Autori Vari

IL CASO GOOGLE / VIVIDOWN

nella giurisprudenza e nella opinione della dottrina

a cura di GIUSEPPE CASSANO

Tribunale di Milano, 12/04/2010, n. 1972, sez. IV, Est. Magi

Il gestore o proprietario di un sito web qualificabile come «content provider» non è titolare di una posizione di garanzia da cui derivi un obbligo di attivazione, in mancanza del quale ricorre la previsione del c.p.v. dell'art. 40 c.p., e pertanto non può essere ritenuto responsabile di concorso omissivo nel reato di diffamazione, derivabile dal contenuto del materiale caricato, poiché non esiste un obbligo di legge codificato che impone un controllo preventivo sui dati immessi nella rete.

(*Omissis*). Parte seconda: i capi di imputazione del presente procedimento e la valutazione in diritto delle emergenze processuali

1) I capi di imputazione residui e la competenza territoriale Va innanzitutto rammentato che la vicenda in esame appare più circoscritta rispetto alla originaria formulazione dei capi di imputazione di cui al decreto di citazione diretta dei P.M. di Milano. Ed infatti la remissione di querela di D.L. al capo A di imputazione (con conseguente declaratoria di improcedibilità nei confronti degli imputati ex 469 e 129 c.p.p.), ha inevitabilmente limitato l'accertamento del fatto alla sola violazione degli articoli di legge contestati in relazione alla posizione di parte lesa dell'associazione V.D. Questo fatto (e cioè l'improcedibilità per le parti lese D.L.), a parere delle difese degli imputati, costituirebbe un elemento pregiudiziale e rilevante ai fini della ricostruzione del fatto contestato, dovendosi ritenere il capo A come «depurato» dalla presenza del D.L., anche soprattutto ai fini della rivalutazione del prospettato obbligo di garanzia in capo agli imputati, come riferibile solo ai dati personali dell'associazione in parola.

Va ritenuto, invece, che nella vicenda in esame non vada confuso il tema delle condizioni di sussistenza dell'obbligo di garanzia con quello della mancanza delle condizioni di procedibilità: in altre parole, la remissione di querela da parte dei D.L. esclude solo la configurabilità del fatto (in termini di responsabilità) nei confronti degli imputati in relazione alla parte lesa in questione, ma non incide sugli elementi costitutivi del capo di imputazione, e, in particolare, sulla ricostruzione dello stesso così come prospettato, e cioè come obbligo giuridico di impedire l'evento dannoso ai danni del D.L. in primis e, in conseguenza di ciò, anche nei confronti dell'associazione V.D. È, naturalmente, ovvio che si potrà parlare di evento dannoso (in termini di responsabilità e di eventuale risarcimento del danno) solo nei confronti dell'Associazione V.D., la cui reputazione è rimasta in gioco nella vicenda in esame.

Quanto al capo C dell'originaria imputazione, lo stesso è stato stralciato in seguito all'ordinanza di questo giudicante in data 21 aprile 2009, con contestuale trasmissione degli atti all'A.G. di Roma per competenza territoriale. Nella stessa ordinanza citata (e richiamata in toto nel corso della presente trattazione) è stata risolta la questione sollevata dalle difese relativa alla incompetenza territoriale dell'A.G. di Milano, con reiezione della stessa ed incardinamento del procedimento presso questa autorità procedente.

La valutazione, allora fatta da questo giudice in termini prospettici atteso il momento processuale in corso, deve ritenersi confermata all'esito della vicenda processuale esaurita: non vi è dubbio che la competenza per il reato sub B (più grave rispetto a quelli contestati) spetti all'autorità milanese; il reato di cui all'art. 167 d.lg. 30 giugno 2003, n. 196 è stato sicuramente commesso anche in Milano (sotto il profilo del trattamento dei dati inteso come elaborazione ed organizzazione degli stessi) avendo sede a Milano la società "G. I." indicata nel capo di imputazione come responsabile dei comportamenti incriminati, i cui responsabili direttivi ed operativi sono stati individuati dall'A.G. procedente nelle persone poi imputate. Risulta quindi rispettata la limitazione contenuta nell'art. 5 comma 1 del codice privacy (che cioè la normativa sul trattamento dei dati personali è applicabile solo a soggetti stabiliti in Italia), avendo, come si è detto, G.I. sede a Milano, ed avendo la predetta società (per i motivi che si espliciteranno in seguito) operato il trattamento dei dati del D.L. senza il consenso previsto dalla stessa legge.

2) Il capo B di imputazione: il trattamento dei dati personali del D.L. «Il trattamento dei dati personali sensibili senza il consenso dell'interessato, dal quale derivi nocumento per la persona offesa, già punito ai sensi dell'art. 35 comma 3 l. 31 dicembre 1996, n. 675, è tutt'ora punibile con la stessa pena ai sensi dell'art. 167 comma 2 d.lg. 30 giugno 2003, n. 196, in quanto le condotte di "comunicazione" e "diffusione" dei dati sensibili, sono ora ricomprese nella più ampia dizione di "trattamento" dei dati sensibili, ed il nocumento della persona offesa, che si configurava nella previgente fattispecie come circostanza aggravante, rappresenta nella disposizione in vigore una condizione obiettiva di punibilità» (Cass., sez. III, n. 28680 del 26 marzo 2004).

La sentenza della S.C., di cui si è riportata la massima rappresenta una sintesi completa dei parametri giuridici di riferimento al fine di inquadrare la complessa vicenda qui in esame; elencando, gli elementi essenziali del reato contestato sono i seguenti: a) l'avvenuto trattamento dei dati sensibili di una persona; b) il mancato consenso da parte del soggetto; c) il nocumento della persona offesa; d) Il dolo specifico da parte del soggetto agente. Per completezza esegetica va fatto riferimento alla elencazione ed esplicitazione definitoria del concetto di "trattamento" e di "dato personale" o di "dato sensibile" contenuta nell'art. 4 d.lg. in parola: aa) trattamento come qualunque operazione o complesso di operazioni ... concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione, di dati..." bb) dati sensibili i dati personali idonei a rivelare l'origine razziale o etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, ... nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale». Infine vanno richiamati gli artt. 13, 17, 23 e 26 dello stesso decreto in relazione alla modalità di trattamento dei dati personali e sensibili ed all'obbligo del consenso scritto da parte dell'interessato per il loro corretto utilizzo.

Nella vicenda in questione i P.M. di Milano ritengono che gli imputati D., D.L.R. e F., nella loro rispettiva qualità di responsabili di G.I. i primi due e di G. Inc. il terzo, in relazione alla policy per la privacy per l'Europa, abbiano commesso il reato in questione, omettendo il corretto trattamento dei dati personali e sensibili di D.L.F.G., consentendo il caricamento del file video incriminato in data 8 settembre 2006 ed il suo mantenimento sul sito G. video.it, al fine di trarne un profitto; tale profitto deriverebbe, sempre secondo l'accusa, dal rapporto esistente tra la società G.I. ed il servizio G.V. (gestito da G. Inc.), rapporto commerciale consistente, tramite la gestione e l'operatività del sistema AD words, nel beneficiare degli indotti pubblicitari degli inserzionisti, indotti collegati alla gestione dei dati immessi sul G. V., e quindi direttamente dipendenti dalla quantità e qualità dei medesimi. In parole più semplici, G. I. sarebbe stato il motore pubblicitario ed economico, in Italia, di G. Inc., che (a partire dal luglio del 2006, data di localizzazione in Italia del servizio G. V.), avrebbe, con una politica aggressiva e spregiudicata nel mercato dei video sul web, tentato di accaparrarsi una grossa fetta del mercato italiano dei video amatoriali, consentendone il caricamento e l'utilizzo senza rispettare in modo adeguato le regole relative alla concreta protezione dei dati personali.

Questo comportamento, fatto, come si è detto, per un fine di lucro (e cioè consentire a G. I. l'accaparramento di numerosi ed importanti clienti privati che pagavano per potersi «inserire», attraverso la gestione di parole chiave, nel sito dei video privati) avrebbe causato una voluta «disattenzione» nelle politiche societarie relative alle problematiche del trattamento dei dati personali, al fine di occupare una fetta di mercato consistente a livello quantitativo e di poter quindi scalzare i relativi concorrenti (tra i quali c'era, non bisogna dimenticarlo, anche Y.T., allora non ancora di proprietà di G. Inc.).

Sempre secondo i P.M., le complessive modalità di esplicazione di tale servizio, incidendo sui dati immessi nel sistema G. V., comporterebbero necessariamente un trattamento degli stessi e quindi escluderebbero la possibilità di considerare G. I. (o comunque G. V.) un «mero intermediario passivo» (host provider) che agisce a richiesta del destinatario del servizio, ma un «content provider» e cioè un gestore di contenuti, con tutte le relative conseguenze in termini di responsabilità penale per i contenuti immessi.

Le difese degli imputati, naturalmente, contestano le affermazioni e le valutazioni dei PM facendo osservare: − che il c.d. codice privacy (d.lg. n. 196 del 2003) non è applicabile a G. I., in quanto il trattamento dei dati contenuti nel video incriminato non sarebbe avvenuto in Italia, ma, al più negli Stati Uniti, a Denver, luogo ove sono ubicati i server di G. Inc. che immagazzinano e trattano i dati provenienti dal caricamento dei video in ogni parte del mondo; − che G. I., in quanto esercente mera attività di marketing a favore di G. Inc., non aveva alcun potere ed alcuna possibilità di trattare i dati di proprietà di G. Inc.; − che non vi è alcun legame tra il sistema AD Words e G. V.; − che G. V. (e quindi a maggior ragione G. I.) è soltanto un intermediario di hosting (e quindi un Host provider) e, anche sulla base della recente normativa sul commercio elettronico

(d.lg. n. 70 del 2003), non è assolutamente responsabile del contenuto dei dati sullo stesso immessi; − che non vi è quindi nessun «obbligo di controllo» da parte della medesima società sulle informazioni che trasmette o memorizza, né un obbligo generale di ricerca di fatti o circostanze che indichino la presenza di attività illecite sulle informazioni medesime (vedi art. 17 d.lg. n. 70 del 2003); − che l'unico obbligo di controllo sui dati contenuti nel video incriminato spettava a chi ha caricato il video, che avrebbe dovuto procurarsi il consenso del D.L.; − che l'unico obbligo dell'host provider, nel caso in questione, nel momento in cui mette a disposizione del privato un servizio web quale quello poi concretamente utilizzato, è quello di indicare nelle «condizioni di servizio termini del contratto» l'esistenza di obblighi a carico dell'utente, quale quelli relativi alla legge sulla privacy, la cui ottemperanza è di esclusiva responsabilità del privato, con assoluta esclusione della responsabilità del provider; − che, quindi, unica responsabile dell'eventuale illegittimo trattamento dei dati in questione è la persona che ha caricato il video senza procurarsi il consenso del D.L., non incombendo sull'host provider alcun obbligo di controllo successivo sui dati medesimi; − che, in ogni caso, i dati del D.L. rinvenibili sul video non riguardano il suo stato di salute (essendo egli autistico e non affetto da sindrome di Down), e quindi non possono essere considerati come dati sensibili; − che non vi è stata alcuna violazione né dell'art. 17 che dell'art. 13 del codice privacy, avendo G. V. fornito una completa informativa agli utenti in merito al trattamento dei dati; − che, infine, vi è una assoluta insussistenza del fine di profitto da parte di G. I., che non trae alcun tipo di guadagno dal servizio G. V., che è gratuito. Come può facilmente evidenziarsi da quanto fin qui riportato, la questione è piuttosto complessa e, a parere dello scrivente, richiede una attenta disamina dei dati fin qui riassunti, ponendo alcuni punti fermi da cui partire per la successiva esegesi del fatto e delle norme allo stesso applicabili. In primo luogo occorre, partendo dal capo di imputazione, verificare se si è in presenza di una violazione di cui all'art. 167 d.lg. n. 196 del 2003, così come contestata agli imputati; in secundis va accertato se gli imputati medesimi siano da considerare colpevoli della stessa.

Ora, partendo dalla disamina della prima questione citata, deve rilevarsi che: − non vi è possibile dubbio sul fatto che il video in questione contenga delle «pesanti» allusioni allo stato di salute del soggetto D.L.: il fatto che tali allusioni siano state fornite in forma tecnicamente imprecisa e non siano pienamente corrispondenti all'effettiva situazione medica dello stesso, a parere di chi scrive, non appare così importante ai fini della responsabilità penale contestata; deve, tra l'altro, ritenersi, che la sola evidenziazione visiva dello stato di minorità del soggetto costituisca condotta colpevole del reato in questione; così come avverrebbe se, per esempio, si mostrasse in un video una particolare preferenza sessuale di un soggetto, pur non dando allo stesso alcuna connotazione negativa o derisoria. In altre parole la definizione verbale è solo uno dei modi in cui può esercitarsi il comportamento colpevole, ma non esaurisce le modalità commissive del reato contestato.

− In questo senso, non vi è nemmeno possibilità di dubbio in ordine al fatto che il video in questione sia, di per sé, un «dato personale sensibile» riferibile al D.L., e, come tale, possa essere inquadrato nella previsione dell'art. 167 d.lg. citato. − Nemmeno risulta dubitabile il fatto che il D.L. non abbia prestato alcun tipo di consenso in ordine alla divulgazione del video incriminato, men che meno scritto così come prevede la norma (artt. 23 e 26 d.lg. citato): lo dimostra, quantomeno, la denuncia relativa effettuata dalla parte (in questo caso il padre, trattandosi di soggetto minore). − Che il consenso non gli sia stato nemmeno richiesto, risulta anche questo chiaramente dalla disamina degli atti processuali relativi (denuncia del padre, indagini di PG sul punto). − Che vi sia stato, senza ombra di dubbio, un evidente nocumento della persona offesa, lo dimostra, se non altro, il risarcimento del danno a cui effettuato da parte degli imputati. − Che quindi, concludendo su questo punto, si sia in presenza di una palese violazione dell'art. 167 d.lg. n. 196 del 2003, perlomeno da un punto di vista oggettivo, è circostanza non dubitabile in alcun modo. Occorre, a questo punto, verificare altre due circostanze fondamentali: − su chi incombesse l'obbligo previsto dalla norma di richiedere il consenso e comunque di non trattare i dati contenuti nel video senza il consenso medesimo; − se vi sia stato, e per chi, un fine di profitto nel comportamento in questione.

