IL DIRITTO DELL'INFORMAZIONE E DELL'INFORMATICA
Anno XXVI Fasc. 3 - 2010

Alessandro Mantelero

LA RESPONSABILITÀ *ON-LINE*: IL CONTROLLO NELLA PROSPETTIVA DELL'IMPRESA

Estratto

MVLTA PAVCIS AG

Milano • Giuffrè Editore

ALESSANDRO MANTELERO

LA RESPONSABILITÀ *ON-LINE*: IL CONTROLLO NELLA PROSPETTIVA DELL'IMPRESA

SOMMARIO: 1. Premessa: i termini del problema. — 2. L'attuale stato dell'arte: i controlli esigibili. — 3. (*Segue*): il quadro normativo. — 4. Le prospettive future.

1. Premessa: i termini del problema.

Per cogliere la portata dei fenomeni digitali e fornire adeguate risposte di politica del diritto occorre far proprio il recente monito rivolto da Lerry Lessig a quanti si occupano di diritto dell'informazione e dell'informatica, con cui sollecitava a guardare avanti, al futuro, con gli occhi dei nostri figli[1]. In tal ottica il giurista deve dunque sì trarre ispirazione dai principi della sua scienza e dalle norme e regole operative, ma nel contempo volgere il suo sguardo alla realtà che ha di fronte e (possibilmente) a quella che verrà, in estrema sintesi al dato tecnologico e sociale.

Questo è il presupposto, senza il quale il ragionamento giuridico diviene incapace di calarsi nel concreto, di attuazione ed in tal modo di effettiva incidenza sulla realtà sociale ed imprenditoriale.

In questo senso il dibattito innescato dalla recente sentenza sul « caso Google »[2], che tanto scalpore ha destato e tanta risonanza ha avuto, ed ancor più le motivazioni di quella sul caso R.T.I. c. YouTube[3], di minor rilievo mediatico ma ben più dirompenti sotto il profilo organizzativo d'impresa, sembrano per certi aspetti

* Relazione al convegno « *Il futuro della responsabilità sulla rete. Quali regole dopo la sentenza Google/ViviDown* », organizzato dalla Università di Roma Tre e dalla Fondazione Calamandrei e svoltosi il 21 maggio 2010. La sentenza Trib. Milano 12 aprile 2010 è pubblicata *infra* p. 474.

[1] Cfr. L. Lessig, *L'ideale di trasparenza che viene dalla Rete. E la sua realtà*, intervento al convegno « Internet è libertà. Perché dobbiamo difendere la rete », tenutosi l'11 marzo 2010 presso la Sala della Regina della Camera dei Deputati, visionabile in *streaming* su *http://www.radioradicale.it/scheda/299126* (tutti i siti web riportati nel presente contributo sono stati consultati fra il 10 maggio 2010 ed il 20 maggio 2010).

[2] Cfr. Trib. Milano, 12 aprile 2010.

[3] Cfr. ordinanza Trib. Roma, 16 dicembre 2009, in *http://www.tgcom.mediaset.it/res/doc/sentenzatribunale.pdf*.

riportarci indietro nel tempo, alle discussioni iniziali su quello che veniva chiamato « cyberdiritto » e che manifestava un senso di estraneità per quella che allora pareva la nuova frontiera[4]. Così oggi dinnanzi alla dilagante novità del web sociale si può rischiare di essere smarriti, cedendo alla tentazione di rifugiarsi nel porto quieto dell'« ingegneria normativa »[5], senza mettere in luce come le stesse norme siano in questa materia sempre, e da sempre, superate dalla realtà tecnologica. Si corre nuovamente il rischio di un ragionamento giuridico avulso dal reale e, come tale, incapace di dialogare con le imprese e, soprattutto, di dare risposte efficienti ai problemi che ci sono di fronte.

Facile, in presenza dell'evidente violazione dei diritti della persona[6] e del consolidamento della pirateria digitale, assumere che occorrono maggiori controlli e che andrebbe rivista la neutralità dei fornitori dei servizi dell'informazione consistenti nell'attività di *hosting*[7], ma il ragionamento si infrange poi contro il dato informatico: su Google/YouTube[8] vengono caricate ventiquattro ore di contenuti multimediali al minuto[9]... chi può controllare una tale mole di dati?

Se si auspicasse un controllo efficace (ammesso che sia davvero realizzabile) questo comporterebbe la cessazione del servizio o, quantomeno, il suo snaturamento in termine di tempi di fruizione, ma davvero un web senza YouTube e magari (allargando il discorso) senza Facebook, Twitter e tanti altri servizi a connotazione « sociale » sarebbe una realtà migliore?

Già solamente questi semplici interrogativi inducono a ritenere che le soluzioni ai problemi esistenti in materia vanno ponderate

---

[4] Per maggiori indicazioni a riguardo e per i riferimenti bibliografici, in ragione dell'economia del presente contributo, sia consentito rinviare ad A. Mantelero, *Attività di impresa in Internet e tutela della persona*, Padova, 2004, 5 ss.

[5] Cfr. il commento conclusivo espresso in Trib. Milano, 12 aprile 2010, citata *supra*: « in attesa di una buona legge che costruisca una ipotesi di responsabilità penale per il mondo dei siti Web (magari colposa, ed allora sì per omesso controllo), non resta che assolvere gli imputati ».

[6] La vicenda su cui si è pronunciato il Trib. Milano, 12 aprile 2010, citata *supra*, riguardava la distribuzione *on-line* mediante la piattaforma UGC (*User-generated content*) video di Google (*http://video.google.it*) di un filmato realizzato da un utente in cui un disabile veniva pesantemente offeso e vessato da un gruppo di ragazzi coetanei; nei confronti dei minori autori degli illeciti e del video nel 2007 è stato celebrato un processo presso il Tribunale per i Minorenni di Torino, conclusosi con la messa alla prova degli stessi.

[7] Cfr. art. 16, comma 1, del D.Lgs. 70/2003, ai sensi del quale tale attività consiste « nella memorizzazione di informazioni fornite da un destinatario del servizio »; per una definizione della nozione di servizi dell'informazione cfr. invece art. 1, punto 2, della direttiva 98/34/CE e, con riferimento alla normativa nazionale, art. 2, comma 1, lett. *a*), del D.Lgs. 70/2003.

[8] Google ha acquisito YouTube sul finire del 2006, successivamente non è stato più possibile per gli utenti caricare video sulla piattaforma UGC di Google video, cfr. *http://video.google.it/support/bin/answer.py?hl=it&answer=138275*, che è rimasta attiva con riferimento ai video già presenti, suggerendo comunque agli utenti di spostare i contenuti esistenti (oltre che inserire i nuovi) su YouTube o Picasa.

[9] Il dato è riportato da C. Tamburrino, *YouTube, due miliardi di questi video*, 17 maggio 2010, in *http://punto-informatico.it*.

anche alla luce della loro praticabilità tecnologica e del rapporto costi/benefici. Questo non vuole dire però abdicare ad una tutela forte della persona ed optare per una funzionalizzazione della stessa agli interessi dell'impresa che, anche nel migliore dei casi, è animata da fini di profitto e non certo filantropici. Certamente la persona deve essere preminente, come la nostra carta costituzionale ed in generale tutte le dichiarazioni internazionali ci ricordano, ove ce ne fosse bisogno; tuttavia, proprio perché tutela vi sia, occorre prospettare soluzioni realistiche e funzionali, che tengano in adeguato conto le possibilità ed i limiti della realtà con cui ci si deve raffrontare e siano nel contempo attente all'evoluzione della sensibilità sociale.

