibattito dottrinale e giurisprudenziale ha poi portato a definire, seppur con talune difficoltà, la distinzione fra provider attivo e passivo. Il secondo compie un'attività “di ordine meramente tecnico, automatico e passivo” (considerando n. 42, direttiva 2000/31/CE), come più compiutamente esposto nel prosieguo, e ciò giustifica, nella visione del legislatore comunitario, un diverso regime di responsabilità. Il primo, invece, svolge un'attività idonea a consentirgli un ruolo attivo nel controllo e nella gestione dei dati, oltre che la loro effettiva conoscenza. “Provider «attivo» è quello che commette illeciti direttamente, alla pari di qualsiasi altro soggetto di diritto (salva solo la particolarità dell'utilizzo del mezzo tecnico della rete), il quale, pertanto, in linea di principio, deve poter essere chiamato a rispondere della propria attività antigiuridica, ai sensi dall'art. 2043 c.c. oppure anche di previsioni speciali, non esplicitamente riferite al provider, di cui eventualmente ricorrano tutti i presupposti applicativi”¹⁷. Ovviamente, rimane fermo il regime di responsabilità contrattuale qualora il danneggiato sia legato al provider da un contratto e dunque quest'ultimo non risponda a titolo di responsabilità aquiliana.

La terza distinzione sopra ricordata è rinvenibile nel d.lgs. 70/2003, che regola le ipotesi di esenzione di responsabilità del provider, di seguito esposta.

6.2.1 IL D.LGS. 70/2003: PREMESSA E ASPETTI GENERALI

In Italia, la responsabilità del *provider* ha trovato una prima disciplina solo con il d.lgs. 9 aprile 2003, n. 70 e la mancanza di una normativa di settore ha in alcuni casi portato la giurisprudenza ad applicare analogicamente la legge sulla stampa nei confronti del *provider*¹⁸, anche se non sono mancate le pronunce in senso opposto¹⁹. In realtà, i

¹⁶ “1. Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. Il presente articolo non impedisce agli Stati di sottoporre a un regime di autorizzazione le imprese di radiodiffusione, cinematografiche o televisive. 2 L'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, alla sicurezza nazionale, all'integrità territoriale o alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del giudizio”.

¹⁷ M. Tesaro, *Schemi legali e opposte tendenze giurisprudenziali in tema di responsabilità civile dell'internet provider*, in *Giur. merito*, 2013, 12, p. 2584B.

¹⁸ Trib. Napoli 8 agosto 1997, in *Giust. civ.*, 1998, 1, I, p. 259, con nota di L. Albertini, *Le comunicazioni via Internet di fronte ai giudici: concorrenza sleale ed equiparabilità alle pubblicazioni a stampa*, pp. 261–267; inoltre, va segnalata l'ord. 23 giugno 1998, con la quale la Procura della Repubblica presso la Pretura di Vicenza ha disposto il sequestro preventivo del server di “Isole nella rete”.

¹⁹ Ad es., Trib. Teramo 11 dicembre 1997, in *Dir. inf.*, 1998, 2, p. 370, con nota di P. Costanzo, *Libertà di manifestazione del pensiero e “pubblicazione” in Internet*, pp. 372–378; G.U.P. Trib. Oristano 25 maggio 2000, in *Dir. inf.*, 2000, 4–5, p. 653, con nota di P. Costanzo, *Ancora a proposito dei rapporti tra diffusione in Internet e*

tentativi di estendere alle comunicazioni telematiche la normativa sulla stampa hanno costituito "maldestre operazioni di disciplina giuridica di realtà assai diverse e ben più complesse. Un sistema può ben vivere con delle lacune e l'*horror vacui* nasconde spesso solo una radicata vocazione dirigistica degli apparati statali cui nulla deve e può sfuggire"²⁰. Del resto, anche se si volesse far rispondere il *provider* per *culpa in vigilando*, non si terrebbe conto dell'impossibilità tecnica di controllare tutto ciò che transita fra questi e l'utente che accede ad Internet²¹.