Ora, se non può esservi dubbio sul fatto che l'obbligo in questione incombesse certamente sul soggetto che ha girato e poi caricato il video sul sito web G.V., va valutato con attenzione se tale obbligo fosse riferibile anche al soggetto che tale video ha avuto in carico, che tali dati poi ha gestito e diffuso tramite lo strumento di comunicazione che viene comunemente chiamato internet (e cioè l'ISP internet service provider). La domanda che, a questo punto, bisogna porsi è molto precisa: esiste un obbligo per il proprietario o gestore del sito web (provider, host provider, access provider, service provider, content provider che sia) di adeguamento e di rispetto ai dettami di una legge della repubblica operativa (come si è visto) fin dal 1996?

E, se tale obbligo esiste, in che misura esso è richiedibile al soggetto/web? Ovvero è un obbligo che impone un controllo preventivo dei dati immessi o che prevede soltanto un comportamento di corretta informazione degli utenti? Per una risposta precisa a questa domanda occorre fare un passo indietro e verificare quali siano i comportamenti che la legge (anzi il d.lg.) indica come automaticamente significativi di trattamento dei dati: come si è visto poc'anzi, tali comportamenti (indicati all'art. 4 d.lg. citato) sono molteplici e vanno dalla raccolta dei dati alla loro diffusione ed (addirittura) alla cancellazione degli stessi.

Non può esservi quindi dubbio, a parere di chi scrive, che non esiste, in materia, una zona franca (da un punto di vista oggettivo) che consenta ad un qualsiasi soggetto (persona fisica o meno che sia) di ritenersi esente dall'obbligo di legge, nel momento in cui venga, in qualsiasi modo, in possesso di dati sensibili: trattamento di dati è qualsiasi comportamento che consenta ad un soggetto di «apprendere» un dato e di mantenerne il possesso, fino al momento della sua distruzione. A maggior ragione non può escludersi (come si è detto da un punto

di vista meramente oggettivo) che «tratti» un dato di chi «raccolta, elabori, selezioni, utilizzi, diffonda, organizzi» dati che, per la loro natura, siano qualificabili come «sensibili». In questo senso a poco vale la distinzione che fanno sia i P.M. che le difese fra host provider e content provider: il proprietario o il gestore di un sito web che compia anche solo una di tali attività prima indicate senza possibilità di dubbio si trova nella scomoda posizione di chi «tratti» i dati che gli vengono consegnati e che lui gestisce e, quantomeno, diffonde nell'esteso mondo di internet.

Senza dubbio il content provider (e cioè il «gestore − produttore di contenuti») è in una posizione ancora più delicata, perché, in qualche modo, contribuisce a creare o comunque a far propri dei dati dallo stesso gestiti, ma, come si è detto e qui si ripete, anche l'Host provider (e cioè il mero intermediario) non è esente da comportamento oggettivamente inquadrabile nella norma, attesa la sua funzione, quantomeno, di diffusore dei dati raccolti. È evidente che questo comportamento può essere considerato colpevole ai fini della legge citata solo e soltanto se vi sia una coscienza e volontà dello steso: prima di arrivare alla valutazione del dolo specifico (di cui tra poco si parlerà) deve ritenersi che non possa essere considerato punibile chi raccolga, utilizzi o diffonda dati che egli, in buona fede, debba o possa considerare come «lecitamente raccolti» da altri. In questo senso l'IP (e cioè l'internet provider) che fornisca agli utenti un semplice servizio di interconnessione e che avvisi correttamente gli stessi degli obblighi di legge concernenti l'ottemperanza da parte dell'utente all'obbligo di legge citato. «Ad impossibilia nemo tenetur», e cioè non è possibile imporre a qualcuno un obbligo a cui egli non è in grado di fare fronte con i normali mezzi a sua disposizione: sarebbe del tutto impossibile pretendere che un IP possa verificare che in tutti i migliaia di video che vengono caricati ogni momento sul suo sito web siano stati rispettati gli obblighi concernenti la privacy di tutti i soggetti negli stessi riprodotti. È però necessario (ed è quindi legittimo richiedere il rispetto di tale comportamento) che l'IP fornisca agli utenti medesimi tutte le necessarie avvertenze in ordine al rispetto delle norme citate, con particolare attenzione a quelle che concernono la necessità di procurarsi l'obbligatorio consenso in ordine alla diffusione di dati personali sensibili.

Esiste quindi, a parere di chi scrive, un obbligo NON di controllo preventivo dei dati immessi nel sistema, ma di corretta e puntuale informazione, da parte di chi accetti ed apprenda dati provenienti da terzi, ai terzi che questi dati consegnano. Lo impone non solo la norma di legge (art. 13 d.lg. citato), ma anche il buon senso, nella particolare modulazione dello stesso che può applicarsi alla gestione di un sistema informatico. Per la verità, in questo particolare segmento di ricostruzione logica e giuridica del fatto, i P.M. 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'IP 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. Tale interpretazione viene corroborata con il richiamo al contenuto di una importante sentenza della S.C. (sez. III penale, n. 49437/09 del 23 dicembre 2009), in materia di responsabilità penale degli IP per quel che attiene il diritto d'autore; sentenza nella quale viene evidenziata una possibile partecipazione dell'IP al reato contestato agli uploaders (a titolo di concorso ex art. 110 c.p.) nel momento in cui il predetto non si limita ad una «messa a disposizione del protocollo di comunicazione» ma compie un quid pluris e cioè «...indicizza le informazioni che gli vengono dagli utenti... perché gli utenti possano orientarsi...

Chiedendo il downloading di quest'opera piuttosto che di un'altra... e quindi il sito cessa di essere un mero corriere che organizza il trasporto di dati... a quel punto l'attività di trasporto dei file non è più agnostica» consentendo una valutazione dell'apporto causale al reato lì contestato. Sulla base di tale interpretazione dovrebbe quindi ritenersi corresponsabile del reato di cui all'art. 167 d.lg. citato, quel tipo di IP che (come nel caso in esame) non si limiti a fornire un semplice rapporto di interconnessione, ma, gestendo i dati in suo possesso, ne divenga in qualche modo «dominus» e quindi «titolare del trattamento» ai sensi della legge, con gli obblighi corrispondenti.

Deve dirsi che questo tipo di impostazione accusatoria da un lato sembra richiedere un livello di approfondimento probatorio forse troppo elevato (quando un IP può con certezza definirsi un hoster attivo? quando può ritenersi esaurita la ricerca di quel quid pluris di cui parla la S.C.?), dall'altra esclude dal novero dei potenziali responsabili tutte le numerose platee degli host providers che, come si è cercato di dimostrare, non sembrano poter sfuggire alle ricadute concorsuali delle condotte di reato evidenziate. La normativa che punisce le violazioni del diritto d'autore non sembra, peraltro, di così facile trasportabilità nell'ambito del presente procedimento: l'oggetto della tutela, in quel caso, appare chiaramente ricollegabile alla mera condotta di caricamento del dato, di talché l'eventuale «apprensione » del dato medesimo da parte dell'ISP (sotto forma di indicizzazione dello stesso o altro) costituisce di per sé un concorso nel reato preesistente; nel caso in esame, invece, la violazione della legge è, per così dire, più nascosta, o comunque occultata nelle pieghe di un possibile comportamento altrui, e non può essere quindi «trasportata» nelle mani del provider solo e soltanto perché il dato viene gestito o organizzato dallo stesso. In parole più semplici il provider che indicizza dei testi coperti dal diritto d'autore che altri caricano e si scambiano, consentendone una commercializzazione più veloce e facile, certamente può essere ritenuto corresponsabile del reato contestato agli uploaders (così come indicato dalla S.C.); ma un provider che carica dei video contenenti dati sensibili di soggetti a cui non è stato richiesto il consenso, e li organizza e gestisce, non può essere ritenuto responsabile della mancata richiesta di consenso (nonostante la gestione dei dati in parola) se non viene provata la sua piena consapevolezza di tale mancanza; consapevolezza che, naturalmen-

te, può e deve derivarsi da una mancanza di segnali o di elementi significativi all'atto della prima comunicazione del caricamento.

A parere di chi scrive, comunque, il fatto che l'ISP faccia qualcosa di più del suo dovere di mero intermediatore (e cioè diventi un hoster attivo ouncontent provider, come anche può dirsi), è, una volta provato, certamente un elemento importante ai fini della ricostruzione delle ipotesi di reato contestate o contestabili, ma non trasforma, sic et simpliciter, l'ISP in un immediato realizzatore dei possibili reati emergenti dai dati caricati: non esiste, a parere di chi scrive, perlomeno fino ad oggi, un obbligo di legge codificato che imponga agli ISP un controllo preventivo della innumerevole serie di dati che passano ogni secondo nelle maglie dei gestori o proprietari dei siti web, e non appare possibile ricavarlo aliunde superando d'un balzo il divieto di analogia in malam partem, cardine interpretativo della nostra cultura procedimentale penale.

Ma, d'altro canto, non esiste nemmeno la «sconfinata prateria di internet» dove tutto è permesso e niente può essere vietato, pena la scomunica mondiale del popolo del web. Esistono, invece, leggi che codificano comportamenti e che creano degli obblighi, obblighi che, ove non rispettati, conducono al riconoscimento di una penale responsabilità. È pertanto ovvio che l'hoster attivo o il content provider che dir si voglia avrà certamente un livello di obblighi e comportamenti più elevato di quello di un semplice host provider o service provider o access provider: lo rende inevitabile il suo diventare «dominus» di dati che, per il solo fatto di essere organizzati e quindi selezionati e quindi «appresi», non sono più il flusso indistinto che non si conosce e che non si ha l'obbligo di conoscere; ma, tale fatto, non crea una specie di effetto a catena che fa dell'hoster attivo automaticamente il corresponsabile di tutti i reati che gli uploaders hanno commesso comunicando e caricando i dati in loro possesso. In tutti questi casi varranno, come in effetti valgono, le normali coordinate interpretative e valutative che si usano per ogni tipo di reato che il legislatore ha inteso codificare nel codice penale o nelle leggi complementari, sia da un punto di vista oggettivo che soggettivo.

E perciò, nel caso in esame, se è ben vero che un hoster attivo (come nel caso G. I.) ha sicuramente più elementi per poter riconoscere l'esistenza di un reato commesso da un singolo uploader, ed ha, inoltre, sicuramente degli obblighi che la legge gli impone per il trattamento dei dati sensibili dei soggetti che vengono «caricati» sul suo sito web, è altrettanto vero che non può essere imposto (perché irrealizzabile) allo stesso un obbligo generale e specifico di controllo su tutti i dati «sensibili» caricati (obbligo impossibile, se non altro, perché si imporrebbe ad un terzo la preventiva conoscenza di tutti i dati personali e particolari di tutte le persone che ogni momento «transitano» sul web); quello che, come si è detto, è imponibile allo stesso è un obbligo di corretta informazione agli utenti dei conseguenti obblighi agli stessi imposti dalla legge, del necessario rispetto degli stessi, e dei rischi che si corrono non ottemperandoli (oltre che, naturalmente, l'obbligo di immediata cancellazione di quei dati e di quelle comunicazioni che risultassero correttamente segnalate come criminose).

È peraltro evidente, perlomeno a parere di chi scrive, che NON costituisce condotta sufficiente ai fini che la legge impone, «nascondere» le informazioni sugli obblighi derivanti dal rispetto della legge sulla privacy all'interno di «condizioni generali di servizio» il cui contenuto appare spesso incomprensibile, sia per il tenore delle stesse che per le modalità con le quali vengono sottoposte all'accettazione dell'utente; tale comportamento, improntato ad esigenze di minimalismo contrattuale e di scarsa volontà comunicativa, costituisce una specie di «precostituzione di alibi» da parte del soggetto/web e non esclude, quindi, una valutazione negativa della condotta tenuta nei confronti degli utenti.

Da questo punto di vista, tornando alla valutazione del caso concreto, non può dubitarsi dei seguenti elementi conoscitivi e probatori: − G. I. costituiva la «mano operativa e commerciale» di G. Inc. in Italia; − attraverso il sistema AD Words ed il riconoscimento di parole chiave, G. I. aveva sicuramente la possibilità di collegare, attraverso la creazione di link pubblicitari, le informazioni riguardanti i clienti paganti alle schermate riguardanti G. V., e quindi, in qualche modo, gestire, indicizzare, organizzare anche i dati contenuti in quest'ultimo sito; − G. I., quindi, «trattava» i dati contenuti nei video caricati sulla piattaforma di G. V. e ne era quindi responsabili, perlomeno ai fini del d.lg. sulla privacy; − l'informativa sulla privacy, visualizzabile per l'utente dalla pagina iniziale del servizio G. V. in sede di attivazione del relativo account al fine di porre in essere il caricamento dei files da parte dell'utente medesimo, era del tutto carente, o comunque talmente «nascosta» nelle condizioni generali di contratto da risultare assolutamente inefficace per i fini previsti dalla legge. − Si veda, in questo senso, l'annotazione di P.G. della G.d.F. di Milano del 19 giugno 2008 (reperibili negli atti del P.M. faldone 11, n. 13, pp. 462/490), alla quale sono stati allegati i «termini e condizioni di servizio di G.», i «termini e condizioni del programma di caricamento di G.V.», «i punti salienti delle norme sulla privacy di G.» datate 14 ottobre 2005, «le norme sulla privacy di G.» datate 14 ottobre 2005, agli indirizzi web ricollegati ai servizi in questione: tutte le informazioni comunicate all'utente relative alla Privacy fanno riferimento, senza possibilità di dubbio, alla tutela della privacy dell'utente medesimo, utente che accetta di sottoscrivere il contratto con G. e che carica il video (o qualsiasi altro dato o informazione) in suo possesso, senza fare alcun esplicito riferimento alla privacy di altre persone eventualmente presenti nel video o nel contenuto dell'uploading; è ben vero che al punto 9 dei «termini e condizioni del programma di caricamento di G. v.» si chiede all'utente di garantire che il contenuto «autorizzato» che sta caricando non violi «diritti o obblighi verso qualsiasi persona, inclusi... i diritti di privacy», ma l'avviso in questione, al di là della sua genericità ed astrattezza, è dato in modo «nascosto ed anonimo», quasi a garantirsi (come si è già detto) la presenza di un alibi in un eventuale momento successivo di contrasto. Ad assoluta riprova di quanto fin qui riferito, nel momento in cui l'utente più attento e testardo di altri avrebbe voluto compulsare «i punti salienti della normativa sulla privacy di G.» avrebbe scoperto, al punto 2 della medesima («Quali sono i dati personali e gli altri dati che raccogliamo») che «G. raccoglie dati personali

quando vi registrate per accedere ad un servizio G....»: non vi è chi non veda che chiunque legga questa frase non può che pensare ai «propri» dati personali e non certo a quelli delle persone incautamente citate o riprese nei «contenuti autorizzati». − Il fine di profitto (richiesto dalla norma specificamente per la sussistenza del dolo) era, evidentemente, ricollegabile alla interazione commerciale ed operativa esistente tra G. I. e G. V., interazione derivante dalla operatività del sistema AD Words e dal collegamento esistente tra le keywords (parole chiave) utilizzate in quest'ultimo ed il sito web ospitante i video (vedi, sul punto, le precise risultanze di indagini effettuate dai P.M. e riportate nella parte iniziale della presente motivazione).