Guardando con questi occhi il problema del controllo sui contenuti da parte del fornitore del servizio occorre da subito tenere a mente che per l'impresa il controllo è un costo e che dalla sostenibilità dello stesso deriva sia la propensione a porlo in essere, sia, qualora l'ordinamento giuridico imponga un tale comportamento, la decisione di permanere nel mercato che preveda il monitoraggio come condizione necessaria. Così se, come alcuni vorrebbero, si costringessero i *provider* a fare gli « sceriffi della rete », delegandoli ad analizzare il traffico dati alla ricerca di illeciti (specie in chiave anti-pirateria), prima ancora degli utenti sarebbero forse gli stessi fornitori a protestare ed a meditare se orientare verso altri indirizzi il loro *business*, con ovvie ricadute dirompenti sull'accessibilità e sull'esistenza stessa dell'attuale modello di rete internet da noi conosciuto.

A ben vedere il controllo potrebbe rivelarsi un bene per l'impresa, non solo in termini di contenimento del contenzioso potenziale, ma anche di posizionamento sul mercato, quale soggetto affidabile e corretto agli occhi dei consumatori, degli investitori e dei *partner* commerciali. Tuttavia, già lo abbiamo visto in materia di tutela dei dati personali, a gran parte delle imprese queste ricadute positive sfuggono[10].

Alla maggior sensibilità per i costi rispetto a quella per i benefici, si aggiunge poi, in campo informatico, l'atteggiamento inge-

[10] Così un altro colosso del web come Facebook ha nel tempo modificato le proprie politiche in tema di *privacy* in senso addirittura peggiorativo nella sostanza; cfr. G. Pontico, *Facebook, il Web sono io*, 22 aprile 2010, in *http://punto-informatico.it/2864843/PI/News/facebook-web-sono-io.aspx* e K. Opsahl, *Facebook's Eroding Privacy Policy: A Timeline*, 8 aprile 2010, in *http://www.eff.org/deeplinks/2010/04/facebook-timeline*. A riguardo è stata anche intrapresa una *class action* presso la District Court for the Northern District della California e recentemente, il 27 aprile 2010, alcuni senatori statunitensi hanno inviato una lettera critica al fondatore di Facebook, il cui testo è pubblicato su *www.politico.com*. Cfr. da ultimo sulla vicenda Articolo 29-Gruppo di lavoro per la tutela dei dati personali, *European data protection group faults Facebook for privacy setting change*, comunicato stampa, Bruxelles, 12 maggio 2010, in *http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_12_05_10_en.pdf*.

gneristico che mira alla soluzione tecnica funzionale e trascura sovente le implicazioni giuridiche di quest'ultima, salvo poi correre ai ripari.

Luci ed ombre dunque in un'ottica di impresa sono frammiste sotto la nozione di controllo. Due i termini da considerare per ponderare le politiche di controllo e per stimolarle: il rapporto costi/benefici ed i limiti tecnologici. Sullo sfondo, inutile ribadirlo, il criterio ordinatore della preminenza della tutela della persona.

2. L'attuale stato dell'arte: i controlli esigibili.

Nuovamente ripensando alla decisione sul caso Google, emerge la peculiarità della posizione dell'impresa che funge da vettore di contenuti prodotti da terzi e destinati alla divulgazione *online*: essa non è diretta autrice dell'illecito, ma è agevolmente individuabile, ha un patrimonio aggredibile e (almeno in alcuni casi e quanto ai profili di diritto civile) potrebbe avere una propensione alla transazione onde evitare un danno di immagine[11]. Tutti elementi che possono ragionevolmente indurre le corti in interpretazioni volte a ravvisare profili di illiceità nell'agire dell'intermediario, in un'ottica (più o meno consapevole) di allocazione ottimale della responsabilità.

Tre sono però i profili che ostano ad una simile opzione: *in primis* il fondamento giuridico di un'operazione di politica del diritto di tal fatta, secondariamente la ragionevolezza della pretesa di controllo sui contenuti che ne deriverebbe e da ultimo la sostenibilità della stessa.

Quanto al primo aspetto, va ricordato che ci troviamo di fronte ad un intermediario e non ad un fornitore di contenuti propri, o comunque condivisi[12], e ciò pare fuori di dubbio, basti guardare alla distanza presente fra un servizio quale Google ed un *content provider*[13]. Che poi l'intermediario persegua fini di profitto, poco

[11] Si vedano in tal senso le supposizioni circa l'esistenza di una soluzione transattiva a fondamento della decisione del ritiro della querela, e della mancata costituzione di parte civile, ad opera dei genitori del disabile leso proprio nel processo penale, v. *supra* nota 6, cui si collega la vicenda Google, cfr. a riguardo *Disabile molestato finì sul web: il padre ritira la querela a Google*, in *http://quotidianonet.ilsole24ore.com*.

[12] Tale diversa lettura pare invece adombrata dal ragionamento della pubblica accusa circa il ruolo assunto da Google, cfr. Trib. Milano, 12 aprile 2010, citata *supra*, ove si legge: « IPM appaiono, nelle loro memorie scritte, molto più ''tranchantes'' di questo giudice monocratico, ritenendo che la responsabilità derivante dal trattamento dei dati sensibili possa essere addebitata all'lSP solo e soltanto ove lo stesso non svolga una mera intermediazione tecnica, ma compia un ''qualcosa di più'' rispetto all'host provider, *assicurando mediante un servizio da esse sfruttato, la memorizzazione e la diffusione dei contenuti memorizzati* e diventando in tal modo un hoster attivo, responsabile dei contenuti medesimi » (corsivo del testo originale).

[13] Si pensi a siti quali: *www.repubblica.it*, *www.leonardo.it*, *www.libero.it*.

rileva, anzi è ovvio. Nello specifico non pare possibile semplicisticamente estrapolare e mutuare singoli elementi costitutivi degli orientamenti maturati nella giurisprudenza statunitense in materia di *copyright*, ove la finalità di profitto è stata considerata un indice di concorso nell'illecito. Al di là dei limiti posti ad una simile operazione già dalle peculiarità dei differenti sistemi giuridici, basti osservare come nei casi considerati non rilevasse il fine di profitto in termini generici, bensì in quanto strettamente correlato all'illecito commesso dai terzi e ad esso conseguente[14], nonché come la responsabilità non fosse incentrata unicamente sulla presenza di tale scopo e gli stessi presupposti fattuali fossero differenti, trattandosi di ipotesi in cui la natura illecita dei contenuti era la regola e non l'eccezione[15].

Stanti i limiti strutturali al controllo dell'attività dei fruitori del servizio, l'assenza di una specifica finalità dell'impresa di arrecare un dato danno e l'estraneità rispetto all'agire di chi ha commesso l'illecito, pare dunque difficile estendere una qualche teoria che legittimi in tal contesto la responsabilità dell'impresa in ragione del profitto conseguito. Per giunta, anticipando il richiamo all'art. 16 del D.Lgs. 70/2003 che limita in maniera assai significativa la responsabilità degli intermediari[16], va osservato come nep-

[14] Ragionando invece solo in base alla presenza di un profitto anche indirettamente correlato si potrebbe giungere all'assurdo di ritenere anche il gestore telefonico responsabile per i danni da molestie, essendo noto che il telefono può essere (ed è) anche impiegato a tali fini ed essendovi una relazione (ancorché circoscritta) fra tale uso ed il profitto del gestore.