In linea di principio, il *provider* dovrebbe invece rispondere qualora rimanga inerte o rifiuti di rimuovere dal proprio *server* messaggi, immagini, filmati o quant'altro denunciati quali lesivi di diritti altrui, qualora essi si appalesino tali, in base ad un giudizio sereno ed obiettivo: sul *provider* deve dunque gravare l'obbligo di attivarsi al più presto in caso di illecito conosciuto o conoscibile commesso tramite il proprio *server*²². Un obbligo siffatto dovrebbe ritenersi inoltre previsto dall'art. 1176 cod. civ., ai sensi del quale "nell'adempimento delle obbligazioni inerenti all'esercizio di un'attività professionale la diligenza deve valutarsi con riguardo alla natura dell'attività esercitata": dunque, il *provider* dovrebbe seguire delle regole di buona condotta tecnica che possono qualificare il suo comportamento quale "professionalmente diligente", con ovvie ripercussioni sul piano della responsabilità civile.

L'emanazione del d.lgs. 70/03, di recepimento della direttiva 2000/31/CE ("Relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno", c.d. direttiva sul commercio elettronico), avrebbe dovuto sopire il dibattito in materia²³, perché esso, come si è accennato, ha disciplinato anche la responsabilità del provider, oltre a regolamentare parzialmente il commercio elettronico²⁴: numerose disposizioni all'uopo applicabili, infatti, sono contenute nel d.lgs. 206/2005 (Codice del consumo).

Tanto premesso, è opportuno riassumere talune definizioni di cui al d.lgs. 70/2003 prima di definirne alcuni aspetti generali per poi soffermarsi sulla regolamentazione della responsabilità del provider:

- Servizi della Società dell'informazione: "le attività economiche svolte in linea – on line" e "qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per

pubblicazione a mezzo stampa, pp. 657–664.

²⁰ V. Zeno-Zencovich, La pretesa estensione della telematica al regime della stampa: note critiche, in "Dir. inf.", 1998, p. 28.

²¹ S. Bariatti, *Internet e il diritto internazionale privato: aspetti relativi alla disciplina del diritto d'autore*, in *AIDA*, 1996, p. 61; F. Lolli, *Il contenuto in rete tra comunicazione e informazione*, in *Resp. com. impr.*, 1999, 3, p. 447.

²² F. Di Ciommo, op. cit., p. 761; P. Sammarco, *Atti di concorrenza sleale attraverso Internet e responsabilità del provider*, in *Dir. inf.*, 2002, 1, p. 107.

²³ Il testo del d.lgs. 70/03 è stato definito "criptico, confuso, ridondante, con diversi passaggi che fanno rabbrivire i giuristi più attenti. [...] Da una parte ci sono previsioni criptiche, incomprensibili anche nel testo originale in inglese, che il nostro legislatore ha ottusamente tradotto senza curarsi del loro significato, e che quindi possono significare tutto e nulla stesso tempo" (M. Cammarata, *Le trappole nei contratti di hosting*, in <http://www.interlex.it/regole/trappole.htm>).

²⁴ Il recepimento della direttiva, però, è avvenuto mediante l'emanazione di un testo normativo che costituisce la mera trasposizione di quello comunitario: il legislatore italiano, infatti, non si è curato di apportare quelle modifiche che si palesano necessarie per il corretto inserimento delle disposizioni comunitarie nell'ambito dell'ordinamento giuridico italiano; in questo senso anche G. M. Riccio, *La responsabilità degli internet providers nel d.lgs. n. 70/03*, in *Danno e resp.*, 2003, 12, p. 1157. Un ulteriore carattere che denota la scarsa qualità del testo normativo in oggetto è messa in luce dall'a., il quale osserva che "è quantomeno singolare che, nel rubricare le norme, il legislatore adotti una doppia dizione, in italiano ed in inglese, accostando ai termini [semplice trasporto, memorizzazione temporanea, memorizzazione ...] rispettivamente quelli di *mere conduit*, *caching* e *hosting*: una aggettiva che, francamente, non si comprende, attesa la sua inutilità e la sua irrilevanza sul piano giuridico" (p. 1159).

via elettronica e a richiesta individuale di un destinatario di servizi".