− Si vedano inoltre, ad ulteriore riprova di quanto fin qui riferito, le affermazioni di G. contenute nel punto 17 dei «termini di servizio e condizioni di contratto»: «alcuni dei servizi sono finanziati dalle pubblicità e possono visualizzare pubblicità e promozioni. Queste pubblicità possono avere come oggetto il contenuto di informazioni memorizzate nei servizi...» nonché il punto 3 dei «termini e condizioni del programma di caricamento di G. V.»: «G. può rendere disponibile... uno o più link al sito web specificato dall'utente ... in relazione a qualsiasi messa a disposizione dei contenuti autorizzati, e rendere disponibili i link ai siti web di rivenditori commerciali di terzi in cui, eventualmente, è possibile acquistare i contenuti autorizzati».

− L'esistenza di tutti questi «indici rivelatori» di tipo fattuale e documentale dimostra, a parere di chi scrive, una chiara accettazione consapevole del rischio concreto di inserimento e divulgazione di dati, anche e soprattutto sensibili, che avrebbero dovuto essere oggetto di particolare tutela; non solo, ma anche dell'interesse economico ricollegabile a tale accettazione del rischio e della chiara consapevolezza di quest'ultimo. In parole semplici: non è la scritta sul muro che costituisce reato per il proprietario del muro, mail suo sfruttamento commerciale può esserlo, in determinati casi ed in presenza di determinate circostanze. Per queste ragioni non può esservi dubbio in ordine al riconoscimento della responsabilità penale degli imputati in relazione al reato contestato sub B (illecito trattamento di dati personali e sensibili): le risultanze probatori e ottenute ed utilizzabili permettono la ricostruzione del fatto/ reato così come contestato dai P.M. nel decreto di citazione diretta e ne impongono la conseguente valutazione di responsabilità penale in termini di colpevolezza. Nemmeno può esservi dubbio in ordine alla corretta identificazione degli imputati come responsabili del reato contestato in quanto funzionalmente incardinati nei loro rispettivi ruoli amministrativi e gestionali delle società in questione (vedi le considerazioni svolte dall'ufficio del P.M. nella memoria riportata pagg. 36/51, considerazioni ed argomenti fattuali che non appaiono scalfiti dal contenuto delle dichiarazioni spontanee rilasciate dagli imputati ed allegate dalle difese nella loro memoria di replica conclusiva).

3. Il capo di imputazione sub A: il concorso nel reato di diffamazione. Quanto fin qui esposto in termini di responsabilità penale del IP (Internet provider) e di possibile prospettabilità della stessa in termini generali ed astratti secondo le

normali regole del diritto penale vigente, può essere dato per accertato. Il ragionamento fin qui riportato deve, ovviamente, essere calato nell'ambito del capo di imputazione riportato sub A, e cioè il concorso omissivo (ex art. 40 cpv. c.p.) degli imputati nel reato di diffamazione commesso ai danni del D.L. e dell'Associazione V.D.; reato commesso ai sensi degli artt. 595 commi 1 e 3 (con ogni altro mezzo di pubblicità) c.p. in primis dalle persone apparse nel video in questione in qualità di primi autori dell'atto di bullismo mediatico ai danni del D.L. medesimo e della associazione citata. Il discorso che deve qui affrontarsi non può che partire dalla disamina del video contestato in quanto, a seguito della remissione di querela dei D.L. e quindi alla sentenza di improcedibilità emessa, i difensori degli imputati hanno evidenziato una carenza di offensività dei comportamenti dei soggetti agenti nei confronti della parte lesa residua (e cioè l'Associazione V.D.), la cui reputazione non sarebbe stata offesa dalle parole pronunciate e dalle condotte tenute. Le difese motivano tale affermazione sostanzialmente facendo rilevare che le parole pronunciate dal ragazzo, che appare nel video come «persecutore» della parte offesa D.L., sono evidentemente dette ioci causa da persona che non faceva parte dell'associazione e che, quindi, nessuna lesione effettiva della reputazione di quest'ultima è deducibile dai comportamenti in questione.

È bene ricordare che il contesto complessivo in cui si svolgono le azioni riportate nel video è quello di un'aula scolastica, e che il ragazzo citato dice, nel corso dello stesso, le seguenti parole: «Salve, siamo dell'Associazione V.D.; un nostro mongolo si è cagato addosso, e mò non sappiamo che minchia fare, perché l'odore di merda ci è entrato nelle narici» accompagnando tali espressioni con numerosi ed odiosi atti di vessazioni nei confronti della parte lesa. Deve preliminarmente rilevarsi che è proprio la serie di comportamenti complessivi che vengono effettuati ai danni del ragazzo disabile (e non solo le parole citate) che evidenziano un atteggiamento dei responsabili del fatto che non può essere ridotto ad un «gioco», per quanto «cattivo» esso possa essere ritenuto: in questo senso questo giudicante, pur comprendendo le ragioni che sottendono alle affermazioni contenute nel provvedimento del T.M. di Torino sul punto, si permette di osservare che tali affermazioni appaiono riduttive della gravità del fato e non ne esprimono la compiuta carica lesiva.

Di gioco si sarebbe trattato (anche se gioco pesante) se le parole fossero rimaste tali e non fossero state accompagnate da gesti inequivocabili e da comportamenti assolutamente vessatori e violenti nei confronti della parte lesa, il quale rimane numerosi (ed interminabili) minuti in balia dei suoi persecutori che lo deridono, lo spingono in un angolo, gli gettano addosso carte ed epiteti assolutamente gravissimi. In breve, non sembra a questo giudicante di essere in presenza di un «gioco tra ragazzi», ma di qualcosa d'altro, di una serie di atti di persecuzione di una persona solo perché «diversa», atti nella sequenza dei quali le parole diffamatorie sono solo una piccola parte della violenza complessiva. In questo senso anche la citazione dell'associazione V.D. come «responsabile» del fatto in questione appare tutt'altro che priva di elementi diffamatori, costituendo

una evidente denigrazione di tutto l'universo down, comprensivo anche di quella parte di quel mondo che dovrebbe occuparsi della tutela dello stesso.

Non esiste, quindi, dubbio, a parere di questo giudicante, della portata e valenza diffamatoria del fatto (nel suo complesso) a danno della parte lesa V.D. Detto questo, ed esclusa la questione difensiva per l'improcedibilità per difetto di querela a cui questo giudice ha già esaurientemente risposto nella prima ordinanza di questo procedimento (a cui si fa integrale riferimento), si può passare a trattare il tema centrale della prospettazione accusatoria. L'ufficio dell'accusa, infatti, ha costruito (con innegabile perizia) un capo di imputazione strutturato in modo tale da consentire una possibilità di concorso nel reato di cui all'art. 595 c.p. (commesso, come si è detto, in primis, dai ragazzi apparsi nel video) anche ai responsabili del sito web (G.V.it) dove il video è stato poi caricato (uploading dell'8 settembre 2006), facendo derivare un obbligo giuridico di controllo dei contenuti del video in questione dall'omissione del corretto trattamento dei dati personali della parte lesa D.L., omissione già affrontata nella disamina del capo B di imputazione.

Per la verità i P.M., nel corso della loro requisitoria e nelle memorie finali presentate, dicono anche qualcosa di più rispetto alla formulazione del capo di imputazione: che cioè i responsabili di G. indicati come imputati, essendo G.V., a cui G.it aveva accesso tramite il sistema ADwords, una piattaforma web qualificabile come hoster attivo o come content provider, avevano un obbligo preventivo di controllo sul contenuto dei video caricati e «fatti propri», e che non avrebbero attivato tutti i possibili «filtri» che la tecnologia prevede in casi del genere per controllare i video, limitandosi ad un sistema di controllo successivo degli stessi solo in seguito alla segnalazione degli utenti (flag in). Da un lato, quindi, i P.M. ritengono l'esistenza di una posizione di garanzia a carico del sito web in parola, posizione derivante da un obbligo giuridico contenuto nella legge sulla privacy; dall'altro si spingono a costruire tale posizione come causativa di un obbligo «preventivo» di controllo sui video caricati sul sito, di talché l'aver lasciato sul sito G.V. il video in questione per un periodo di quasi due mesi (8 settembre/7 novembre 2006) senza rimuoverlo costituirebbe una evidente compartecipazione omissiva nel reato di diffamazione. Le difese degli imputati hanno rigettato con forza tale costruzione affermando l'inesistenza di tale obbligo giuridico di controllo preventivo e rilevando come l'attività dei responsabili di G.V. nella vicenda in esame sia da considerarsi priva di qualsiasi profilo di responsabilità penale, avendo gli stessi rimosso il video incriminato nell'arco di 24 ore dalla prima segnalazione pervenuta. Prima di affrontare la disamina della questione «in diritto» qui evidenziata, occorre, molto brevemente, raccontare quello che è successo «in fatto» nella vicenda in questione: − il video viene girato nella classe di un Istituto Tecnico di Torino in data 24 maggio 2006; − tra l'8 e il 10 settembre 2006 il video viene caricato su G.V. (da tale G.L., che non risulta imputata nel presente procedimento); − il video, nel corso dei due mesi successivi, viene visualizzato dagli utenti del sito 5500 volte, prendendo il primo posto tra i video più divertenti ed il ventinovesimo tra i video più scaricati;

− in data 5 novembre 2006 il «blogger» D'A. A. segnala sul suo blog (giornalettismo: il cannocchiale.it) la presenza del video sul sito (non è chiaro se egli abbia anche inviato una segnalazione a G.V. sulla inopportunità della presenza del video, come afferma, o comunque se la sua segnalazione sia stata correttamente recepita); − in data 6 novembre tale S.B. richiede la rimozione del video tramite il Centro di assistenza di G.; − in data 7 novembre la Polizia Postale di Roma richiede la rimozione del video; − in data 7 novembre 2006 il video viene rimosso.

Sulla base di tali evidenze fattuali e di quanto poi ricostruito dai P.M. nel corso delle indagini preliminari, può affermarsi quanto segue: − dal momento della sua immissione nel circuito comunicazionale di internet il video è stato messo a disposizione di un numero indeterminato di utenti (quantomeno 5500, così come risulta dal numero degli accessi al sito, ma tale valutazione deve ritenersi minimale attesa la possibilità di ulteriore comunicazione a terzi del video preventivamente scaricato − effetto virologico della comunicazione sul sito —); − secondo la costante giurisprudenza della S.C. essendo la diffamazione un reato di evento, esso si consuma «nel momento e nel luogo in cui i terzi percepiscono l'espressione ingiuriosa e dunque, nel caso in cui frasi o immagini lesive siano state immesse sul web, nel momento in cui il collegamento viene attivato» (Cass., sez. V, n. 25875 del 21 giugno 2006); − per impedire la commissione del fatto (e, in particolare per evitare che la condotta lesiva sfoci nell'evento del reato) il soggetto/web proprietario o gestore del sito avrebbe dovuto «impedire l'evento» e cioè controllare preventivamente il contenuto della comunicazione, non ammettendone il caricamento a motivo della presenza, all'interno dello stesso di frasi ed espressioni ingiuriose e diffamatorie; − tale fatto (e cioè il controllo preventivo del video) non è avvenuto, tanto è vero che il video è stato presente sul sito web per quasi due mesi; − il video è stato rimosso soltanto all'esito di una doppia segnalazione (privato, Polizia postale), in un tempo ragionevolmente rapido dal ricevimento delle stesse (24 ore circa).

Secondo i P.M., come si è detto, la responsabilità degli imputati deriverebbe dal mancato controllo (preventivo) sul contenuto del video, agli stessi addebitabile in virtù della posizione di garanzia rivestita dal «content provider» nei confronti del trattamento dei dati personali dei soggetti contenuti negli uploading degli utenti: dicono cioè i P.M. che l'omesso controllo del corretto trattamento dei dati personali contenuti nel video, avrebbe causato l'evento del reato contestato, che altrimenti non sarebbe avvenuto (o sarebbe avvenuto con minor danno da diffusione per la persona offesa). Ricavano tale convincimento dal fatto che, essendo il «content provider» un produttore o gestore di contenuti, la illiceità del contenuto si propagherebbe al gestore medesimo in virtù del ricordato principio collegato alla posizione di garanzia (principio riaffermato, a loro dire, dalla sentenza della S.C. in tema di diritti d'autore già ricordata). L'assunto dell'accusa non può essere condiviso.

Come si è già affermato nel corso di questa motivazione: «non esiste, a parere di chi scrive, perlomeno fino ad oggi, un obbligo di legge codificato che im-

ponga agli ISP un controllo preventivo della innumerevole serie di dati che passano ogni secondo nelle magie dei gestori o proprietari dei siti web, e non appare possibile ricavarlo aliunde superando d'un balzo il divieto di analogia in malam partem, cardine interpretativo della nostra cultura procedimentale penale.». La presenza di una «posizione di garanzia» da cui derivi un obbligo di attivazione in mancanza del quale ricorre la previsione del cpv. dell'art. 40 c.p., non può essere frutto di una seppur ingegnosa costruzione giurisprudenziale, ma, come insegna la S.C., deve derivare da «da un lato, da una fonte normativa di diritto privato o pubblico, anche non scritta, o da una situazione di fatto per precedente condotta illegittima, che costituisca il dovere di intervento, dall'altro lato, dall'esistenza di un potere giuridico, ma anche di fatto, attraverso il corretto uso del quale il soggetto garante sia in grado, attivandosi, di impedire l'evento» (Cass., sez. IV, n. 32298 del 6 luglio 2006).