[15] Cfr. *Metro-Goldwyn-Mayer v. Grokster*, 545 US 913 (2005), ove si ravvisa il concorso del distributore di un *software* per la creazione di reti *peer-to-peer* (*contributory copyright infringement*) nell'illecito compiuto dagli autori dello scambio di materiale coperto da *copyright*. Nello specifico, benché il *software* fosse astrattamente idoneo per lo scambio di contenuti di qualsiasi genere, anche legali, è stata esclusa l'applicabilità della *doctrine Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984), in traduzione italiana in *Foro it.*, 1984, IV, 351 ss., secondo cui « the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial non-infringing uses ». A tal fine i giudici della Suprema Corte hanno dato una lettura restrittiva di tale principio, attribuendo rilievo determinante alla sussistenza di un « intent to promote infringement » provato, fra l'altro, proprio sulla base del fatto che « respondents make money by selling advertising space, then by directing ads to the screens of computers employing their software », cui si aggiungevano però ulteriori elementi quali la conoscenza dell'illecito commesso dai terzi a mezzo del servizio ed addirittura la volontà di sollecitare un simile comportamento e di inserirsi in tale « mercato ». Cfr. recentemente nello stesso senso *Arista Records LLC et al v. Lime Group et al*, U.S. District Court, Southern District of New York, No. 06-05936, dell'11 maggio 2010, pubblicata in *http://www.wired.com/images_blogs/threatlevel/2010/05/limewireruling.pdf*, *in cui viene espressamente richiamato il precedente del caso Grokster*.

[16] Sul fatto che la responsabilità dell'intermediario, ancorché fortemente limitata, non venga comunque meno in relazione ad alcune ipotesi residuali definite dalla norma stessa, cfr. in dottrina V. Zeno-Zencovich, *Profili attivi e passivi della responsabilità dell'utente in internet*, in *La tutela del navigatore in internet*, a cura di A. Palazzo-U. Ruffolo, Milano, 2002, 139 s. e S. Sica, *Le responsabilità civili*, in *Commercio elettronico e servizi della società dell'informazione*, a cura di E. Tosi, Milano, 2003, 301.

pure tale limitazione sia subordinata alla sussistenza o meno di un profitto o da quest'ultima condizionata[17].

Passando dal piano giuridico a quello organizzativo inerente la gestione d'impresa, occorre poi interrogarsi sulla ragionevolezza della pretesa di controllo e, conseguentemente, sull'esigibilità della stessa[18]. Va in proposito considerato come le possibilità di monitoraggio trovino forti resistenze tanto nel volume dei dati trattati dai gestori delle piattaforme UGC, quanto nella riconoscibilità dei contenuti illeciti. Con riguardo al primo aspetto e prendendo ad esempio proprio Google/YouTube, come si è detto mediante tale servizio vengono caricate ventiquattro ore di filmati al minuto, da qui, ipotizzando la visione da parte di un operatore in maniera integrale di tutti i contenuti, la necessità di dotarsi di uno *staff* di controllori di circa cinquemila unità. Pur immaginando che si possa pretendere che un'impresa del settore digitale debba impiegare l'equivalente della popolazione di un piccolo centro urbano per proteggere i propri utenti (cosa dovrebbe allora chiedersi agli industriali dei settori chimici o farmaceutici!), questo comunque non basterebbe. Guardando infatti alla riconoscibilità degli illeciti, occorrerebbe prevedere il ricorso a controllori in grado di conoscere le centinaia di idiomi presenti in rete, non solo, oltre alle barriere linguistiche occorrerebbe superare anche quelle culturali, in quanto un dato comportamento può essere neutro per un certo gruppo sociale, ma nel contempo offensivo per un altro. Da ultimo va osservato che non sempre, anche ammettendo di possedere tutte le conoscenze di cui si è detto, la natura dell'offesa, ad esempio, è esplicita, così come può non essere palese la differenza fra un comportamento reale di derisione e la parodia dello stesso.

La ragionevolezza del controllo esigibile induce infine a riflettere, tenuto conto della natura imprenditoriale dei soggetti, sulla sostenibilità economica delle misure; a riguardo è di tutta evidenza come l'incidenza dei costi relativi al monitoraggio sia assai notevole, tanto in termini di ore lavorative quanto di strumenti e risorse occorrenti, a fronte di profitti derivanti dagli introiti pubblicitari connessi alla visualizzazione dei filmati non sufficienti a giustificare un tal modello di *business* che dia tanta rilevanza al controllo[19].

---

[17] Sulla peculiare posizione assunta in tema di responsabilità d'impresa dalla direttiva 2000/31/CE, di cui l'art. 16 del D.Lgs. 70/2003 è attuazione, cfr. V. Zeno-Zencovich, *Profili attivi e passivi della responsabilità dell'utente in internet*, citata *supra*, 138 ss.

[18] Nel senso dell'inesigibilità di un controllo preventivo su tutti i materiali caricati *on-line* dagli utenti si è espresso anche Trib. Milano, 12 aprile 2010, citata *supra*.

[19] Vero è che, rimanendo sul caso Google, la quasi totalità dei proventi generati dalle diverse attività riconducibili al noto motore di ricerca derivano dalla pubblicità erogata attraverso i propri siti, tuttavia non va dimenticato che il settore dei video costituisce solo una piccola parte del materiale indicizzato e reso accessibile dagli utenti e che, nel contempo, è assai significativo l'impatto dei servizi pubblicitari correlati alla funzione principale di motore di ricerca generico.

È alla luce di queste composite risultanze che vanno quindi valutate le disposizioni normative applicabili.

3. (*Segue*): il quadro normativo.

Occorre in primo luogo interrogarsi sull'applicabilità del D.Lgs. 196/2003 ad un servizio di pubblicazione di contenuti fornito dall'utente al fine di consentirne la visibilità sul web. In proposito, laddove detti contenuti rappresentino immagini di persone o comunque contengano dati personali è indubbio che la loro elaborazione configuri una forma di trattamento dati, come costituisce trattamento l'archiviazione dei *file* in relazione ad un determinato nominativo dell'utente registrato sulla piattaforma[20].

V'è dunque un duplice trattamento: un primo (in ordine temporale) attinente i dati forniti dall'utente per accedere al servizio ed un secondo inerente i materiali caricati. Quanto ai dati dell'utente, pare potersi applicare l'art. 24, comma 1, lett. *b*), del D.Lgs. 196/2003, rendendo superflua l'acquisizione del consenso, poiché necessari all'esecuzione del contratto. Con riguardo invece ai materiali resi di pubblico accesso, il trattamento posto in essere dal fornitore del servizio è appunto quello della pubblicazione, per altro lasciando nella disponibilità dell'utente la possibilità di rimozione dei contenuti, appare dunque applicabile il disposto del successivo art. 136, comma 1, lett. *c*), riguardante il trattamento « temporaneo finalizzato esclusivamente alla pubblicazione o diffusione occasionale di... manifestazioni del pensiero anche nell'espressione artistica ». Che la finalità degli utenti dei servizi in esame sia appunto quella di manifestare il proprio pensiero a terzi è infatti fuori di dubbio, costituendo la condivisione la ragione stessa di tali servizi[21]. Né il fatto che il gestore della piatta-

[20] Su YouTube, ad esempio, i video vengono pubblicati con l'indicazione dell'*uploader*, unitamente alle informazioni che questi ha inteso rivelare su di sé; anche nell'ipotesi dell'uso di uno pseudonimo, si potrebbe dunque essere in presenza di dati riferiti ad un soggetto identificabile.

[21] Sull'interpretazione della norma nel senso di una nozione ampia di « manifestazione di pensiero », supportata ad oggi anche dalla crisi della concezione tradizionale di giornalismo, cfr. G. Votano, *L'attività giornalistica*, in F. Cardarelli-S. Sica-V. Zeno-Zencovich, *Il codice dei dati personali*, Milano, 2004, 510 ss. Con riguardo agli utenti potrebbe anche essere richiamata la più generale norma derogatoria di cui all'art. 5, comma 3, del D.Lgs. 196/2003, che esclude dall'ambito operativo della legge il « trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali », tuttavia quest'ultima è completata dall'inciso secondo cui il trattamento è comunque soggetto al D.Lgs. 196/2003 « se i dati sono destinati ad una comunicazione sistematica o alla diffusione », cosa che si verifica in relazione all'attività posta in essere da moltissimi utenti delle piattaforme UGC. L'art. 3, paragrafo 2, della direttiva 95/46/CE, nel definirne il campo di applicazione, esclude invece i trattamenti « effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico » senz'altro aggiungere, cfr. anche il 12° considerando della direttiva richiamata, ed a tale disposizione hanno fatto riferimento alcuni documenti ufficiali

forma introduca forme pubblicitarie nel sito pare confliggere con l'idea di trattamento « finalizzato esclusivamente » alla pubblicazione, come d'altra parte accade per i *media* tradizionali.