- Prestatore di servizi della Società dell'informazione: "la persona fisica o giuridica che presta un servizio della società dell'informazione" (ossia il provider).
- Destinatario del servizio: il soggetto che, a scopi professionali e non, utilizza un servizio della società dell'informazione, in particolare per ricercare o rendere accessibili informazioni.
- Consumatore: qualsiasi persona fisica che agisca con finalità non riferibili all'attività commerciale, imprenditoriale o professionale eventualmente svolta.

Il prestatore, in aggiunta agli obblighi informativi previsti per specifici beni e servizi, deve rendere facilmente accessibili, in modo diretto e permanente, ai destinatari del servizio e alle Autorità competenti talune informazioni generali obbligatorie, fra cui:

- Nome, denominazione o ragione sociale;
- Domicilio o sede legale;
- Estremi di contatto;
- Numero di partita IVA o equivalente;
- Prezzi o tariffe dei servizi forniti, oltre a imposte e spese di consegna.

Non è questa la sede per una disamina delle altre disposizioni del d.lgs. 70/2003; basti qui ricordare che vengono regolamentate anche le comunicazioni commerciali e i contratti on line; vengono inoltre previsti codici di condotta e la possibilità di accedere a procedure di composizione delle controversie (anche per via telematica, c.d. *on line dispute resolutions*).

6.2.2 IL D.LGS. 70/2003: LA RESPONSABILITÀ DEL PROVIDER

Nel sistema delineato dal d.lgs. 70/03 si distinguono tre tipologie principali:

- 1) **responsabilità nell'attività di semplice trasporto** (*mere conduit*, art. 14): si prevede l'esonero da responsabilità sia per il prestatore di un servizio consistente nella trasmissione, su una rete di comunicazione, di informazioni per conto degli utenti (*mere conduit*) sia per un *access provider*, purché essi:
 - a. non diano origine alla trasmissione, e
 - b. non ne selezionino il destinatario, e
 - c. non selezionino né modifichino le informazioni trasmesse²⁵.

Le predette condizioni devono sussistere cumulativamente: dunque il provider non deve effettuare azioni ulteriori a quelle connaturate alla tipologia del servizio. In tali ipotesi, quindi, il prestatore deve essere assolutamente neutrale, svolgendo un'attività di ordine meramente tecnico, automatico e passivo (difatti non conosce né controlla le informazioni trasmesse o memorizzate)²⁶ e ricoprendo pertanto un ruolo simile a quello dell'operatore telefonico²⁷. Esso deve agire su ordine dell'autorità giudiziaria o amministrativa per impedire o terminare attività illecite.

- 2) **Responsabilità nell'attività di memorizzazione temporanea** (*caching*, art. 15): si esonera da responsabilità il prestatore di un servizio di *caching*, ossia della memorizzazione sui propri elaboratori di determinate informazioni reperite *on line*,

²⁵ "Tale previsione pare, invero, tradire una disapplicazione del principio di neutralità tecnologica della norma, giacché nella prestazione di servizi internet, a differenza di quanto avviene nei servizi telefonici, il prestatore/provider assume un ruolo "tecnicamente" attivo nella gestione e nell'instradamento delle comunicazioni in transito, adottando politiche di gerarchizzazione dei contenuti anche attraverso indici automatici, ma senza avere la possibilità di incidere specificamente sui contenuti stessi" (A. Putignani, *Sul provider responsabilità differenziate*, in *Guida dir.*, 2003, 20, p. 48).

²⁶ In tal senso depone anche il già ricordato considerando n. 42 della dir. 2000/31/CE.