Non appare quindi conforme a tali prescrizioni (ma anche alla possibilità logica ed umana di intervento sulla rete) far derivare l'esistenza di tale obbligo di intervento dalla violazione di una legge che non abbia per oggetto tali condotte e che sia stata emanata a copertura di comportamenti diversi da quello contestato. In altre parole, pur non essendovi dubbio che il gestore o proprietario del sito web qualificabile come «content provider» possa e debba essere ritenuto potenzialmente responsabile della violazione del d.lg. sulla privacy (per le ragioni che si sono esposte precedentemente e che trovano un appiglio diretto alla esistenza di una norma specifica), non appare conforme alle situazioni di fatto e di diritto finora esistenti, renderlo per ciò solo corresponsabile di altro reato di diffamazione (ma non solo) derivabile dal contenuto del materiale caricato.

Non lo consente sia l'attuale formulazione legislativa sul punto (che non prevede l'esistenza di una norma di controllo generale sugli ISP) sia la logica fattuale da applicarsi al caso concreto. Ed infatti, pur ammettendo per ipotesi che esista un potere giuridico derivante dalla normativa sulla privacy che costituisca l'obbligo giuridico fondante la posizione di garanzia, non vi è chi non vede che tale potere, anche se correttamente utilizzato, certamente non avrebbe potuto «impedire l'evento» diffamatorio. In altre parole anche se l'informativa sulla privacy fosse stata data in modo chiaro e comprensibile all'utente, non può certamente escludersi che l'utente medesimo non avrebbe caricato il file video incriminato, commettendo il reato di diffamazione. In realtà i P.M., nel costruire la loro (come si è detto, ingegnosa) ipotesi accusatoria, hanno, in un certo senso, detto meno di quello che in effetti hanno pensato: perché la costruzione di una posizione di garanzia impone al soggetto nei cui confronti viene affidata, un obbligo «preventivo» di impedire l'evento e non un generico obbligo di farne cessare gli effetti già avvenuti. Per cui, nell'ipotesi in esame, l'obbligo del soggetto/web di impedire l'evento diffamatorio, imporrebbe allo stesso un controllo o un filtro preventivo su tutti i dati immessi ogni secondo sulla rete, causandone l'immediata impossibilità di funzionamento.

Considerata l'estrema difficoltà tecnica di tale soluzione e le conseguenze che ne potrebbero derivare, si è quindi in presenza di un comportamento «inesi-

gibile», e quindi non perseguibile penalmente ai sensi dell'art. 40 cpv. c.p. In breve, la «torsione» esegetica che i P.M. fanno nella lettura ed applicazione dell'art. 167 d.lg. n. 197 del 2003, non può essere accolta o considerata applicabile nella vicenda in questione. La responsabilità penale degli ISP, mancando una precisa legislazione in materia che li equipari alle produzioni stampate o alle reti televisive, non può essere costruita al di là dei canoni interpretativi ed applicativi dell'attuale quadro normativo (quadro a cui si è recentemente aggiunta la Legge sul commercio elettronico − d.lg. n. 70 del 2003 − che, tuttavia appare applicabile soltanto agli host provider e nei limiti oggettivi identificati dalla stessa).

Sarà possibile considerarli responsabili dei contenuti dei file sugli stessi caricati (soprattutto nel caso si tratti di hoster attivi o content provider) solo nel momento in cui si provi la consapevolezza del fatto delittuoso, al di là della esistenza di posizioni di garanzia non mutuabili da altri settori dell'ordinamento. Per esempio, nel caso in questione, l'ufficio dell'accusa vi è andato molto vicino (si ripete, al di là della esistenza della posizione di garanzia): il fatto, indubitabile, che il video sia stato presente sul sito web per due mesi e che lo stesso sia stato inserito nei video più divertenti e più «cliccati» dagli utenti (sic!) già costituisce un principio di prova della «consapevolezza» da parte dei gestori del suo contenuto; principio che non ha raggiunto la pienezza della prova solo per l'estrema difficoltà dell'effettuazione degli indagini (e della ricostruzione del dolo del soggetto agente) che aprire le cataratte della libertà assoluta e senza controllo non costituisce un buon esercizio del principio di responsabilità e di correttezza, che sempre dovrebbe presiedere alle attività umane (anche se esercitate nel mondo «parallelo» di internet). Perciò, 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 dal reato di cui al capo A, reato che, così come formulato, non sussiste.

4. Il trattamento sanzionatorio. Agli imputati riconosciuti colpevoli del reato sub B possono essere concesse le attenuanti generiche: lo consente sia la loro incensuratezza, sia il buon comportamento processuale complessivamente tenuto (la rimozione del video incriminato è comunque avvenuta in tempi brevi della richiesta del privato e della polizia postale; gli stessi hanno pagato un risarcimento del danno —per il capo A—alle parti lese maggiormente colpite dalla vicenda in questione). Va, inoltre, concessa la diminuente del rito abbreviato. La pena base, contenuta per tutti nei minimi edittali di un anno, va quindi ridotta a mesi 9 per le generiche e da mesi 6 per il rito. Può essere concessa a tutti la sospensione condizionale della pena, sussistendone i presupposti di legge. Anche la pena accessoria della pubblicazione della sentenza è prevista ex lege (art. 172 d.lg. n. 196 del 2003). 5. Considerazioni finali. La grande (ed inaspettata) ricaduta mediatica di questo procedimento e della sua sentenza finale di primo grado, impone a questo giudicante una breve chiosa conclusiva: − verrebbe da dire, parafrasando il titolo di una famosa commedia di Shakespeare, «too much ado

about nothing (molto rumore per nulla)»; e cioè non sembra, a questo giudice, di aver alterato in modo sensibile i parametri valutativi e giurisdizionali che presiedono alla decisione di casi quali quello trattato (si vedano, in particolare, come riferimento le motivazioni delle sentenze del Tribunale penale di Milano del 28 marzo 2004 e del Tribunale civile di Lucca del 20 agosto 2007).

− La condanna del webmaster in ordine al reato di illecito trattamento dei dati personali, infatti, non viene qui costruita sulla base di un obbligo preventivo di controllo sui dati immessi, ma sulla base di un profilo valutativo differente che è, come detto, quello di un insufficiente (e colpevole) comunicazione degli obblighi di legge nei confronti degli uploaders, per fini di profitto. − il d.lg. sulla privacy (legge attualmente vigente in Italia) «copre» in modo legislativamente completo i comportamenti di chi si trovi nella situazione di «maneggiare» dati sensibili, e quindi non può essere trascurato nel momento in cui se ne appalesi la possibilità di intervento. − La distinzione tra content provider e service provider è sicuramente significativa ma, allo stato ed in carenza di una normativa specifica in materia, non può costituire l'unico parametro di riferimento ai fini della costruzione di una responsabilità penale degli internet providers.

− Tuttavia questo procedimento penale costituisce, a parere di chi scrive, un importante segnale di avvicinamento ad una zona di pericolo per quel che concerne la responsabilità penale dei webmasters: non vi è dubbio che la travolgente velocità del progresso tecnico in materia consentirà (prima o poi di «controllare» in modo sempre più stringente e attendo il caricamento dei dati da parte del gestore del sito web, e l'esistenza di filtri preventivi sempre più raffinati obbligherà ad una maggiore responsabilità chi si troverà ad operare in presenza degli stessi; in questo caso la costruzione della responsabilità penale (colposa o dolosa che sia) per omesso controllo avrà un gioco più facile di quanto non sia stato nel momento attuale. − In ogni caso questo giudice, come chiunque altro, rimane in attesa di una «buona legge» sull'argomento in questione: internet è stato e continuerà ad essere un formidabile strumento di comunicazione tra le persone e, dove c'è libertà di comunicazione c'è complessivamente più libertà, intesa come veicolo di conoscenza e di cultura, di consapevolezza e di scelta; ma ogni esercizio del diritto collegato alla libertà non può essere assoluto, pena il suo decadimento in arbitrio. E non c'è peggior dittatura di quella esercitata in nome della libertà assoluta: «legum servi esse debemus, ut liberi esse possumus» dicevano gli antichi e, nonostante il tempo trascorso, non si è ancora arrivati a scoprire una definizione migliore.

P.Q.M.

- dichiara D.D.C., DL.E.G., F.P. colpevoli del reato di cui al capo B della rubrica e, concesse agli stessi le attenuanti generiche e la diminuente del rito, li condanna Alla pena di mesi 6 di reclusione ciascuno, oltre al pagamento delle spese processuali. Pena sospesa per tutti. Visto l'art. 172 d.lg. 30 giugno 2003, n. 196 dispone a cura e spese dei medesimi imputati, la pubblicazione della presente sentenza, una sola volta e per estratto, sui quotidiani «Il Corriere della Sera», «La Repubblica» e «La Stampa». Visto l'art. 530 c.p.p. assolve D.D.C.,

D.L.R.G., F.P. e D.A. dal reato di cui al capo A della rubrica, perché il fatto, così come per gli stessi contestato, non sussiste. Indica in giorni 90 il termine di deposito per la motivazione della presente sentenza.

Google v. ViviDown. Responsabilità "assolute" e fine di Internet?

di Giuseppe Cassano (*)

Il presente saggio costituisce la trascrizione del video intervento - il giorno successivo al deposito della sentenza in esame - di Giuseppe Cassano, direttore della Rivista Diritto dell'Internet e delle nuove tecnologie e Direttore del Dipartimento di Scienze Giuridiche della European School of Economics.

Il caso

La video ripresa acquisita con un cellulare delle molestie ai danni di un ragazzo down perpetrata a scuola da alcuni compagni di classe è stata caricata sulla piattaforma Google Video e così diffusa a una quantità indeterminata di altri utenti. La particolare crudezza dell'episodio e il riferimento sprezzante all'associazione (Vivi Down) che si occupa dei ragazzi con questo tipo di problemi ha destato lo sdegno nel mondo digitale. Appena si è assunta la consapevolezza dell'accaduto sono scattate le denunce alla Procura della Repubblica, sia da parte dell'associazione, sia da parte del padre del ragazzo coinvolto. I responsabili materiali del filmato e dell'upload alla piattaforma di Google Video, appresa la notizia dai giornali, si sono autodenunciati ad un'insegnante. Il citato filmato veniva rimosso da Google Video a circa due mesi di tempo dalla sua inserzione on-line e a ventiquattrore ore di distanza dal momento in cui un privato cittadino ed un agente di P.S. formalmente avvisavano la redazione del noto motore di ricerca della presenza del video *de quo* nel proprio spazio virtuale di competenza.

Le condotte contestate agli amministratori di Google

I capi di imputazione contro gli amministratori della *net company* si sostanziano in concorso omissivo nel reato di diffamazione e nel reato di trattamento illecito di dati sensibili.

Mentre il primo capo di imputazione non trova accoglimento, gli amministratori-imputati vengono, invece, condannati per il reato di cui all'art. 167 D.lgs. 196/2003.

Invero, le questioni sottese ai capi d'imputazione formulati sono, come del resto considera lo stesso Giudice, strettamente interdipendenti, in quanto la configurabilità del concorso omissivo nel delitto di diffamazione dipende dall'idoneità del sistema normativo in tema di privacy a fondare un obbligo giuridico, a carico del titolare del trattamento dei dati, volto ad evitare eventi, quali quelli imputati a Google.

Sullo sfondo di tutte le considerazioni che la vicenda in oggetto suggerisce, si attagliano due questioni che a ben vedere rappresentano l'imprescindibile presupposto per definire correttamente gli eventuali profili di responsabilità degli amministratori della net company.

(*) In *Vita Notarile*, 2010, 579.

Da una parte, vi è la tanto discussa (in processo) qualificazione di Google alla stregua di un *hoster provider* o di un *content provider* (distinzioni classificatorie dalle quali, in un primo momento, il Giudice sembra prescindere ai fini della configurabilità del delitto di trattamento illecito dei dati personali, per poi attribuirle (pare), nel proseguo della motivazione, significato dirimente per la condanna degli imputati). Dall'altra parte, vengono in rilievo le interrelazioni tra gli ambiti di applicazione della disciplina della *e-commerce*, di cui al D.lgs. 70/2003 e la normativa sulla *privacy*, delineata dal D.lgs. 169/2003.

Anticipando le conclusioni a cui perviene il Giudice, il motore di ricerca Google viene qualificato non un semplice intermediario, ma un *content provider*.

La condotta penalmente rilevante che viene riconosciuta in capo ai responsabili di Google Italia s.r.l. sarebbe quella di aver gestito il servizio offerto da Google Video, omettendo di fornire (colpevolmente) ai propri inserzionisti telematici chiare e puntuali informazioni sulla corretta modalità del trattamento dei dati personali, con riferimento a quei dati appartenenti alle persone che compaiono nel video, diverse da quelle che tale video hanno immesso nella rete; avrebbero fatto ciò al fine di raccogliere un numero sempre più elevato di filmati per accrescere l'interesse al servizio da parte di eventuali acquirenti di spazi pubblicitari su Internet, in tal modo concretizzandosi il dolo specifico richiesto dall'art. 167 D.lgs. 196/2003.

Una prima riflessione: il (benvenuto) tradimento delle (non auspicabili) aspettative suscitate dalla lettura del dispositivo.

La lettura della sentenza, in esame, ben 111 pagine, lascia certamente sconfortati, venendo in mente quanto Schopenhauer diceva dei filosofi del suo tempo: «Secondo il metodo omeopatico, un minimo insignificante di pensiero viene diluito in un profluvio di parole e si continua così tranquillissimi a cianciare di pagina in pagina, con una fiducia illimitata nella pazienza del lettore. Invano l'intelligenza condannata a questa lettura spera in pensieri autentici, solidi e sostanziali: essa spasima, spasima attendendo un qualsiasi pensiero - come il viaggiatore nel deserto d'Arabia sospira l'acqua - e dovrà morire di sete»

Tanto più se si considera che il relativo principio di diritto che viene affermato in sentenza e che costituisce la base giuridica su cui viene fondata la condanna degli amministratori di Google, al di là della correttezza o meno di quanto ritenuto, appare tradire le aspettative (o sconfessare le paure, a seconda del punto di vista in cui ci si pone) che la lettura del dispositivo aveva suscitato nell'opinione pubblica. Basti considerare che allo stesso Giudice, nella parte finale della sentenza, parafrasando una famosa commedia di Shakespeare, viene da dire "*too much ado about nothing*" (molto rumore per nulla).

In dottrina, peraltro, a mo di profezia infausta, ci si era anche spinti ad osservare: <<(…)Escludendo, infatti che tutto si riduca al fatto che nelle condizioni generali di Google non c'era o era carente l'informativa all'utente circa la necessità di acquisire il consenso del terzo ripreso prima di caricare il video, con-

siderato che vi erano dati sensibili - perché se così fosse saremmo di fronte ad uno di quegli inutili formalismi che invece di elevare la tutela della privacy, ne fanno scadere ogni sostanziale percezione tra i comuni mortali (non avvocati)>>.