Dall'applicabilità dell'art. 136 del D.Lgs. 196/2003[22] derivano specifiche conseguenze in termini di semplificazione degli adempimenti: non occorre l'autorizzazione del Garante al trattamento dei dati sensibili[23], non si applicano le disposizioni sui flussi transfrontalieri dei dati[24] e, soprattutto, non occorre il consenso dell'interessato (in questo caso dei soggetti cui le immagini o, più in generale, i dati si riferiscono)[25]. Poiché tuttavia, come anche esplicitato dall'art. 137, comma 3, la tutela dei dati personali non esaurisce l'intero ambito di protezione riconosciuto dall'ordinamento alla persona, permanendo diversi ed ulteriori profili (l'immagine, il riserbo, la dignità, l'identità, ecc.), con riguardo a tali aspetti il gestore della piattaforma potrebbe richiamare la

per escludere l'applicabilità delle norme comunitarie in materia di trattamento dati alle informazioni immesse dagli utenti nei *social network*, cfr. ARTICOLO 29-GRUPPO DI LAVORO PER LA TUTELA DEI DATI PERSONALI, *Parere 5/2009 sui social network on-line*, Bruxelles, 12 giugno 2009, 14, in *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_it.pdf*, esclusione da cui si è poi talora desunto anche un effetto « riflesso » sul trattamento effettuato dai fornitori dei servizi, cfr. ARTICOLO 29-GRUPPO DI LAVORO PER LA TUTELA DEI DATI PERSONALI, *The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, Bruxelles, 1° dicembre 2009, 18, in http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf, secondo cui « Directive 95/46/EC does not apply to the individual who uploads the data for 'purely personal' purposes or 'in the course of a household activity'. Arguably it does not apply either to the organization that provides the service, i.e. hosts and makes available the information uploaded by the individual (unless the service processes data for its own purposes) insofar as the service provider may not be deemed to be a controller ». Cfr. anche le osservazioni ancora valide espresse da V. FRANCESCHELLI, *sub* art. 3, in *La tutela dei dati personali. Commentario alla l. 675/1996*, a cura di E. Giannantonio-M. Losano-V. Zeno-Zencovich, Padova, 1997, 34 ss.

[22] Non sembra aver tenuto conto della norma Trib. Milano, 12 aprile 2010, citata *supra*, in cui vengono solamente richiamati gli « artt. 23 e 26 DL citato ».

[23] Cfr. art. 137, comma 1, lett. *a*), del D.Lgs. 196/2003; vedi anche la successiva lett. *b*).

[24] Cfr. art. 137, comma 1, lett. *c*), del D.Lgs. 196/2003.

[25] Cfr. art. 137, comma 2, del D.Lgs. 196/2003. Tale norma esclude la necessità per il gestore della piattaforma UGC di richiedere altresì il consenso relativamente alle immagini ed ai dati di terze persone diverse dall'utente e da quest'ultimo fatte oggetto di *upload*. Posto che la finalità degli utilizzatori di tale tipologia di piattaforma è anch'essa riconducibile allo scopo di manifestare il proprio pensiero se ne dovrebbe poi dedurre che pure quest'ultimi, anche ove non operi la deroga di cui all'art. 5, comma 3, del D.Lgs. 196/2003, non siano tenuti ad acquisire preventivamente il consenso dei terzi cui fanno riferimento i contenuti. Sempre con riferimento all'utente, poiché tuttavia l'art. 137, come testimoniato anche dall'ultimo comma dello stesso, si inquadra nell'ottica di permettere l'esercizio del diritto di cronaca e, più in generale, della libertà di espressione del pensiero, occorrerà guardare altresì agli orientamenti giurisprudenziali affermatisi in materia, che riconoscono come tale libertà venga ad essere limitata in ragione della tutela dei contrapposti interessi della persona inerenti l'immagine, il riserbo, la dignità e l'identità personali. In quest'ultimi casi il riferimento alla generica categoria delle « manifestazioni del pensiero » di cui all'art. 136 del D.Lgs. 196/2003, renderà sì superfluo il consenso al fine del trattamento, ma esso, senza i formalismi richiesti dalla normativa sui dati, potrà invece essere rilevante per escludere l'eventuale illiceità della condotta *ex* art. 2043 c.c.

nozione di consenso implicito, ritenendo che esso sussista in riferimento ai terzi effigiati, onde escludere ogni responsabilità per eventuali illeciti[26].

Unico obbligo cui è tenuto l'intermediario, ai sensi del D.Lgs. 196/2003, è dunque quello dell'informativa, che nel caso di servizi *on-line* dovrebbe essere fornita « in linea in modo agevole e interattivo »[27]. A riguardo ci si può interrogare circa l'obbligo di dare la medesima informativa anche ai soggetti rappresentati nel materiale multimediale reso pubblico, qualora si tratti di terzi rispetto all'autore. In proposito potrebbe soccorrere l'art. 13, comma 5, lett. *c*), del D.Lgs. 196/2003, secondo cui l'informativa può essere omessa quando « comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile ».

Così circoscritti gli adempimenti imposti dalla normativa in materia di trattamento dati, può ritenersi che, ove vi sia stata ottemperanza agli stessi, il gestore di una piattaforma UGC non è responsabile di aver posto in essere un trattamento illecito di dati. Né l'eventuale illecita acquisizione dei dati da parte dell'*uploader* comporta di per sé una responsabilità diretta del fornitore del servizio, salvo che questi ne sia a conoscenza e, così facendo, concorra nell'illecita diffusione, venendo meno l'esclusività del fine di pubblicazione o diffusione delle manifestazioni di pensiero di cui all'art. 136 del D.Lgs. 196/2003; tuttavia, laddove il fornitore del servizio sia posto a conoscenza dell'illiceità del trattamento, i dati acquisiti diverranno da esso inutilizzabili ai sensi dell'art. 11, comma 2, del D.Lgs. 196/2003 e conseguentemente i materiali andranno rimossi.

Da ultimo occorre interrogarsi sull'operatività delle norme in materia di trattamento dati ora richiamate; in particolare bisogna porre mente all'art. 5, commi 1 e 2, del D.Lgs. 196/2003, che esclude l'applicabilità della normativa italiana, e più in generale comunitaria, sul trattamento dati a soggetti non stabiliti nel territorio italiano, né impieganti mezzi strumentali ivi situati per porre

[26] Qualora invece emergesse la mancanza di detto consenso, risponderebbe dei danni comunque unicamente l'autore dell'*upload*, non solo in ragione del disposto di cui all'art. 16 del D.Lgs. 70/2003, su cui *infra* nel testo, ma anche in virtù dell'assenza di un agire colposo dell'intermediario, non essendo allo stesso possibile rendersi conto dell'illecito, specie laddove abbia specificamente indicato nelle condizioni d'uso la necessità di ottenere il consenso delle terze parti per i materiali pubblicati ad esse inerenti. Ovviamente, tanto ai sensi dell'art. 16 del D.Lgs. 70/2003, quanto secondo le più generali regole in materia di responsabilità extracontrattuale colposa, l'eventuale inerzia dell'intermediario assumerà invece rilievo ove questi risulti a conoscenza dell'assenza di un consenso implicito (ad esempio qualora, nel caso di segnalazione da parte degli utenti di video contenenti scene di violenza o intrusione nell'altrui intimità, dall'esame dei contenuti emerga in maniera palese l'assenza di un consenso implicito dell'effigiato).