²⁷ M. Tesaro, *Schemi legali e opposte tendenze giurisprudenziali in tema di responsabilità civile dell'internet provider*, op. cit..

al fine di agevolare l'accesso ai destinatari del servizio, purché:

- a. non modifichi le informazioni, e
- b. si conformi alle condizioni di accesso alle informazioni ed alle norme di aggiornamento delle informazioni, e
- c. non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni, e
- d. agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che:
 - i. le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete, o
 - ii. che l'accesso alle informazioni è stato disabilitato, o
 - iii. che un organo giurisdizionale od un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione.

In altri termini, per esimersi da responsabilità, il prestatore non può essere coinvolto in alcun modo nell'informazione trasmessa, che non può modificare; inoltre, deve rimuovere prontamente le informazioni (o disabilitare l'accesso) appena a conoscenza della rimozione/disabilitazione delle informazioni (o della relativa richiesta dell'autorità giudiziaria o amministrativa); infine, deve agire su ordine dell'autorità giudiziaria o amministrativa per impedire o terminare attività illecite. Pertanto, la condotta che deve essere intrattenuta dal provider, affinché lo stesso possa esimersi da responsabilità, è sia omissiva (lettere a, b, c) che commissiva (lettera d).

3) **Responsabilità nell'attività di memorizzazione delle informazioni** (*hosting*, art. 16): si esonera da responsabilità l'*hosting provider* per le informazioni memorizzate a richiesta di un destinatario del servizio, purché:

- a. non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita, e
 - i. per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione; e
- b. non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

Inoltre, l'autorità giudiziaria o quella amministrativa competente può esigere, anche in via d'urgenza, che il prestatore impedisca o ponga fine alle violazioni commesse. Rispetto alle prime due tipologie di prestatori suindicate, l'*hosting provider* si caratterizza per la natura stessa del servizio, tendenzialmente più "stabile", nel senso che la memorizzazione dei dati informatici, svolta su richiesta del destinatario del servizio, non ha carattere temporaneo (come nel caso del semplice trasporto e del caching) – fermo restando che i medesimi dati possono comunque tendenzialmente essere cancellati da chi ne ha il controllo.

Infine, bisogna prendere in considerazione l'art. 17 (**Assenza dell'obbligo generale di sorveglianza**). Esso dispone che il provider (nelle ipotesi di prestazione di servizi di semplice trasporto, caching, hosting):

- a) non è assoggettato:
 - i. né ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza,
 - ii. né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite;

- b) deve comunque:
- i. informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione;
 - ii. fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite;
- c) è civilmente responsabile del contenuto dei servizi se:
- i. richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l'accesso a detto contenuto, o
 - ii. se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non ha provveduto ad informarne l'autorità competente.

Pertanto, non sussiste un obbligo di sorveglianza e il prestatore non deve ricercare fatti o circostanze indicanti attività illecite. Su di esso grava, tuttavia, l'obbligo di informare l'autorità giudiziaria o amministrativa qualora venga a conoscenza di attività o informazioni illecite di un proprio destinatario del servizio, nonché quello di fornire alle autorità competenti (su richiesta) le informazioni idonee a identificare il destinatario del servizio. Inoltre, esso deve agire su ordine dell'autorità giudiziaria o amministrativa per impedire o terminare attività illecite, o informare l'autorità competente se a conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso. Secondo la Corte di Appello di Milano (in un caso relativo alla violazione di diritti d'autore), "la responsabilità a posteriori dell'hosting provider sorge per non avere ottemperato a una richiesta (diffida) di rimozione dei contenuti illeciti proveniente dalla parte che assume essere titolare dei diritti, ovvero per non avere ottemperato a un ordine d'autorità (injunction), sia essa giurisdizionale o amministrativa, cui si sia rivolto il titolare del diritto per ottenere il medesimo effetto"²⁸.

6.3 IL PROVIDER. ALCUNI CASI GIURISPRUDENZIALI

La giurisprudenza si è occupata, in più occasioni, della responsabilità di diverse tipologie di prestatori di servizi: da motori di ricerca a siti di aste on line ed e-commerce. Di seguito, vengono presentati alcuni casi significativi.