In tale ottica, sembra che la costruzione di ingegneria giudica, abbastanza claudicante – come definita dal Garante Privacy – sia stata l'effetto di una pressione mediatica, e di una precomprensione del giudice, tale per cui a fronte di una richiesta di condanna per violazione della privacy e per diffamazione, un mimino di pena si sarebbe dovuta scontare, almeno sotto il profilo della "sanzione mediatica"; orbene, in questo ragionamento, nelle pieghe della disciplina della privacy, si scopre una norma che sembra funzionale al caso *de quo*.

Con ciò si raggiungono due obiettivi, il ragionamento di condanna autonomo del giudice (anche io sono in grado di rinvenire in determinati comportamenti un reato, con distinguo, quindi, dalle posizioni della procura, di cui in verità la sentenza costituisce per gran parte un "copia ed incolla"), l'irrogazione della sanzione che nella logica buoni/cattivi, deboli/forti, era giusto comminare.

La valutazione in diritto delle emergenze processuali

Dopo una prima parte che costituisce per lo più la fedele trasposizione degli atti d'indagine preliminare compiuti dall'organo d'accusa, la seconda sezione di cui è composta la motivazione si apre con una "valutazione in diritto delle emergenze processuali".

Il giudice premette che il ritiro della querela da parte dei familiari del ragazzo offeso limita l'accertamento ai fatti che riguardano la seconda parte lesa, l'associazione Vivi Down, ma non fa decadere l'imputazione del capo A (concorso omissivo nel reato di diffamazione), contrariamente a quanto sostenuto dalla difesa.

Quindi, risolve il problema della competenza territoriale, affermando che il reato è stato commesso anche a Milano, dove ha sede la società Google Italy "sotto il profilo del trattamento dei dati inteso come elaborazione e organizzazione degli stessi".

Sarebbe lungo esaminare tutti i passaggi del ragionamento del giudice. Limitiamoci, quindi, alle questioni più rilevanti che hanno dato luogo alla condanna e a quelle che possono avere conseguenze su una non impossibile futura regolamentazione delle attività *on line*. E anche sul precedente che la sentenza può costituire per altri giudizi su casi simili (pur nei limiti di una decisione di primo grado, contro la quale è già stato annunciato l'appello).

La questione processuale che merita di essere sottolineata in tale prospettiva riguarda la giurisdizione: la normativa sul trattamento dei dati personali si applica (art. 5 D.Lgs. 196/2003) ai trattamenti di dati personali "anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato" e anche "effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato anche di-

versi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea".

Dunque, venendo alla vicenda in esame, la prima parte del trattamento, cioè il caricamento del video, si svolge senza dubbio nell'ambito della giurisdizione italiana. Ma è stato giudicato in un altro processo.

Qui si discute solo della responsabilità di Google. E dalla ricostruzione fin troppo dettagliata compiuta dall'accusa, si evince che la rappresentanza italiana di Google non ha alcun ruolo nel trattamento: tutto è deciso negli USA. Dove non c'è alcun obbligo di rispetto della nostra normativa.

Tuttavia, il giudice arriva alla conclusione opposta, rifacendosi alla sentenza della Cassazione n. 49437 del 2009 (processo Pirate Bay), secondo la quale il *provider* concorre al reato di violazione del diritto d'autore nel momento in cui indicizza le informazioni. Ma le due situazioni non sono paragonabili, perché nel caso di Pirate Bay il processo di selezione e indicizzazione dei siti di *file sharing* è specificamente volto a fornire i link dai quali scaricare i contenuti illeciti, mentre nel caso di Google video c'è solo un'indicizzazione, passaggio strumentale indispensabile per raggiungere qualsiasi contenuto.

In ogni caso, il collegamento tra il trattamento effettuato negli USA e l'Italia consisterebbe, se ho letto bene la sentenza, nel "lucro" che deriva dalla pubblicità, per la quale l'azienda ha una rappresentanza nel nostro paese.

Qui si potrebbe aprire un'interminabile discussione sulla connessione tra il trattamento svolto all'estero e il lucro conseguito in Italia, ma non è questo il caso. Perché la difesa ha dimostrato che all'epoca dei fatti non c'era un collegamento diretto tra Google Video e la pubblicità e l'argomentazione appare convincente (ora, con Facebook la situazione è cambiata).

Dunque, basterebbe questo dato, l'assenza di lucro, per escludere la giurisdizione italiana, quindi l'applicabilità della normativa interna in tema di trattamento dei dati personali e, in ultima analisi, il reato contestato e ritenuto.

La portata dell'obbligo informativo ritenuto in tema di *data protection*: il cortocircuito evidenziato dalla sentenza

Venendo alla condotta ritenuta penalmente rilevante a carico degli imputati, il ragionamento che compie il giudice al fine di sostenere la condanna dei medesimi è che Google avrebbe dovuto informare i suoi utenti del fatto che se si pubblica il video che riguarda una terza persona, il consenso di quel terzo è necessario perché non ci sia reato.

Per il giudice questo non è avvenuto e soprattutto il trattamento del video attraverso l'indicizzazione, le classifiche di popolarità e il potenziale inserimento dei programmi pubblicitari di Google indica una "conoscenza" del video e questo complica la posizione dei responsabili. In particolare, questi elementi vengono valorizzati dal Giudice al fine di accertare in capo agli imputati una chiara accettazione consapevole del rischio concreto di inserimento e divulgazione di dati che avrebbero dovuto essere oggetto di particolare tutela.

Nonostante neghi la possibilità di un controllo preventivo, qui è come se il giudice chiedesse che "l'*hoster* attivo" (è scritto così nel testo) si faccia carico di rendere edotto tutto il suo potenziale pubblico della normativa sulla privacy. Obbligo informativo che, secondo quanto ritenuto dal Giudice, dovrebbe essere adempiuto non solo nei confronti di quella parte di pubblico che direttamente carica video nella rete, ma anche (e qui sta il principio inaccettabile della decisione *de qua*) in relazione a chiunque, in un modo o nell'altro, in quei video compaia o ne risulti in altro modo interessato.

Il giudice si rende conto che non si può chiedere un controllo diretto alle piattaforme e si rifugia, così, nel calcio d'angolo dell'avvertenza al pubblico. Questo sgraverebbe la responsabilità della piattaforma.

Insomma, l'omesso controllo o comunque una responsabilità colposa come per giornali e tv o una cosa che ci somigli. E allora ci vuole la censura preventiva, poteva dirlo prima, dottor Magi.

Quanto al dolo specifico richiesto per la configurabilità del reato contestato, il fine di lucro dell'ISP viene individuato nel servizio di AD Words, ovvero del software mediante cui si collegano a parole chiave immesse nella barra di ricerca i links ai siti commerciali logicamente collegabili, che abbiano fatto richiesta di inserzione. Gli inserzionisti pagano Google sulla base del metodo cosiddetto Pay per click. Si tratta di un corrispettivo in funzione della quantità di click eseguiti sul link del cliente.

In tal modo, però, al fine di configurare un profitto di Google, necessario per l'integrazione della fattispecie penale contestata, il giudice confonde la volontà dell'ISP con degli automatismi tipici della Rete e collegati al servizio AD Words che presenterà sicuramente dei difetti, ma di certo non quelli individuati dal magistrato.

Una volta argomentata l'esistenza della violazione delle norme privacy in punto di informativa, nel senso prima precisato, e verificata l'esistenza del profitto, il Giudice non può che concludere per il riconoscimento della responsabilità penale degli imputati per illecito trattamento di dati personali e sensibili.

Alla luce di quanto esposto, è difficile rintracciare nella decisione l'enucleazione chiara, puntuale e rigorosa di un solo principio idoneo a sorreggere l'impianto accusatorio

Google Italy, infatti - secondo il Giudice - sarebbe, in buona sostanza, responsabile di violazione della disciplina sulla privacy perché - nell'ambito di un'attività svolta con finalità lucrativa - non avrebbe avvertito in maniera sufficientemente chiara la ragazzina che ha caricato on line il video, della necessità di prestare attenzione al rispetto della privacy del protagonista - specie perché disabile - del proprio video.

Ma si può davvero ipotizzare che se Google nelle proprie condizioni generali di utilizzo del servizio avesse avvertito, in caratteri più grandi e magari in grassetto, una bambina di dodici anni dell'esigenza di assicurarsi il consenso al trattamento dei dati personali del bambino disabile protagonista del video caricato, questa vi avrebbe provveduto?

Personalmente credo di no, e sono in buona compagnia, perché lo stesso magistrato, qualche pagina più avanti, nel rigettare la tesi accusatoria che avrebbe voluto Google Italy responsabile anche di concorso in diffamazione, scrive testualmente "anche se l'informativa sulla privacy fosse stata data in modo chiaro e comprensibile all'utente, non può certamente escludersi che l'utente medesimo non avrebbe caricato il file video incriminato, commettendo il reato di diffamazione".

Difficile seguire la coerenza logica prima ancora che giuridica che lega i due passaggi della Sentenza: mi sfugge probabilmente qualcosa ma, l'impressione è che a pagina 96 il Giudice abbia ritenuto che se Google avesse dato correttamente l'informativa la ragazzina non avrebbe caricato il video incriminato, mentre a pagina 104 si mostri convinto del contrario, ovvero che lo avrebbe comunque caricato.

L'eccentrica interpretazione fornita del combinato disposto degli artt. 13 e 23 D.lgs. 196/2003

Ma fino a questo punto siamo ancora alle considerazioni di carattere generale. Alla fine della storia ci sono i reati contestati ai tre imputati. Questi consistono nella violazione degli articoli 23 (consenso), letto in combinato disposto con l'art. 13 (informativa), 17 (trattamento che presenta particolari rischi) e 26 (garanzie per i dati sensibili) del codice privacy.

La violazione dell'art. 23 è punita dal primo comma dell'art. 167 con la reclusione da sei a ventiquattro mesi.

L'art. 167 non contiene un'ipotesi penale per la violazione dell'art. 17, elencata nel capo di imputazione, ma solo per quella dell'art. 26, e la pena va da uno a tre anni.

In sostanza, i tre dirigenti di Google, secondo il giudice, avrebbero omesso (prima, di informare la persona che carica il video circa la necessità di chiedere e, quindi) di ottenere il consenso scritto dell'interessato (la persona danneggiata) per il trattamento dei dati sensibili.

Dunque avrebbero dovuto: a) controllare i contenuti del video prima di metterlo in rete; b) identificare e trovare l'indirizzo della persona ritratta; c) attendere il suo consenso scritto prima di dare il via libera alla diffusione.

Non vi è chi non veda come l'impostazione accolta si riveli del tutto errata da un punto di vista fattuale, ossia del contemperamento degli interessi in gioco nella situazione concreta, nonché assolutamente eccentrica nell'ottica dell'interpretazione delle norme giuridiche che sono state ritenute alla base della condanna degli amministratori di Google Italy.

In questo mondo reale, il grande beneficio recato da strumenti di diffusione e interazione informativa come Google Video devono e possono essere conciliati sinergeticamente con la protezione dei diritti umani. Eticamente, la strategia migliore non è instaurare un'autoritaria censura preventiva, che causerebbe un immenso danno al libero scambio delle informazioni e soffocherebbe una buona cultura della rete, ma censurare tempestivamente e fermamente chi non rispetta

le regole della convivenza civile online. In altre parole: applicare regole come quella del *safe harbor*, che fanno prosperare il nostro ambiente digitale e la cultura liberale che esso promuove, nonché attribuire il rilievo che merita al principio del *notice and takedown* (ossia, della rimozione del contenuto illecito dopo un'apposita segnalazione), perno fondante la normativa comunitaria e italiana sul commercio elettronico.

Dal punto di vista strettamente giuridico, la ricostruzione effettuata dal giudice nelle motivazioni non chiarisce affatto la possibile violazione derivante dagli artt. 17 e 26 D.lgs. 196/03, mentre è contraddittoria per quanto riguarda l'articolo 23 D.lgs. 196/03.

In relazione al disposto da ultimo citato, il Giudice si concentra sulla presunta mancanza di chiarezza nell'informativa sulla privacy, ai sensi dell'art. 13 D.lgs. 196/03, senza considerare che tale violazione non comporta una sanzione penale ai sensi dell'art. 167 D.lgs. 196/03, ma una mera sanzione amministrativa ai sensi dell'art. 161 D.lgs. 196/03.

Se da un lato, però, non ci si deve mai fermare di fronte alla prima lettura fatta in questi giorni e alcune considerazioni presenti all'interno della motivazione non permettono di banalizzare la questione in questi termini, dall'altro non si può certo dire che manchino gli aspetti problematici e che la ricostruzione effettuata sia convincente.

Pare, infatti, che alla base della decisione vi sia l'insofferenza per la mancanza di una legislazione di carattere internazionale che disciplini Internet e, quindi, le diverse attività illecite configurabili. A tal punto il giudice, per affermare la sua competenza e principalmente l'applicazione della normativa italiana ha dovuto subito individuare un illecito di rilevanza penale che incida così sul territorio italiano.

Al fine, però, di configurare un trattamento illecito di dati personali ha dovuto fornire una propria interpretazione estensiva dell'art. 13 del Codice per la protezione dei dati personali. Difatti, sapendo bene di non poter accusare Google di omesso controllo dei contenuti immessi in Rete da parte di terzi (non perché ciò non sia possibile tecnicamente, ma perché manca una norma esplicita in tal senso), ha ritenuto che l'informativa prevista dalla normativa sulla privacy doveva comunque essere ben presente sulla pagina web dove è disponibile il servizio di Google. Ciò perché l'Internet Service Provider (ISP) tratta i dati, sia pure nel solo segmento finale del processo, ed avrebbe avuto quindi l'obbligo di informare l'utente sui vincoli di legge da rispettare: cioè sul fatto che le persone riprese nel video dovevano essere avvertite e si doveva ottenere il loro consenso.

In pratica e a conclusione delle considerazioni in diritto sugli addebiti mossi agli amministratori-imputati, il giudice Magi legge l'articolo 23, in combinato disposto con l'art. 13, come se imponesse a YouTube l'obbligo di verificare se gli utenti abbiano ottenuto l'autorizzazione dei soggetti presenti nei filmati destinati a essere condivisi tramite la piattaforma.

Solo che in realtà l'articolo dice tutt'altro.