[27] Cfr. art. 133 del D.Lgs. 196/2003.

in essere il trattamento, salvo il mero transito dei dati[28]. Ipotesi in cui dovrebbero rientrare i principali fornitori di contenuti del web sociale, che gestiscono i dati mediante *server* ubicati fuori dall'Unione europea[29]. In questi casi sarebbe comunque opportuno che i fornitori del servizio rendessero noto agli utenti che non trovano applicazione le suddette norme[30] e, nel caso di imprese statuni-

[28] Cfr. a riguardo, S. Sica, *sub* Articoli 1-6, in S. Sica-P. Stanzione, *La nuova disciplina della privacy*, Bologna, 2005, 36 s.

[29] Così il Garante per la protezione dei dai personali in diversi provvedimenti, ha ritenuto essere Google Inc. autrice del trattamento dei dati degli utenti del servizio UGC video e non applicabile a tale soggetto la disciplina comunitaria, essendo i *server* di Google Inc. ubicati negli USA (anche se le attuali *privacy policy* di Google sono meno nette sul punto, dichiarando che « Google elabora i dati personali sui propri server, ubicati negli Stati Uniti d'America e in altri Paesi » non definiti, cui si aggiunge il fatto che dalla pronuncia Trib. Milano, 12 aprile 2010, citata *supra*, sembra emergere una, non meglio indagata, attività di controllo sui contenuti video posta in essere all'interno dei confini comunitari ad opera di Google Ireland); cfr. a riguardo: Gar. 3 novembre 2009, doc. web n. 1687662; Gar., comunicato stampa, 30 maggio 2006; Gar., 22 marzo 2006, doc. web n. 1339146; Gar., 2 febbraio 2006, doc. web n. 1244676; Gar., 18 gennaio 2006, doc. web n. 1242501; Gar., 9 novembre 2005, doc. web n. 1213678 (tutti i provvedimenti sono pubblicati in *www.garanteprivacy.it*). Né ad una diversa conclusione « paneuropea » dovrebbe indurre la lettera dell'art. 4 della direttiva 95/46/CE, su cui U. Pagallo, *Sul principio di responsabilità giuridica in rete*, in questa *Rivista*, 2009, 719 ss. In particolare l'art. 4, paragrafo 1, lett. *c*) e *d*), della direttiva 95/46/CE non considera applicabile la normativa comunitaria sul trattamento dati per il semplice fatto che questo venga posto in essere entro i confini comunitari, bensì fa riferimento alla presenza in tale spazio di strumenti operativi funzionali al trattamento (« strumenti, automatizzati o non automatizzati, situati... a meno che questi non siano utilizzati ai soli fini di transito »), ne consegue che la finalità che traspare non è quella di considerare soggetto alle norme comunitarie il trattamento in quanto tale, quanto piuttosto quella di evitare che mediante l'*escamotage* di una localizzazione delle sedi al di fuori dell'Unione si possa bypassare l'applicazione della normativa a fronte di un'attività organizzata con mezzi sul territorio comunitario, cfr. anche 20° considerando della direttiva 95/46/CE. Tale situazione, anche alla luce delle considerazioni emerse dalla sentenza milanese, non pare ravvisarsi nel caso di Google, che sembra aver mantenuto effettivamente un forte accentramento organizzativo e gestionale negli Stati Uniti, come già affermato in Trib. Lucca, 20 agosto 2007, inedita; cfr. però l'ampia nozione di prestatore stabilito cui si fa riferimento in Articolo 29-Gruppo di lavoro per la tutela dei dati personali, *Parere 1/2008 sugli aspetti della protezione dei dati connessi ai motori di ricerca*, Bruxelles, 4 aprile 2008, 10, in *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_it.pdf*. Va in proposito rilevato come una rivendicazione orientata ad un'estesa applicabilità delle disposizioni degli Stati comunitari in materia di tutela di dati personali sia stata avanzata in Articolo 29-Gruppo di lavoro per la tutela dei dati personali, *Tutela della vita privata su Internet - Un approccio integrato dell'EU alla protezione dei dati on-line*, Bruxelles, 21 novembre 2000, 30 s., in *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37it.pdf*, secondo cui anche il semplice invio di *cookie* sarebbe di per sé sufficiente a costituire un impiego di strumenti atti al trattamento ai sensi dell'art. 4, paragrafo 1, lett. *c*), della direttiva 95/46/CE, posizione successivamente ribadita nel parere 1/2008 poc'anzi richiamato e poi generalizzata in Articolo 29-Gruppo di lavoro per la tutela dei dati personali, *Parere 5/2009 sui social network on-line*, citata *supra*, 5, in cui si afferma che « Le disposizioni della direttiva sulla protezione dei dati si applicano ai fornitori di SNS [social network services] nella maggior parte dei casi, anche se la loro sede si trova al di fuori del territorio SEE ». Al riguardo non sono mancate già in passato fondate critiche, cfr. in tal senso C. Kuner, *European data privacy law and online business*, Oxford-New York, 2003, 94 e 100 ss.

[30] Cfr. Gar., 22 marzo 2006, doc. web n. 1339146, in *www.garanteprivacy.it*.

tensi, che non rileverà neppure l'eventuale adesione ai Safe Harbor Principles[31].

Alla luce delle considerazioni espresse, laddove prevista, l'ottemperanza dell'impresa alle norme in materia di trattamento dati non risulta dunque particolarmente onerosa né impone particolari obblighi di controllo, si tratta semmai di obblighi informativi, della necessità di attivarsi nel caso di conoscenza della natura illecita del trattamento e, eventualmente, di consentire ai terzi interessati l'esercizio dei diritti di cui all'art. 7 del D.Lgs. 196/2003, tra cui spiccano nelle fattispecie qui considerate il diritto di ottenere il blocco e la cancellazione dei dati illecitamente raccolti e resi pubblici mediante il web.

Dal momento che l'illecito trattamento dei dati non esaurisce tuttavia le possibili ipotesi di violazione dei diritti altrui mediante la divulgazione di contenuti multimediali, occorre quantomeno considerare anche le ulteriori e diverse fattispecie, con specifico riguardo alla lesione della reputazione, del decoro, dell'immagine, del riserbo e dell'identità personale, cui vanno aggiunti i profili inerenti la violazione del diritto d'autore. Può infatti accadere che, pur nel rispetto degli adempimenti di cui al D.Lgs. 196/2003 summenzionati, il fornitore del servizio finisca per rendere accessibili *on-line* materiali che violano quest'ultimi diritti.

A tal proposito va ribadito come anche solo sul piano fattuale, con riferimento agli aspetti inerenti la persona, sia remota l'ipotesi di un concorso omissivo nell'illecito, anche ove (per assurdo) si ammettesse un monitoraggio di tutti i contenuti antecedentemente alla loro collocazione *on-line*: le barriere linguistiche e contestuali, unitamente ai casi di irriconoscibilità dell'offensività, riducono infatti drasticamente la possibile percezione dell'illecito attraverso la visione delle immagini. Sotto il profilo giuridico poi l'art. 16, del D.Lgs. 70/2003, sancisce che il prestatore « non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio »[32], salvo che non sia a conoscenza o nelle condizioni di

[31] Cfr. Decisione della Commissione del 26 luglio 2000, in *GUCE* L 215 del 25 agosto 2000, si veda in specie la FAQ 3 dell'All. II.