CACHING

Caching e Google (Trib. Firenze, ord., 25/05/2012)

Caso: pretesa violazione di diritti di marchio, campagne diffamatorie e offensive, utilizzo di foto e ritratti non pubblici del ricorrente, webmaster ignoto.

Google Inc. viene considerata un caching provider poiché ha la gestione diretta dell'omonimo motore di ricerca, con cui procede all'indicizzazione dei siti ed alla formazione di copie cache dei loro contenuti, con memorizzazione temporanea delle informazioni.

Per ciò che riguarda:

- l'accusa di utilizzo dei marchi, il Tribunale ha affermato che, nel caso di specie, non si ravvisavano né l'utilizzo commerciale né le ipotesi di contraffazione, usurpazione o sfruttamento abusivo;

²⁸ App. Milano, 7 gennaio 2015.

- la conoscenza effettiva della pretesa illiceità dei contenuti del sito *de quo*, il Giudice di merito ha sostenuto che essa non [può] essere desunta [...] dal contenuto delle diffide di parte, trattandosi di prospettazioni unilaterali. In tal senso, sarebbe necessario che un "organo competente abbia dichiarato che i dati sono illeciti, oppure abbia ordinato la rimozione o la disabilitazione dell'accesso agli stessi, ovvero che sia stata dichiarata l'esistenza di un danno" e che l'ISP stesso sia a conoscenza di una tale decisione dell'autorità competente (ma come si può notare, anche se ciò è relativo a una fattispecie diversa (hosting), la Corte di Appello di Milano ha considerato in modo diverso gli effetti derivanti dall'invio della diffida da parte del danneggiato).

In riferimento alla decisione, il Tribunale adito ha affermato che "risultando pubblicati sul sito in questione, atti giudiziari, quanto in essi affermato non può essere in questa sede confutato", per cui non si può impartire alcun ordine alla società resistente [Google], posto che quanto contenuto nel sito *de quo* appare espressione di un diritto di critica che si fonda proprio sul tenore di tali provvedimenti giurisdizionali, emessi nei confronti del ricorrente.

Il procedimento si è concluso con la compensazione delle spese di lite, con ordinanza del 25 maggio 2013 a seguito di scioglimento di riserva del 27 marzo 2013.

HOSTING

Hosting ed eBay (Trib. Milano, ord. 3/10/2013, RG 44529/13)

Caso: banchiere italo-svizzero, doglianza di pubblicità online di un libro con toni aggressivi.

Nel caso di specie, si è avuto un primo provvedimento d'urgenza che ha disposto la rimozione di messaggi da diversi siti di e-commerce.

Successivamente, un nuovo ricorso al Tribunale è stato rigettato, poiché veniva richiesto a eBay di ricercare attivamente altre violazioni dei diritti del ricorrente. Si è infatti rilevato che la richiesta verso eBay pare confondere i profili di tutela che si può utilmente vantare nei confronti dei singoli inserzionisti di eBay rispetto a quelli che può eventualmente invocare nei confronti dell'hosting provider che ha "ospitato" le inserzioni ritenute illecite: gli illeciti commessi dai destinatari del servizio fornito da eBay non possono essere confusi con il prestatore del servizio (hosting provider). Pertanto, non possono sostenersi:

- un controllo preventivo dell'hosting provider sugli interventi (inserzioni) degli utenti;
- un obbligo generale di sorveglianza;
- un obbligo per eBay, una volta venuta a conoscenza che alcuni suoi utenti - esattamente individuati - hanno inserito informazioni non lecite (poi rimosse), di verificare se (eventualmente) altri suoi utenti in via del tutto autonoma abbiano pubblicato inserzioni di analogo contenuto illecito.