L'interessato al quale si riferisce il consenso è colui che ha un rapporto con il titolare del trattamento, cioè chi carica il video. Non la persona che ha tratto "nocumento" dal contenuto, che è un terzo nel rapporto tra il provider e il destinatario del servizio.

L'esigenza di un apporto di razionalità (normativa) alla risoluzione della questione in esame

Ma al di là delle considerazioni in diritto appena svolte e delle critiche avanzate al magistrato per la scarsa consapevolezza mostrata circa l'esistenza di regole sufficientemente in grado di realizzare un corretto bilanciamento tra i valori e le esigenze sottese alle dinamiche del mondo virtuale, rispetto agli insopprimibili diritti umani, in sintonia con il principio di *extrema ratio* del sistema penale, quello di cui appare maggiormente bisognosa la sentenza in esame è di un apporto di razionalità (normativa) che consenta di effettuare un corretto inquadramento normativo della vicenda in esame.

Come accennato, le questioni che si attagliano sullo sfondo del caso deciso dal Tribunale di Milano concernono i rapporti tra la disciplina della *data protection* e quella dell'*e-commerce*, da un lato, e la qualificazione giuridica di Google alla stregua di un *host* o *content provider*, dall'altro, onde definirne compiutamente il regime di responsabilità dello stesso.

A tal fine, appare opportuno partire di nuovo da quanto è stato ritenuto dal Giudice in sentenza, per poi svolgere le relative considerazioni.

L'*hoster* attivo, in cui alla fine viene identificato Google, ad avviso degli argomenti presentati dall'accusa e in parte condivisi dall'autorità giudicante è una figura sottratta all'applicazione della disciplina sul commercio elettronico (principio dell'irresponsabilità dell'intermediario) e sussunta nell'ambito della disciplina privacy (principio di responsabilità del titolare del trattamento) a causa del tipo di attività condotta.

Il motore di ricerca o *hoster attivo* non si limita a fornire un semplice rapporto di interconnessione, ma indicizzando i patrimoni informativi immessi da terzi finisce per eseguirne un vero e proprio trattamento.

Conseguentemente, nella mente del giudicante la disciplina del relativo operato abbandona l'ambito dell'*e-commerce* e rimane sottoposta al settore della *data protection*.

Si legge nella sentenza:

"Esiste quindi, a parere di chi scrive, un obbligo NON di controllo preventivo dei dati immessi nel sistema, ma di corretta e puntuale informazione, da parte di chi accetti ed apprenda dati provenienti da terzi, ai terzi che questi dati consegnano.. E' pertanto ovvio che l'*hoster* attivo avrà certamente un livello di obblighi e di comportamenti più elevato di quello di un semplice *host provider*".

Peraltro, occorre sottolineare che nel pensiero del Giudice, l'individuazione di una condotta oggettivamente inquadrabile in quelle sanzionate dalla normativa sulla *data protection* non è condizionata in alcun modo dalla possibilità di qualificare il motore di ricerca come *hoster* attivo. Secondo quanto emerge dalla

lettura di qualche pagina precedente il passo della sentenza appena riportato, la fattispecie delittuosa ben può concretizzarsi in capo al soggetto che si trovi "nella scomoda posizione di chi tratti i dati che gli vengono consegnati e che lui gestisce e, quantomeno, diffonde nell'esteso mondo di internet", a prescindere dalla sua qualificazione in termini di *host provider* o *content provider*.

"In questo senso a poco vale la distinzione che fanno sia i PM che le difese fra *host provider* e *content provider*… Senza dubbio il *content provider* (e cioè il "gestore – produttore di contenuti") è in una posizione ancora più delicata, perché in qualche modo, contribuisce a creare o comunque a far propri dei dati dallo stesso gestiti, ma, come si è detto e qui si ripete, anche l'*host provider* (e cioè il mero intermediario) non è esente da comportamento oggettivamente inquadrabile nella norma, attesa la sua funzione, quantomeno, di diffusore dei dati raccolti".

A questo punto, preso atto di quanto ritenuto in sentenza, i quesiti a cui rispondere per inquadrare correttamente dal punto di vista normativo la vicenda in questione sono i seguenti:

- E' impensabile che la presunta intelligenza della piattaforma- o il fine economico degli obiettivi perseguiti - ci conduca automaticamente nel settore della *data protection*?

- Non sarebbe forse più appropriato collocare la questione nell'ambito dei servizi della Società dell'Informazione, proponendoci di adeguare ai nuovi sviluppi della tecnologia la disciplina dell'*e-commerce*?

Ma l'ultima parte di questo interrogativo ci porterebbe di nuovo fuoristrada, in quanto la relativa considerazione andrebbe gestita sotto il profilo della sollecitazione normativa.

Venendo al fulcro della questione, invece, al fine di rispondere positivamente alla prima domanda è necessario partire dall'assunto che la normativa sulla *privacy* e la normativa sul commercio elettronico, in realtà, costituiscono un quadro giuridico coerente e completo e che quest'ultima non trova applicazione solo in caso di specifico contrasto con la normativa sulla *privacy* che non sussiste nel caso di specie, in quanto la normativa in materia di protezione dei dati personali non impone un qualsivoglia onere di controllo.

Per dimostrare tale affermazione è necessario muovere da alcune fondamentali considerazioni di carattere generale, ancor prima di affrontare la questione specifica.

Privacy e commercio elettronico rappresentano due macrocategorie del tutto indipendenti l'una dall'altra che possono avere punti di interconnessione in determinati casi.

In particolar modo, riguardo il commercio elettronico sappiamo bene che sia la Direttiva 2000/31/CE che lo stesso D.lgs. 70/03 parlano in termini ancora più generali di "servizi della società dell'informazione", facendovi rientrare tutte le attività economiche svolte "on line" e qualsiasi altro servizio prestato, normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi. Il commercio elettronico non trova, quindi, una

specifica definizione nel nostro ordinamento ed in quello europeo, ma viene fatto rientrare nella più ampia nozione di cui sopra. L'ampiezza e la varietà della nozione di commercio elettronico viene comprovata dal fatto che i contratti di *e-commerce* sono disciplinati innanzitutto dal nostro codice del consumo (D.lgs. 6 settembre 2005 n. 206), laddove non regolati dal d.lgs. 70/2003.

Dal predetto quadro normativo si apre lo scenario della struttura Internet.

Si tratta di una realtà complessa, cui confluiscono la maggior parte delle componenti che accompagnano la nostra quotidianità. Internet è un universo di servizi messi a disposizione dell'utente (gratuitamente o a pagamento). La rete non può essere annoverata unicamente nei media. La rete è anche un media, ma è soprattutto una realtà di servizi.

Per comprendere appieno la problematica, il dato da cui partire è costituito dall'autonoma rilevanza della tutela dei dati personali di cui l'*e-commerce* e le stesse comunicazioni elettroniche rappresentano uno specifico campo di applicazione.

Un importante argomento a favore di tale tesi viene fornito da Picotti – che singolarmente sembra essere l'Autore più citato dall'accusa - che nell'esaminare i rapporti tra Internet e diritto penale sostiene che spesso molte norme rilevanti in materia sono state emanate in attuazione di convenzioni, direttive, raccomandazioni di fonte europea e sovranazionale che hanno portato ad una molteplicità di interventi settoriali in cui le norme penali svolgono una funzione meramente "sanzionatoria" di precetti e discipline extrapenali, come: il diritto d'autore, la protezione delle topografie per semiconduttori, il trattamento dei dati personali, il commercio elettronico. Quindi, lo stesso Picotti riconosce l'indipendenza e la necessità del coordinamento delle due materie, con la precisazione relativa alla impossibilità del controllo delle informazioni, attesa la natura mutevole o sostanzialmente non gestibile delle informazioni messe in Rete.

Sulla stessa lunghezza d'onda si pone anche Bessone che, svolgendo un intervento di prima approssimazione sul mondo dell'*e-commerce*, ammette quanto siano numerosi i punti di interferenza tra normative che regolano materie diverse. Chiaramente, in tale ottica assume rilevanza anche la tutela della *privacy*, laddove viene in rilievo il sistema delle garanzie di protezione dei dati personali.

La opinione che più ci vede concordi è quella espressa - peraltro già da Noi sostenuta in più scritti - da un autorevole Studioso della materia, Draetta, esperto del diritto internazionale, che più volte ha affrontato le tematiche del diritto dell'Internet:

Secondo Draetta, la direttiva 2000/31 sul commercio elettronico intende sì favorire l'instaurazione di un mercato digitale unico, offrendo nello stesso tempo agli Stati membri un quadro normativo di riferimento per loro misure nazionali, ma al contempo prevede tutta una serie di esclusioni dall'ambito di applicazione della direttiva nel suo complesso, di eccezioni dall'ambito di applicazione dell'art. 3, nn 1 e 2 che pone il principio della libera circolazione dei servizio della società della informazione sulla base delle norme del paese di origi-

ne, e di possibilità per gli stati membri di introdurre deroghe all'art.3, n. 2, che si riferisce specificamente alla sola libera circolazione.

La formulazione di alcune esclusioni e deroghe - come all'unisono rilevato da tutti i commentatori – non risponde ad eccessive preoccupazioni di natura sistematica e presenta elementi molto disomogenei. Accanto ad esclusioni vere e proprie, come quella relativa al settore tributario, in alcuni casi i settori sono esclusi o derogati perché oggetto di apposita norma comunitaria relativa proprio ai servizi della società dell'informazione (come nel caso della moneta elettronica o dei servizi finanziari).

In altri casi, la non applicabilità riflette piuttosto la necessità di coordinamento con altre disposizioni comunitarie che intersecano a matrice quella del commercio elettronico, quali la tutela giuridica del diritto d'autore, delle banche dati e la tutela dei dati personali.

"L'esclusione di queste materie dall'ambito di applicazione della direttiva sul commercio elettronico va intesa, quindi, nel senso che tali materie sono disciplinate da altri atti comunitari, i quali restano pienamente applicabili in un ambito telematico, anche se relativi a campi più vasti di quello telematico, salvo che la direttiva qui in esame non preveda diversamente " (Draetta).

Il pensiero – condiviso - di questo Autore può essere ripetuto in relazione alle due normative di attuazione delle rispettive Direttive, con il particolare di seguito evidenziato.

Le normative di cui ci occupiamo *(non rientrano nel campo di applicazione del presente decreto […] le questioni relative al diritto alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle telecomunicazioni di cui alla legge 31 dicembre 1996, n. 675 e al decreto legislativo 13 maggio 1998, n. 171 e successive modifiche e integrazioni*), come noto, sono state entrambe abrogate dal d.lgs. n. 196/2003 - che oggi è il T.U. in materia di trattamento dei dati personali - il quale all'art. 6 d.lgs. 196/2003 ("Disciplina del trattamento") prevede che "le disposizioni contenute nella presente Parte si applicano a tutti i trattamenti di dati, salvo quanto previsto, in relazione ad alcuni trattamenti, dalle disposizioni integrative o modificative della Parte II". La Parte II del d.lgs. 196/03 prevede all'art. 133 una disciplina specifica per "Internet e reti telematiche" .

Aldilà delle questioni relative alla stesura di un Codice deontologico ex art. 133, possiamo certamente affermare come i fornitori di servizi di comunicazione e informazione offerti mediante reti di comunicazione elettronica siano tenuti al rispetto della normativa del decreto 196/2003 avuto riguardo alle modalità di raccolta e trattamento dei dati.

Nel senso che – ed è il cuore del problema – può/deve parlarsi di una questione di trattamento di dati personali esclusivamente in riferimento a quei dati presenti nelle BB.DD. dei fornitori di servizi di comunicazione e informazione offerti mediante reti di comunicazione elettronica che siano stati dagli stessi acquisiti (ad es. attraverso la fornitura dei propri dati da parte del titolare; l'acquisto di BB.DD. da parte di terzi).

E questo è l'unico significato coerente e plausibile che si possa dare all'art. 1, comma 2, lett. b) decreto 70/2003, ossia nel senso che il termine "questioni" deve intendersi riferito alle questioni insorte / insorgende tra fornitori di servizi di comunicazione e informazione offerti mediante reti di comunicazione elettronica, da un lato, e persone fisiche/giuridiche i cui dati personali siano stati inseriti nelle BB.DD dei primi.

E queste questioni effettivamente atterranno all'eventuale illegittimo trattamento di dati (ad es. perché raccolti senza il consenso; trattati - ceduti irregolarmente).

Venendo al caso in cui TIZIO inserisca su Youtube (o su Google video o altra piattaforma) un video che ritrae CAIO, senza il consenso di quest'ultimo, al più di una questione di trattamento di dati personali si potrà parlare tra TIZIO e CAIO.

Youtube (o Google Video o altro soggetto fornitore del servizio on line) non ha trattato dati personali di CAIO, al più ha raccolto i dati personali di TIZIO al quale avrà chiesto di compilare un form e di aderire a un Codice deontologico.

Per Youtube (o Google Video o altro soggetto fornitore di piattaforma on line) opera la normativa del d.lgs. 70/2003, con particolare riferimento al sistema della responsabilità.

In definitiva, per quanto concerne le Reti Telematiche si può così sintetizzare: la normativa sulla *privacy* disciplina il trattamento dei dati personali, la normativa sul commercio elettronico disciplina le forme di responsabilità.

Ritenere diversamente, significa abrogare una normativa a favore dell'altra sulla base di questo assunto.

Innanzitutto la normativa sulla *privacy* è norma che tutela sì i dati personali, ma al contempo tutti i diritti della personalità, in quanto per mezzo del dato personale tutti i diritti della personalità vengono in gioco. Ossia la violazione del diritto all'identità personale, all'onore, alla reputazione, all'immagine, e così a seguire, tutte le altre violazioni di diritti meritevoli di tutela che avvengono attraverso "l'utilizzo" del dato personale.

Per cui, nel momento in cui si affronta la responsabilità dell'intermediario attraverso la normativa sul commercio elettronico, pretendere la non operatività per presunta applicabilità esclusiva della normativa sulla *privacy* significherebbe sancire la assoluta non operabilità della normativa di specificazione delle forme di responsabilità degli intermediari.

Cioè, la specificazione delle forme di responsabilità degli intermediari si sostanzia in violazione dei diritti della personalità altrui; ma se tutte le questioni relative ai diritti della personalità sono demandate alla normativa sulla *privacy*, vi sarebbe a monte la in operabilità delle norme sugli intermediari.