[32] Nuovamente si pone il problema dell'efficacia della normativa comunitaria, e delle conseguenti discipline attuative nazionali, con riguardo a soggetti che al fine di esercitare la propria attività di intermediario si avvalgano di dotazioni strumentali localizzate al di fuori dei confini dell'Unione. A riguardo, ai sensi degli artt. 1, comma 2, lett. *d*), e 3, comma 1, del D.Lgs. 70/2003, si deve ritenere applicabile il regime derogatorio in materia di responsabilità ai soli « prestatori stabiliti » appartenenti allo spazio economico europeo, ovvero a coloro che ivi esercitino « effettivamente un'attività economica mediante una stabile organizzazione per un tempo indeterminato », tenuto conto che la presenza e l'uso dei mezzi tecnici e delle tecnologie necessarie per prestare un servizio non costituiscono di per sé uno stabilimento del prestatore, v. anche ARTICOLO 29-GRUPPO DI LAVORO PER LA TUTELA DEI DATI PERSONALI, *Parere 1/2008 sugli aspetti della protezione dei dati connessi ai motori di ricerca*, citato *supra*, 10; cfr. a riguardo le critiche espresse circa l'errata trasposizione della direttiva 2000/31/CE da V. ZENO-ZENCOVICH, *La nuova disciplina del com-*

avvedersi dell'illiceità[33] o che, avutone conoscenza, non abbia provveduto ad informarne l'autorità competente[34] o non abbia rimosso prontamente o resi inaccessibili tali contenuti su segnalazione delle autorità[35]. Tanto meno è esigibile un controllo preventivo dei materiali caricati dagli utenti volto a non rendere pubbli-

mercio elettronico alla luce del D.Lgs. 70/03: questioni generali e ambiti di applicazione, in *Commercio elettronico e servizi della società dell'informazione*, a cura di E. Tosi, citata *supra*, 40. Tuttavia la situazione che in tal modo si viene a creare appare critica sotto il profilo della coerenza delle politiche del diritto perseguite e dell'uguaglianza di trattamento rispetto ad un fenomeno di natura sovranazionale. Mentre infatti il prestatore comunitario andrebbe esente da responsabilità, e da oneri di controllo, su quello extra-comunitario incomberebbe una responsabilità anacronistica alla luce della sostanziale uniformità delle soluzioni affermatesi in materia nell'Unione ed Oltreoceano, uniformità che invece non si riscontra con riferimento alla disciplina del trattamento dati di cui *supra* nel testo. Da tali considerazioni consegue che, anche ritenendo non applicabile ai soggetti sopra indicati le disposizioni di cui agli artt. 16 e 17 del D.Lgs. 70/2003, andrebbero comunque rigettate, al di là della loro praticabilità giuridica, le interpretazione delle norme codicistiche in materia di responsabilità extracontrattuale volte a ritenere responsabile l'intermediario per i danni derivanti dalla divulgazione di contenuti forniti da terzi della cui illiceità esso non abbia conoscenza o cui non abbia concorso.

[33] Cfr. art. 16, comma 1, lett. *a*), del D.Lgs. 70/2003; la norma distingue a riguardo fra illiceità penale e civile, in proposito si vedano in dottrina: G.M. Riccio, *La responsabilità civile degli* internet providers, Torino, 2002, 206; S. Sica, *Le responsabilità civili*, in *Commercio elettronico e servizi della società dell'informazione*, a cura di E. Tosi, *citata supra*, 292 s.; G.M. Riccio, *Responsabilità civile degli* internet providers, in *Professioni e responsabilità civile*, diretto da P. Stanzione e S. Sica, Bologna, 2006, 753 ss.

[34] Cfr. art. 17, comma 3, del D.Lgs. 70/2003.

[35] Cfr. artt. 16, comma 1, lett. *b*), e 17, comma 3, del D.Lgs. 70/2003. Non pare in proposito condivisibile l'assunto espresso nell'ordinanza Trib. Roma, 16 dicembre 2009, citata *supra*, secondo cui non sarebbe sostenibile la tesi dell'irresponsabilità del *provider* svolgente la funzione di *hosting*, qualora « ''le regole'' stabilite dal provider... [prevedono] il diritto di controllare i contributi, la assoluta discrezionalità nell'interrompere in maniera temporanea o permanente la fornitura del servizio ». Così ragionando si mostra di non ricordare l'origine stessa delle norme comunitarie e dell'antecedente §230 del *Communications Decency Act* (CDA) statunitense del 1996, cui è seguito il § 512 del *Digital Millenium Copyright Act* (DMCA) del 1998, dovendosi allora rievocare alla mente lo storico caso *Stratton Oakmont v. Prodigy Inc.*, 1995 NY Misc. Lexis 229, che sembrava ormai appartenere ad un'epoca passata ed inerire a problemi risolti. Cfr. per l'esperienza italiana Trib. Roma, 4 luglio 1998, in questa *Rivista*, 1998, 807 ss. È infatti del tutto ovvio che ogni *provider* è in grado di agire sui contenuti, ma i limiti alla responsabilità relativa all'attività di *hosting* sono stati previsti proprio alla luce di tale possibilità: da un lato per evitare di addossare oneri eccessivi sugli intermediari, consistenti nei costi finanziari ed organizzativi del monitoraggio, e dall'altro per evitare il paradosso emerso nella giurisprudenza per cui chi controllava i contenuti veniva ritenuto responsabile a titolo omissivo per gli illeciti commessi dagli utenti, mentre chi non effettuava verifica alcuna veniva considerato estraneo al loro agire. La limitazione di responsabilità è stata così utile anche per arginare la potenziale tendenza verso la rinuncia a qualsiasi forma di controllo, indotta dalla giurisprudenza ora richiamata, permettendo al *provider* di introdurre dei filtri senza per questo incorrere in responsabilità a causa del livello di efficacia degli stessi. In proposito recentemente la Corte Giustizia delle Comunità Europee, con la sentenza 23 marzo 2010, procedimenti riuniti C-236/08, *Google France SARL e a. c. Louis Vuitton Malletier SA*, C-237/08, *Google France SARL c. Viaticum SA e a.*, e C-238/08, *Google France SARL c. Centre national de recherche en relations humaines (CNHRRH) SARL e a.* sul caso Google AdWords, pubblicata in http://curia.europa.eu, ha ribadito come l'esclusione di responsabilità per l'attività di *hosting*, ai sensi dell'art. 14 della direttiva 2000/31/CE, venga meno solamente allorché il fornitore del servizio abbia svolto un ruolo attivo tale da avere « la conoscenza o il controllo » dei dati memorizzati.

camente accessibili quelli lesivi degli altrui diritti, posto che ai sensi dell'art. 17, comma 1, del D.Lgs. 70/2003 « il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite ». Escluso dunque il monitoraggio attivo[36], gli unici oneri che incombono sull'intermediario sono quelli di agire prontamente qualora venga a conoscenza di illeciti, collaborando con le autorità giudiziarie ed amministrative nell'individuazione dei responsabili e nell'inibizione di tali attività.

Nuovamente trattasi di adempimenti limitati dal punto di vista dei costi gestionali e finanziari connessi, essendo qui da rigettare quelle letture troppo estensive di tali doveri che finiscono per introdurre in forma surrettizia un obbligo di controllo. In specie, considerata l'ingente mole di dati presenti sulle piattaforme UGC, occorre definire correttamente quale sia il livello di conoscenza dell'illecito oltre cui l'intermediario debba attivarsi; non pare a riguardo che i generici riferimenti dell'art. 16 del D.Lgs. 70/2003 a « l'attività o l'informazione » illecita, come quelli al « contenuto » del servizio di cui al successivo art. 17, comma 3, possano comunque indurre a ritenere sufficiente la semplice conoscenza della presenza, non sufficientemente circostanziata, di materiale lesivo degli altrui diritti. Se infatti bastasse indicare che da qualche parte, fra i contenuti *on-line* gestiti dal servizio, vi sono filmati pregiudizievoli per l'interessato, oppure in danno del suo diritto d'autore, verrebbe indirettamente imposto all'intermediario un gravoso onere di controllo, seppur *ex post*, su tutti i materiali, facendo venir meno l'esonero dalla ricerca attiva dei contenuti illeciti di cui all'art. 17 del D.Lgs. 70/2003[37]. Ne consegue