PROVIDER, NEUTRALITÀ E DIFFAMAZIONE

Caso 1: Google Suggest/Autocomplete e diffamazione (Trib. Pinerolo, ord. 25/03/2013)

Nel caso di specie, è stata richiesta la rimozione dell'accostamento "nome + arrestato o indagato" (poi solo "indagato") dai risultati di ricerca di Google Suggest. A detta della società statunitense, il servizio è oggettivo e neutrale poiché non modifica l'informazione trasmessa o ospitata. Le parole generate automaticamente nella stringa di ricerca, infatti, sono le parole statisticamente più cercate su Google.

Si è dunque affermato che "arrestato" o "indagato" non sono termini offensivi, che una query è una domanda e non un'affermazione, e che gli utenti meno informati sanno che i fatti non sono veri all'esito della ricerca.

Pertanto, a Google non è stata addebitata alcuna responsabilità per la mera diffusione di

una notizia (non lesiva), mentre si è affermata la sua neutralità nello svolgimento della propria attività di ISP, accostandola, con valutazione del fatto concreto, alla figura del giornalista.

Il procedimento si è concluso con il rigetto del ricorso e la condanna alle spese del ricorrente.

Caso 2: Google Suggest/Autocomplete/Ricerche correlate e diffamazione (Trib. Milano, ord. 23/05/2013).

Nel caso di specie, è stata richiesta la rimozione dell'accostamento "nome associazione + setta o truffa o plagio".

Secondo Google, il servizio che rende sarebbe oggettivo e neutrale poiché le parole generate automaticamente nella stringa di ricerca, infatti, sarebbero le parole statisticamente più cercate su Google.

Come si è giustamente rilevato nell'ordinanza del Tribunale di Milano, però, non vi è dubbio che tali "utilità" siano il frutto del meccanismo di ricerca ideato da Google che, pur veicolando dati presenti sulle pagine web e immessi da terzi, propone all'utente ricerche aggregando parole secondo una "logica", certamente automatica, ma comunque ideata in origine da Google, per finalità differenti e non essenziali al funzionamento del motore di ricerca, riconducibili alle scelte tecniche e imprenditoriali della stessa Google.

Ne consegue che con particolare riguardo alle funzioni "Autocomplete" e "Ricerche correlate" Google non può ritenersi un ISP cd. passivo, ma al contrario l'azienda svolge un ruolo attivo nell'aggregazione dei dati, totalmente riferibile alla sua iniziativa, sia pure secondo un criterio automatico e predeterminato che l'azienda si è data a monte dell'erogazione del servizio.

In altri termini, dunque, automatismo del software non equivale a neutralità.

CASO WRITER'S DREAM

Tribunale di Varese (sent. 8/4/2013) (pend. app.)

Il sito "Writer's dream" fornisce consigli utili agli autori emergenti per orientarsi nel mondo dell'editoria; mediante il sito è stata intrapresa la campagna "NO EAP", contro l'editoria a pagamento, con tanto di pubblicazione di una lista degli editori EAP.

Nel caso di specie, è stata presentata una denuncia/querela contro l'amministratrice del sito in seguito alla pubblicazione di alcune frasi asseritamente lesive dell'onorabilità e della dignità delle case editrici citate.

Il Tribunale di Varese ha acclarato l'utilizzo di epiteti e termini offensivi (truffatori, signori della truffa, cosche mafiose, strozzini) ma anche non giuridicamente rilevanti ("pessima qualità" di talune produzioni editoriali) e ha affermato che la disponibilità dell'amministrazione del sito rende l'imputata responsabile di tutti i contenuti di esso accessibili dalla rete, sia quelli inseriti da Lei stessa, sia quelli inseriti da utenti; è indifferente sotto questo profilo sia l'esistenza di una forma di filtro (poiché in tal caso i contenuti lesivo dell'altrui onorabilità devono ritenersi specificamente approvato dal *dominus*) sia l'inesistenza di filtri (poiché in tal caso i contenuti lesivi dell'altrui onorabilità devono ritenersi genericamente e incondizionatamente approvati dal *dominus*). Il regolamento del sito, poi, è inidoneo a esimersi da responsabilità.