Come a volere dire che il legislatore ha previsto delle norme che mai si potranno applicare (ossia la specificazione delle varie forme di responsabilità degli intermediari), perché qualcuno sostiene inopinatamente che questa normativa non si applica, a favore di una responsabilità che viene appaltata completamente alla normativa sulla *privacy*.

Non solo e siamo al secondo quesito. A Google Video va riconosciuta la qualifica giuridica di fornitore di servizio di hosting esattamente come il Tribunal di Grande Istanza di Francia Parigi, 29 ottobre 2007 ha fatto con riferimento a Wikipedia.

Difatti, pur dovendo riconoscere che nel 2000 (data dell'approvazione della direttiva 31/00/CE sul commercio elettronico) e nel 2003 (data della trasposizione in Italia della medesima direttiva con il D.lgs. 70/03) servizi come Youtube o Google Video erano solo nella mente degli informatici della Silicon Valley e non solo, sarebbe assurdo ritenere un servizio che "*hosta*" contenuti di terzi un *content provider*. Inoltre, ai sensi della normativa sul commercio elettronico, l'intermediario di *hosting* è prestatore di un servizio della società dell'informazione "consistente nella memorizzazione di informazioni fornite da un destinatario del servizio", il che descrive con esattezza la funzione svolta da Google Video.

Pertanto, risulta l'operatività dell'art. 16, comma 1, d.lgs. n. 70/2003 per il quale il prestatore di servizi di hosting non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che egli: non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita; per quanto attiene alle azioni risarcitorie, non sia al corrente dei fatti o di circostanze che rendano manifesta l'illegalità dell'attività o dell'informazione; non appena al corrente di tali fatti, su comunicazione delle Autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne.

Viene, poi, in rilievo l'art. 14 del Dlgs 70/2003 che disciplina la responsabilità dei prestatori intermediari con riferimento all'attività di semplice trasporto che sancisce la irresponsabilità del prestatore delle informazioni trasmesse, a condizione che non origini la trasmissione, non scelga il destinatario della trasmissione e non possa modificare le informazioni contenute nella trasmissione stessa.

Sul versante della responsabilità dei prestatori con riferimento alla memorizzazione temporanea, detta "*caching*", occorre considerare l'art. 15 del Decreto. Ai sensi del disposto citato, il prestatore non sarà considerato responsabile della memorizzazione automatica, intermedia e temporanea delle informazioni, effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta, a condizione che egli: non modifichi le informazioni; si conformi alle condizioni di accesso alle informazioni; si conformi alle norme di aggiornamento delle informazioni; indichi tali informazioni in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore; non interferisca con l'uso lecito delle tecnologie ampiamente riconosciute ed utilizzate nel settore, per ottenere dati sull'impiego delle stesse informazioni; agisca prontamente per rimuovere le informazioni che ha memorizzato o per disabilitarne l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione

dell'accesso. Viene, quindi, ipotizzata una limitazione di responsabilità che riguarda principalmente gli *Access providers*, cioè coloro che consentono agli utenti di collegarsi alla rete telematica.

Inoltre, l'art. 17 del Decreto in argomento, in conformità a quanto previsto dalla Direttiva all'art. 15, detta una disposizione comune alle norme sulla responsabilità degli intermediari ribadendo il principio dell'assenza di un generale obbligo di sorveglianza da parte degli intermediari sulle attività degli utenti che utilizzano i loro servizi, un problema molto avvertito dagli *Internet providers*, sui quali però pende sempre il rischio di una forma di responsabilità oggettiva mascherata.

In tutti questi casi, come è facile notare, non c'è alcun riferimento esplicito alla normativa sulla privacy che assume rilevanza solo in caso di aperto contrasto con i relativi principi di carattere generale, o meglio con una normativa che sistematicamente affronta in maniera organica e sistematica le forme di responsabilità dei vari soggetti intermediari della informazione.

Considerazioni conclusive

Queste appena esposte dovevano essere le giuste coordinate attraverso le quali giungere ad una corretta decisione in relazione al ritenuto illecito trattamento dei dati personali.

Ossia, inquadramento giuridico della fattispecie nell'ambito della disciplina dell'*e-commerce*, attribuendo al motore di ricerca i cui amministratori sono imputati la qualifica di *host provider*, con le conseguenze descritte dalle norme appena citate in punto di responsabilità del prestatore di sevizi.

Si è scelto, invece, di ignorare il dato normativo scaturente dal D.lgs. 70/2003, invocato dalle difese degli imputati, rifugiandosi il Giudice esclusivamente nella normativa della *data protection*, accogliendo, peraltro, un'interpretazione del combinato disposto degli artt. 13 e 23 D.lgs. 196/2003 che non si è tardati a definire eccentrica.

Per Pizzetti, questa è "un'operazione di ingegneria giuridica, con un errore tecnico per quanto riguarda la privacy", meritevole nelle intenzioni, ma sbagliata nei modi.

Andando alla ricerca di elementi da valutare positivamente, vi è da riconoscere come la tesi giurisprudenziale non sposi l'argomento accusatorio e l'obbligo di controllo preventivo dell'ISP, ma indica la strada di maggiori obblighi informativi a carico dei gestori di motori di ricerca.

Nel complesso, infatti, la sentenza può davvero essere considerata favorevole alla Rete poiché evita di intraprendere la facile strada del controllo dei contenuti - che il Garante definisce "un obiettivo che per far del bene produce troppo male, mettendo a rischio l'utilità democratica della rete" - poiché "carica solo qualche onere di informativa sugli ISP".

Il guaio è che in America tutto ciò è stato accolto come un tentativo di censura, ed è questo il pericolo che Pizzetti esorta a evitare, poiché il rischio ultimo

è addirittura l'abbandono dell'Italia da parte dei "grandi Isp internazionali", cosa che "sarebbe il massimo del ridicolo".

È innegabile, infatti, che sotto il profilo della politica del diritto, la prima conseguenza pratica di una tipologia di sentenza di condanna così strutturata per responsabilità da illecito trattamento dei dati, come nel caso in oggetto, delinea la scoraggiante prospettiva della morte della net economy. La seconda conseguenza pratica è la morte della libertà di espressione.

La ragione di tale conseguenze, risiede, probabilmente, nel fatto che a fronte di un servizio erogato in 160 Paesi, l'Italia è il primo nel quale si verifica un episodio del genere, ovvero nel quale tre top manager di Big G sono condannati per il contenuto di un video caricato da un utente della piattaforma.

Si consideri, peraltro, che nonostante la condanna irrogata per illecito trattamento dei dati personali, non si può dire che la sentenza ha il merito di soffermare l'attenzione su una questione sempre più pressante: la piattaforma tecnologica a cui il *netizen* affida i propri dati ha un ruolo attivo nel relativo trattamento oppure no?

È ben vero che le piattaforme on line, ormai, non si limitano più a un'attività di semplice trasmissione e scambio delle informazioni, ma sono diventate sempre più intelligenti. Queste piattaforme presentano applicazioni tecniche per caricare i materiali, per scaricarli, per conservarli on line in modo pubblico o in modo riservato, per condividerli.

Ma questo diviene un problema legislativo, la gestione e la soluzione di problematiche così complesse. Stiamo discorrendo di una sentenza penale di condanna; e l'accesso al sistema del diritto penale è sempre considerato come *extrema ratio*, caratterizzandosi per la violazione grave dei principi che fondano il vivere civile dei consociati.

Per cui anche questa lettura è da rifiutare.

Invero, tutta la decisione sembra essere permeata dal disagio del giudicante, che sostiene di essere " 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)" e nell'attesa si barcamena tra la consapevolezza dell'impossibilità di ricondurre al motore di ricerca un obbligo preventivo di controllo e l'assunto della peculiarità di questa figura che è più di un semplice *host provider*, alla ricerca con il lanternino di ipotesi accusatorie e di condanna per le condotte *de quo.*

Peraltro, il fatto stesso che si auspichi l'approvazione di una "buona legge" che limiti la "libertà assoluta" della Rete porta a pensare che in Italia non si sia ancora metabolizzato il principio del *notice and takedown* (ossia della rimozione del contenuto dopo un'appropriata segnalazione) perno fondante l'intera normativa italiana e comunitaria sul commercio elettronico che trova un riscontro anche oltreoceano nel Digital Millenium Copyright Act.

Non rimane, allora, che affidarsi all'auspicio espresso dal Garante: "Vorrei evitare che si avesse un'immagine internazionale che non è fondata, viste le caratteristiche della sentenza e allo stesso tempo evitare di dare su un piatto

d’argento a chi, non per difendere la libertà della rete, ma solo un attività imprenditoriale che oggi non è carica di doveri che dovrebbe invece assumere, l’occasione di fare un atto dimostrativo che avrebbe solo un effetto intimidatorio verso i legislatori di tutto il mondo”.

Ai confini della responsabilità penale: che colpa attribuire a google

di Francesco Giuseppe Catullo (∗)

1. Controversia mediatica

La sentenza in commento che consta di cento otto pagine, suddivise in due parti, ulteriormente parcellizzate in sedici paragrafi si conclude con una chiosa che parafrasa la famosa commedia shakespeariana *Molto rumore per nulla.*

Il suo redattore, infatti, meravigliato per «la grande (ed inaspettata) ricaduta mediatica» del provvedimento in questione, reo di aver «alterato in modo sensibile i parametri valutativi e giurisdizionali che presiedono» alla libertà su Internet, dedica l'ultimo paragrafo della sua lunga e strutturata sentenza a giustificare il proprio operato dinanzi non ai destinatari immediati della sua decisione ma ad una platea molto più vasta, quella dell'opinione pubblica (1).

Rivolgendosi ad essa, il magistrato si auto-esonera dalla responsabilità legata alla conseguenze del giudizio, affermando che il proprio *ius dicere* non avrebbe «alterato in modo sensibile i parametri valutativi e giurisdizionali che presiedono alla decisione di casi quali quello trattato», in quanto la condanna del *webmaster* in ordine al reato di illecito trattamento di dati personali è stata costruita non «sulla base di un obbligo preventivo di controllo sui dati immessi, ma sulla base ... di un'insufficiente (e colpevole) comunicazione degli obblighi di legge nei confronti degli *uploaders*».

Nella specie, Google Video per più di due mesi aveva diffuso sulla Rete un filmato realizzato dagli alunni di una scolaresca che, senza aver raccolto il consenso della persona rappresentata, gravemente ne offendeva la reputazione (2) . Il citato filmato veniva rimosso da Google Video a circa due mesi di tempo dalla sua inserzione on-line e a ventiquattrore ore di distanza dal momento in cui un privato cittadino ed un agente di P.S. formalmente avvisavano la redazione del noto motore di ricerca della presenza del video *de quo* nel proprio spazio virtuale di competenza.

La condotta rilevante penalmente che viene contestata ai responsabili di Google Italia s.r.l. sarebbe quella di aver gestito il servizio offerto da Google Video, omettendo di fornire ai propri inserzionisti telematici chiare e puntuali informazioni sulla corretta modalità del trattamento dei dati personali; avrebbero fatto ciò al fine di raccogliere un numero sempre più elevato di filmati per accrescere l'interesse al servizio da parte di eventuali acquirenti di spazi pubblicitari su Internet.

La questione di maggiore interesse della citata controversia non è stata, quindi, quella di accertare la sussistenza dei reati contestati o la loro riferibilità ai soggetti che avevano partecipato alla messinscena filmica o a coloro che avevano provveduto materialmente all'inserzione del video su Internet, bensì quella d'individuare l'eventuale corresponsabilità di Google Video nella commissione

(∗) in *Giurisprudenza di Merito*, 2011, 159.

del reato di cui all'art. 167 d.lg. 30 giugno 2003, n. 196 per aver ospitato presso il proprio spazio virtuale un filmato dai contenuti delittuosi.

2. Aspetti contraddittori della decisione

Per valutare la suesposta *ratio decidendi*, è necessario soffermarsi su due conclusioni rassegnate dal Giudicante che acquistano significato ermeneutico per comprendere la coerenza dell'intero provvedimento.

La prima, rimarcata per cinque volte dal Tribunale, si sostanzia nell'affermare che non può essere addebitata ai dirigenti italiani di Google la responsabilità penale per aver omesso di effettuare controlli preventivi sul rispetto della legalità dei video da pubblicare on-line; la seconda è che i responsabili di Google Italia non possono essere chiamati a rispondere per i contenuti dei filmati già pubblicati in Rete.

L'ovvia premessa di entrambe le conclusioni è che non può essere considerato punibile penalmente chi «raccolga, utilizzi o diffonda dati che egli, in buona fede, debba o possa considerare come «lecitamente raccolti» da altri».

In entrambe le conclusioni, quindi, la condotta positiva richiesta ai dirigenti del noto portale elettronico ed atta a scongiurare i fatti di reato contenuti nei filmati viene considerata inesigibile dal giudicante, in conformità di un attestato indirizzo giurisprudenziale e dottrinario (3) che ha ravvisato, nella citata causa di esclusione della *tipicità* (4) , l'estraneità dell'Internet Provider dai contenuti illeciti presenti nell'enorme mole di materiale informativo quotidianamente trattato da quest'ultimo.

Date queste due conclusioni, condivise anche da chi scrive, segue una terza su cui dissente: i dirigenti di Google Italia sono responsabili di trattamento illecito di dati personali perché, omettendo di dare informazioni ai propri *uploaders* sul regime della *privacy*, hanno accettato il rischio di diffondere sulla Rete video in spregio alla suesposta normativa.

«Esiste quindi ... un obbligo non di controllo preventivo dei dati immessi nel sistema, ma di corretta e puntuale informazione, da parte di chi accetti ed apprenda dati provenienti da terzi».

La descritta responsabilità penale si concreta in un'intenzionale omissione della prescrizione normativa che impone di raccogliere il consenso della persona rappresentata nel video prima di divulgarlo.

Secondo il giudice meneghino, il dolo specifico del soggetto agente andrebbe ricercato nel momento in cui il *service provider* avrebbe omesso o fornito insufficiente informazione ai propri inserzionisti sulla disciplina da seguire in tema di trattamento di dati personali, per conseguire l'ingiusto vantaggio economico di favorire la raccolta pubblicitaria.

La condotta delittuosa di cui all'art. 167 d.lg. n. 196 del 2003, informata dal dolo specifico, viene ricostruita nel caso *de quo* alla stregua di un'ipotesi di reato commissivo mediante omissione sostenuto da dolo eventuale (5) , ritenendo il Tribunale provata la «chiara accettazione consapevole del rischio concreto di

inserimento e divulgazione di dati, anche e soprattutto sensibili, che avrebbero dovuto essere oggetto di particolare tutela» (6) .