[36] Cfr. in tal senso anche Trib. Milano, 12 aprile 2010, citata *supra*, ove si afferma che « esiste quindi, a parere di chi scrive, un obbligo NON di controllo preventivo dei dati immessi nel sistema » (carattere maiuscolo del testo originale) e che « non esiste, a parere di chi scrive, perlomeno fino ad oggi, un obbligo di legge codificato che imponga agli ISP (*internet service provider*) un controllo preventivo della innumerevole serie di dati che passano ogni secondo nelle maglie dei gestori o proprietari dei siti web ». Non paiono condivisibili invece le valutazioni espresse nell'ordinanza Trib. Roma, 16 dicembre 2009, citata *supra*, secondo cui « la normativa — vedi D.Lgs. n. 70/2003 — e la giurisprudenza sta ormai orientandosi nel senso di una valutazione caso per caso della responsabilità del *provider* che... assoggetta il provider a responsabilità quando non si limiti a fornire la connessione alla rete, ma eroghi servizi aggiuntivi (per es. caching, hosting) e/o predisponga un controllo delle informazioni ». In proposito — oltre a richiamare quanto espresso *supra* nella precedente nota circa la rilevanza da attribuirsi al controllo volontariamente posto in essere — con riferimento ai « servizi aggiuntivi » di *caching* ed *hosting*, va osservato che tanto la direttiva comunitaria quanto il D.Lgs. 70/2003 prevedono una forte limitazione di responsabilità proprio in relazione a tali attività, non certo ravvisando dunque in una simile tipologia di servizi un indice di concorso nell'illecito.

[37] Per queste ragioni non paiono condivisibili le argomentazioni rinvenibili nell'ordinanza Trib. Roma, 16 dicembre 2009, citata *supra*, né quelle della successiva ordinanza emessa in sede di reclamo, inedita, le quali nell'inibire all'intermediario la pubblicazione di futuri contenuti ille-

dunque, anche in un'ottica di bilanciamento degli interessi, che potranno solo ammettersi contestazioni specifiche che consentano al fornitore del servizio di individuare i *file* illeciti, non potendosi ritenere esigibile una verifica completa ed esaustiva — tale quindi da rimuovere qualsiasi elemento *contra legem* — sulla base, ad esempio, della semplice indicazione del nominativo di una persona o di un prodotto creativo[38].

Il prestatore, ai sensi degli artt. 16 e 17 del D.Lgs. 70/2003, può dunque considerarsi tenuto ad effettuare tutti i controlli nelle sue possibilità sulla base di precise indicazioni fornite dal soggetto leso, utili al fine di un'analisi di quanto *on-line*[39], ma pretendere un monitoraggio più approfondito, volto anche al materiale non « taggato » con parole chiave pertinenti[40], appare oltre che non esigibile nell'ottica di una sostenibilità tecnica ed economica dell'attività di intermediario, neppure conforme alle deroghe che le disposizioni in materia di commercio elettronico dettano per tali soggetti. Tale considerazione è ulteriormente comprovata dal fatto che le norme in questione prevedono l'attivazione dell'intermediario qualora venga a conoscenza dell'illecito, se ne desume dunque la necessità che quest'ultimo sia stato individuato in tutti i suoi elementi e non definito solo attraverso un'allegazione di massima, la quale richiederebbe un'attività integrativa ad opera dell'interme-

citi analoghi a quelle oggetto di contestazione, oltre a considerare sufficienti al fine dell'individuazione di tutto il materiale la semplice indicazione del nome del programma televisivo, finiscono per introdurre surrettiziamente un obbligo di controllo attivo generalizzato per il futuro, mentre il medesimo art. 156 della L. 633/1941, nel prevedere l'inibitoria, al comma 2° esplicitamente dichiara che « sono fatte salve le disposizioni di cui al decreto legislativo 9 aprile 2003, n. 70 ». A conclusioni diverse è invece addivenuto, in un caso analogo, il Juzgado de lo Mercantil n. 7 di Madrid, 23 luglio 2008, n. 320, secondo cui « se requiere a las actoras para que de manera inmediata presenten a este Juzgado las identificaciones suficientes de sus contenidos para que se suspendan las emisiones sin autorización y se prohiban nuevas »; la sentenza è pubblicata in *http://civitas.es/index.php/informacion-juridica/jurisprudencia/civil/auto-del-juzgado-de-lo-mercantil-n-7-de-madrid-3202008-de-23-julio*.

[38] Si deve infatti tenere conto che gli utenti possono impiegare nomi di fantasia nel denominare i *file* caricati e solo attraverso una visione di tutti i filmati sarebbe possibile verificarne la pertinenza rispetto al soggetto/prodotto colpito dall'illecito.

[39] A riguardo va sottolineato come non occorra necessariamente individuare il nome del *file* costituente materiale illecito o il nome dell'utente che lo ha caricato, potendosi anche esigere controlli più generalizzati, ma sempre sulla base di elementi gestibili attraverso sistemi che consentano un efficace filtraggio iniziale mediante strumenti di ricerca automatizzata (nel caso di violazione del diritto d'autore potrebbe, ad esempio, essere utile una ricerca in base al nome del protagonista del filmato o al titolo dell'opera) e nei limiti dei risultati rilevabili attraverso tali tecniche.

[40] I *tag* sono le parole chiavi che l'utente, all'atto del caricamento *on-line* di ciascun materiale, indica al fine di segnalare la pertinenza dei contenuti ad una determinata area tematica. È però possibile caricare materiale privo di *tag*, così come non v'è alcun controllo sulla reale coerenza del *tag*, potendo benissimo essere anche totalmente fallace (e ciò può accadere ad esempio per conseguire una diversa indicizzazione nel motore di ricerca, in ragione del maggiore *appeal* del termine scelto).

diario nell'individuazione delle circostanze dell'illecito incompatibile con le finalità stesse delle disposizioni derogatorie richiamate.

Oltre ad uno *screening* che muova dai meta-dati[41] testuali presenti sulla piattaforma UGC, è poi esigibile anche una diversa analisi automatizzata mediante *software* volta ad individuare i contenuti ripresi da trasmissioni televisive in cui compaia il logo dell'emittente o di un dato programma[42]. Un simile controllo attraverso sistemi di riconoscimento di immagine[43], così come quello diverso incentrato sul *fingerprint*[44], può comportare tuttavia dei falsi positivi e negativi, con il rischio di rimozione di contenuti legittimi[45], di cui quantomeno gli utenti andrebbero debitamente informati all'interno delle condizioni del servizio. L'onere di simili procedure sarebbe significativo nella sua iniziale implementazione (per via dell'« arretrato » presente in rete), ma andrebbe a ridursi nel momento in cui il filtro verrebbe successivamente ad operare in maniera automatica all'atto del singolo *upload*[46].

4. Le prospettive future.

Da quanto sin qui osservato emerge come l'attuale stato dell'arte riveli l'esistenza di un bilanciamento fra le esigenze di tutela

[41] I metadati, alla cui categoria appartengono i *tag*, costituiscono qualsiasi informazione impiegata per descrivere un insieme di dati, dunque anche un contenuto multimediale.

[42] Si veda a riguardo anche l'ordinanza Trib. Roma, 16 dicembre 2009, citata *supra*, laddove la tutela del logo di un programma e di una rete televisiva è stata oggetto di specifica domanda inibitoria nei confronti di YouTube.

[43] In pratica, prendendo in esame il fermo immagine del filmato, il *software* dovrebbe individuare automaticamente l'area del logo (solitamente in basso a destra) e quindi confrontare quest'ultimo con il modello standard. Rimarrebbero ovviamente esclusi da tale verifica i contenuti che, benché protetti dal diritto d'autore, non presentino alcun logo perché originariamente assente (es. film derivanti da dvd) o rimosso dall'utente prima dell'*upload*.

[44] Cfr. a riguardo il sistema « Content ID » di YouTube, descritto in *http://www.youtube.com/t/contentid*.

[45] I limiti di tali sistemi di identificazione sono soprattutto legati alla presenza di falsi positivi, riconducibili sia alle ipotesi di libera utilizzazione di materiali coperti dal diritto d'autore, quanto alla diversa fattispecie in cui gli autori stessi, o i produttori, abbiano direttamente immesso in rete, con finalità di libera fruizione e diffusione, materiali già distribuiti mediante altri canali commerciali, con la conseguenza che non risulta accertabile se la copia utilizzata dall'utente sia una copia « pirata » o quella resa pubblica. Cfr. in argomento anche le critiche espresse da F. von Lohmann, *YouTubés Content IS (C)ensorship Problem Illustrated*, 2 marzo 2010, in *http://www.eff.org/deeplinks/2010/03/youtubes-content-id-censorship-problem*.

[46] Il prestatore del servizio, in maniera del tutto volontaria, mancando un obbligo giuridico in tal senso, potrebbe poi ritenere opportuno adottare delle politiche volte alla dissuasione dei comportamenti illeciti agendo sulle clausole contrattuali, ad esempio prevedendo la disabilitazione dell'*account* utente per chi sia risultato autore di condotte illecite in seguito alle verifiche di cui *supra* nel testo. Va tuttavia considerata la limitata efficacia di una simile soluzione, poiché nulla vieta al soggetto medesimo di registrarsi nuovamente sotto altro nome, anche se (specie con riguardo ad utenti molto attivi) potrebbe svolgere una funzione dissuasiva l'onere derivante dalle necessità di caricare nuovamente tutti i propri contenuti multimediali oltre che comunicare la propria nuova identità agli appartenenti al servizio con cui precedentemente si abbiano avuto rapporti.

dei diritti e gli oneri di controllo incombenti sull'intermediario. Bilanciamento che risulta economicamente e tecnicamente sostenibile, oltre che legittimato da specifiche scelte legislative. Occorre dunque da ultimo interrogarsi se nelle pieghe dell'attuale « clima politico » che sembra stia spingendo, per varie ragioni, legislatori e giudici verso una maggior responsabilizzazione di tali soggetti siano da intravvedere le prime avvisaglie di un nuovo e diverso equilibrio, carico di conseguenze sull'organizzazione e sui costi aziendali.

A riguardo sembra opportuno un minimo distinguo fra i due diversi ambiti da cui provengono le istanze di regolamentazione, ovvero quello della tutela delle persone e quello della tutela del diritto d'autore. Mentre infatti nel primo caso si è in presenza per lo più di una pretesa di protezione avanzata da singoli rispetto al proprio io, solitamente avulsa da risvolti economico-patrimoniali, nel secondo si è invece in presenza di uno scontro fra gruppi di interesse economico: da un lato i titolari del diritto d'autore e gli enti deputati alla gestione dei lucrosi proventi della creatività e dall'altro un segmento di operatori di rete, anch'esso non certo privo di rilevanza economica (basti pensare ai fatturati di Google).

Ne consegue una diversità degli interessi tutelati, delle posizioni reciproche di forza e dei rimedi esperibili. Mentre infatti il singolo, violato nel suo riserbo o nella sua dignità, subisce un pregiudizio ad un bene di rango superiore rispetto a quello economico, ma nel contempo non ha altro rimedio che avvalersi degli strumenti tradizionali che la responsabilità civile gli offre, non così per quanto concerne i detentori del diritto d'autore. Quest'ultimi infatti rivendicano la protezione di un diritto che, guardando alla gran parte del contenzioso in essere, emerge solo nel suo connotato meramente economico e si pone dunque alla stessa stregua degli interessi imprenditoriali perseguiti dal fornitore del servizio[47], ragion per cui il bilanciamento va individuato ad un livello diverso e più equamente ripartito rispetto alla prima ipotesi. Va poi osservato come, proprio in tale ottica di equivalenza di interessi, può risultare eccessivo pretendere che un operatore commerciale si faccia carico del ruolo di garante dei diritti di altri soggetti anch'essi agenti con finalità lucrative, non dovendosi dimenticare poi come nello specifico l'imposizione di efficaci misure di prevenzione e controllo comporti costi di notevole entità e, con le tecnologie attualmente disponibili, non sia comunque mai realizzabile in maniera completa. Sempre nella prospettiva del contemperamento degli opposti interessi va poi ricordato come in questo secondo

[47] Cfr. V. Zeno-Zencovich, *Diritto d'autore e libertà di espressione: una relazione ambigua*, in *AIDA*, 2005, 151 s.

caso i titolari dei diritti sui contenuti dispongano anch'essi di misure tecnologiche di protezione, per giunta esplicitamente previste e tutelate dalla legge[48]. Per altro anche in termini di modelli di *business* non mancherebbero soluzioni soddisfacenti per i titolari dei diritti, tenuto altresì conto della pubblicità ai loro contenuti che comunque deriva dalla condivisione degli stessi attraverso le piattaforme UGC[49].

I limiti connaturati ai contrastanti interessi in gioco ed alla tecnologia esistente paiono dunque sconsigliare un mutamento dell'attuale quadro con riferimento alla tutela dei diritti diversi da quelli inerenti la persona. Per quest'ultimi invece, ma il discorso si allarga necessariamente al di là dei soli servizi UGC, è invece forse giunta l'ora di rimeditare l'impostazione iniziale data alla rete, valutando attentamente la transizione verso forme di anonimato « controllato »[50], in cui gli utenti possano essere anonimi verso i terzi, ma non verso le autorità di vigilanza. Si tratterebbe ovviamente di una transizione irta di difficoltà, complicata dalla presenza di autorità di controllo rispondenti a governi illiberali, ma è in ogni caso un passaggio su cui interrogarsi nel momento in cui il mondo digitale è ormai diventato un'estensione di quello reale (ricreandone da ultimo anche la componente sociale) e, conseguentemente, non pare illogico estendere anche ad esso quelle forme di controllo sulle persone già riconosciute ed accettate *off-line*.

---

[48] Cfr. art. 102-*quater*, nonché artt. 71-*quinquies*, 71-*sexies*, 71-*septies* e 171-*ter*, della L. 633/1941.

[49] Si vedano a riguardo gli accordi fra YouTube e diversi produttori per la distribuzione legale di materiale protetto dal diritto d'autore, su cui cfr., *ex multis:* D. Sabbagh, *Going Alternative. Can digital subscriptions and new media steer record companies through uneasy times?*, su *Time*, 17 maggio 2010; *YouTube lancia un servizio per il noleggio di film*, 21 gennaio 2010, in *www.ilsole24ore.com* e A. Balbi, *Accordo YouTube-Hollywood sul sito kolossal e serie tv*, 17 aprile 2009, in *www.repubblica.it*. Cfr. inoltre IFPI, *Digital Music Report 2009. I nuovi modelli di business dell'industria musicale in un mondo che cambia*, 2009, ed IFPI, *Digital Music Report 2010. La tua musica: sempre ed ovunque*, 2010, entrambi consultabili nella versione italiana al sito *www.fimi.it*.

[50] Cfr. a riguardo, seppur con alcune differenze rispetto a quanto qui proposto, G.M. Riccio, *Diritto all'anonimato e responsabilità civile del* provider, in *Internet e il diritto dei privati. Persona e proprietà intellettuale nelle reti telematiche*, a cura di L. Nivarra-V. Ricciuto, Torino, 2002, 39 s. e R. Natoli, *Profili della diffamazione* on line*: spunti dall'esperienza statunitense*, ivi, 92 ss. In generale sulla garanzia giuridica dell'anonimato in rete ed i suoi limiti cfr. invece E. Pelino, *L'anonimato su internet*, in *Diritto all'anonimato. Anonimato, nome e identità personale*, a cura di G. Finocchiaro, in *Trattato di diritto commerciale e di diritto pubblico dell'economia*, diretto da F. Galgano, Padova, 2008, 229 ss.