Allo scopo di valutare la sostenibilità del suesposto argomentare, è necessario individuare in che momento preciso della dinamica della condotta, il Tribunale ravvisa la sussistenza del dolo di cui all'art. 167 d.lg. n. 196 del 2003. Questo momento coinciderebbe con quello in cui i dirigenti di Google avrebbero assunto la decisione di omettere o comunque di fornire insufficiente informazione ai propri inserzionisti e quindi, parafrasando le parole del giudicante, «all'atto della prima comunicazione di caricamento». Da quel momento in poi, i prevenuti avrebbero delimitato la propria sfera di competenza e di responsabilità per gli eventuali reati commessi dai propri *uploaders* in spregio al trattamento dei dati personali (7) .

È proprio in quella frazione di tempo, che precede lo scadere del termine per fornire sufficiente informazione, che andrebbe accertato il dolo eventuale dei responsabili di Google, secondo il Tribunale di Milano.

Confrontando questa terza conclusione con le prime due, si evidenzia la contraddizione del ragionamento giudiziale: il Tribunale prima afferma che i dirigenti di Google non possono essere responsabili penalmente per i «fatti» (diffamazione) posti in essere dai propri inserzionisti, non potendo il *service provider* ricoprire ambiti di competenza per i reati che si consumano nella struttura sociale di Internet; poi specifica che i medesimi dirigenti sono garanti per il delitto di «illecito trattamento di dati personali» che si perfeziona nello spazio virtuale di competenza di Google.

L'equivoco in cui è caduto il giudicante nella terza conclusione è quello di credere di risolvere la citata contraddizione, collegando l'omissione di fornire informazioni al verificarsi di un determinato evento illecito anziché ad una serie indistinta di reati, così come chiarito dal legislatore (8) , dalla dottrina (9) e dalla giurisprudenza (10) .

La conseguenza del giudizio del Tribunale di Milano legata alla sua terza conclusione è stata, dunque, quella di aver ripristinato per Google la posizione di garanzia, inizialmente esclusa, con l'affermazione delle prime due conclusioni. Addirittura, ne ha anticipata la vigenza in un momento precedente rispetto a quello che sarebbe stato individuato se il giudicante avesse ritenuto esigibile la verifica sui contenuti dei Video da diffondere da parte del *service provider*.

È logico, infatti, che tra le due condotte omesse da Google, di fornire informazioni agli inserzionisti ed effettuare controlli preventivi sui contenuti raccolti da questi ultimi, si ravvisa una precedenza cronologica ed un rapporto di inclusione che individua nella prima un *genus* e nella seconda una *species*. Pertanto, se già all'omissione della *species* (che comprende il *genus*) non è ricollegabile la produzione di uno specifico evento di reato, ma la constatazione di un'indeterminata serie di reati su cui il *service provider* non può essere considerato garante, com'è possibile sostenere che all'omissione del *genus* corrisponda la verificazione di uno specifico reato (Trattamento illecito di dati personali) su cui Google sarebbe competente?

Se il Tribunale di Milano, rapportandosi alla struttura sociale di Internet, ha già convenuto che l'omissione di una verifica specifica non è in grado di disegnare un ambito di competenza per Google, cade in contraddizione con se stesso quando afferma che l'omissione di un controllo generico, e cronologicamente antecedente, è idoneo a vincolare il *service provider* in un ambito di responsabilità (11) .

L'individuazione della posizione di garanzia, essendo frutto dell'interpretazione di un senso di razionalità e giustizia che deve essere colto dal giudice *in relazione a determinate strutture sociali* (12) , va mantenuta coerente rispetto a queste.

Il motivo per cui il Tribunale di Milano è caduto in siffatta contraddizione (13) troverebbe spiegazione nel fatto di aver individuato una posizione di garanzia gravante su Google, prima di risolvere la questione relativa al nesso causale che avrebbe dovuto legare l'omessa informazione del Service alla condotta illecita del *contenent provider.*

La maggiore criticità del fatto sottoposto alla valutazione del giudicante non risiedeva, perciò, nell'individuazione della posizione di garanzia e nell'accertamento della tipicità soggettiva, quanto piuttosto nella spiegazione della causalità.

È nell'accertamento di questa che, a parere di chi scrive, andava profuso il maggior impegno interpretativo.

Concludendo, il Tribunale ha convenuto che Google non può essere responsabile dei contenuti illeciti pubblicati dai propri inserzionisti, pur certo che un controllo preventivo del *service provider* avrebbe evitato la commissione di reati: come può il medesimo giudicante ritenere Google garante per i reati commessi dai propri *uploaders* in spregio alla *privacy,* se resta il dubbio che una puntale informazione a questi ultimi sulla corretta modalità del trattamento dei dati personali avrebbe evitato la commissione dei citati reati?

3. Omesso accertamento della causalità

Per accertare la causalità nei delitti omissivi impropri è necessario verificare prima se l'azione prescritta, ove posta in essere, sarebbe stata idonea ad evitare l'evento; poi, l'esistenza dell'obbligo giuridico di impedire l'evento.

Il primo dei due requisiti della causalità dell'omissione, e cioè il giudizio sull'evitabilità, ne presuppone altri due: 1) il tipo di conseguenze che sarebbero derivate se il soggetto avesse posto in essere l'azione omessa; 2) la possibilità di realizzare il comportamento omesso.

Per risolvere il giudizio relativo al «tipo di conseguenze che sarebbero derivate se il soggetto avesse posto in essere l'azione omessa» interviene il criterio della *condicio sine qua non* che esige una risposta certa e non probabilistica su che cosa sarebbe successo (14) :«non può essere imputato all'agente un evento che si sarebbe verificato anche in presenza del perfetto adempimento di quanto voluto dalla legge» (15) .

Nel caso in commento, pertanto, il Tribunale avrebbe dovuto risolvere prima il quesito se il diligente adempimento, agli obblighi informativi da parte di Google, sarebbe stato in grado di dissuadere l'inserzionista dal trattare i dati sensibili di una terza persona senza il suo consenso (16) ; successivamente la questione relativa all'individuazione della posizione di garanzia ricoperta dal citato *service provider*.

A parere di chi scrive, la soluzione alla questione ipotetica relativa al diligente adempimento degli obblighi informativi si risolve in un giudizio negativo, rendendo superfluo qualsiasi altro tipo di verifica successiva.

L'insussistenza del nesso causale in questione discenderebbe da due ordini di considerazioni.

Il *primo*: è irragionevole credere che il perfetto adempimento di Google alle prescrizioni impostegli dall'art. 167 sarebbe stato in grado di dissuadere gli inserzionisti dal realizzare un proposito delittuoso già deliberato, poiché l'informazione che Google avrebbe dovuto fornire con puntualità e precisione ai propri *uploaders* ha come contenuto il medesimo che l'ordinamento presume già noto da qualsiasi consociato, riguardando elementi costitutivi di reato (art. 5 c.p.).

Afferma sul punto il Tribunale di Milano: all'*hoster* attivo «è imponibile ... un obbligo di corretta informazione agli utenti dei conseguenti obblighi agli stessi imposti dalla legge, del necessario rispetto degli stessi, dei rischi che si corrono non ottemperandoli (oltre che, naturalmente, l'obbligo di immediata cancellazione di quei dati e di quelle comunicazioni che risultassero correttamente segnalate come criminose)».

Nonostante sia imperativo il principio per cui «nessuno può invocare a propria scusa l'ignoranza sulla legge penale», secondo il giudicante, Google dovrebbe provvedere non solo a ricordare ai propri inserzionisti che su loro, come su qualunque altro consociato, gravano gli obblighi della legge penale (art. 3 c.p.), ma addirittura sarebbe tenuto a confermare agli stessi due delle caratteristiche principali che connotano i precetti penali e cioè che non vanno trasgrediti e che, in caso di violazione, viene comminata una pena.

È poco attendibile ritenere che l'inserzionista, dopo aver deciso di trasgredire i precetti penali relativi al trattamento illecito dei dati personali e alla diffamazione, possa interrompere la propria azione delittuosa perché disincentivato dall'ammonimento proveniente dal *service provider*. Del resto a pensarla in questi termini sembra essere lo stesso Tribunale di Milano, quando nel sostenere che l'esatto adempimento alla normativa della privacy non è idoneo a prevenire i delitti di diffamazione sul web, afferma: «anche se l'informativa sulla *privacy* fosse stata data in modo chiaro e comprensibile all'utente, non può certamente escludersi che l'utente medesimo non avrebbe caricato il file video incriminato, commettendo il reato di diffamazione». Se fosse così, ci dovremmo confrontare con l'imbarazzante situazione di credere che il potere prescrittivo di Google sia più incisivo e penetrante di quello dello Stato.

Inoltre, qualora venisse ravvisato un nesso causale tra l'omessa informazione di rispettare la legge penale e la commissione di reati da parte degli inserzionisti, Google diventerebbe automaticamente responsabile per qualsiasi contenuto illecito diffuso dai video dei propri *uploaders* se non provasse, di volta in volta, di aver fornito informazioni in merito agli elementi costitutivi del divieto violato. Anche su questo punto si evidenzia una contraddizione nella motivazione della sentenza in commento, perché non risulta coerente addebitare a Google la responsabilità di trattamento illecito di dati personali per non aver esplicitato il divieto di pubblicare video senza il consenso della persona rappresentata mentre non gli si contesta, invece, la responsabilità per il delitto di diffamazione per non aver ammonito i propri inserzionisti di non pubblicare video lesivi della reputazione.

Il *secondo* ordine di considerazioni per cui, nella condotta oggetto di disamina, non ci sarebbe equiparazione tra il «non impedire l'evento» e il «cagionarlo» risiede nel fatto che il Tribunale di Milano ricostruisce la condotta di cui all'art. 167 attraverso il dolo eventuale. Questo elemento psicologico, infatti, stenta a conciliarsi con la modalità omissiva perché la sua individuazione nella condotta diventa difficilmente praticabile in sede di accertamento. Se dall'analisi del *non facere* già traspare poco della rappresentazione e volontà del soggetto agente di cagionare un determinato evento, dalla medesima analisi non potrà risultare niente che sia indiziante della volontà di accettare l'evento che è stato rappresentato negli *interna* del reo solo come conseguenza eventuale rispetto all'obiettivo principale preso di mira (17) .

Ma c'è di più. Il dolo eventuale si coniuga male anche nell'ambito del concorso di persone nel reato quando ad essere eventuale è la volontà di partecipare all'azione altrui (18) . È da escludere la responsabilità concorsuale del soggetto che non ha voluto il fatto altrui come proprio, pur rappresentandosi «la possibilità che oggettivamente il suo comportamento potrà essere utilizzato da altri soggetti per il conseguimento dei loro scopi» (19) .

Concludendo, se il dolo eventuale già stride nella costruzione dei reati dolosi e nella spiegazione delle manifestazioni concorsuali di persone nel reato, risulta veramente ardito il suo appello nelle ipotesi di partecipazione mediante omissione nel reato commissivo (20) .

4. Responsabilità del giudice e opinione pubblica

Ulteriore aspetto innovativo della sentenza in commento è che oltre a strutturarsi attraverso le tradizionali procedure argomentative della «motivazione in fatto» e della «motivazione in diritto», ne esplicita una terza indirizzata all'opinione pubblica che ha il senso ed il contenuto di una «giustificazione» (21) atta a ricomporre la delegittimazione sofferta dal proprio giudizio per non essere riuscito ad incontrare il consenso sociale.

Risulta, dalla lettura del provvedimento, che dal momento decisorio a quello del deposito della motivazione, si è frapposta la critica mediatica (22) alla suesposta decisione che ha indotto il Tribunale a replicare alle contestazioni solle-

vategli, affermando che «La grande (ed inaspettata) ricaduta mediatica di questo procedimento e della sua sentenza finale di primo grado, impone a questo giudicante una breve chiosa conclusiva».

Gli argomenti più rilevanti utilizzati nella citata chiosa possono così sintetizzarsi:

1) esiste un vuoto normativo in materia di responsabilità dei *webmasters*;

2) un'eccessiva libertà del settore degenera in arbitrio;

3) in futuro, il progresso della tecnologia faciliterà la regolamentazione del settore facendo anche riferimento alla categoria della colpa (23) ;

4) la decisione *de qua* ha cercato di avvicinarsi «ad una zona di pericolo per quel che concerne la responsabilità penale dei *webmasters*»;

5) la sentenza in questione, allineandosi all'interno di un indirizzo giurisprudenziale già attestato da due precedenti, non può aver alterato significativamente i parametri valutativi e giurisdizionali che presiedono alla decisione di casi simili

Anche queste ultime giustificazioni proposte dal giudice di Milano, come le motivazioni a sostegno del dispositivo di condanna, convincono poco.

Infatti, a parere di chi scrive, la decisione in commento non solo ha ripristinato una posizione di garanzia esclusa dalla dottrina e dalla giurisprudenza attraverso la categoria della inesigibilità, ma addirittura ne ha ampliato il raggio di azione, anticipandone lo spazio garantito sino al momento della «prima comunicazione del caricamento» del video da parte dei propri inserzionisti. Non si comprende la meraviglia del giudicante per aver raccolto dissenso da parte dell'opinione pubblica nel momento in cui il suo *ius decidere* ha imposto a tutti i *service provider* un inedito (24) sforzo per evitare la sanzione penale, sforzo che oltre ad essere indeterminato (25) , superfluo (26) ed inutile (27) , limita la libertà sulla Rete così come sino a questo momento si è manifestata (28).

Troppo rumore per nulla? Probabilmente no!

NOTE

(1) Hassemer, Il diritto attraverso i media: messa in scena della realtà?, in Ars Interpretandi, 2004, 151, che − condividendo la dottrina della «prevenzione generale positiva» − spiega come la giustizia penale, in quanto istituzione statale e sociale, non può fare a meno del giudizio dell'opinione pubblica. «In base a tale dottrina, il diritto penale ha il compito di trasmettere la fiducia in un'effettiva legalità e in un ordine giuridico stabile. La speranza nella prevenzione generale positiva è che il diritto si dimostri giusto ed efficace agli occhi e nel cuore di tutti, che il torto subito non si trasformi in normalità per quanto costituisca un'esperienza quotidiana, che gli uomini possano attendersi che alla fine il diritto prevarrà». Quasi cento anni prima, sul medesimo tema, Lanza, Il giurì e le assoluzioni dei vendicativi passionali, in Riv. pen., LXIX, 1909, 381 ss. che scrive «Uno dei principali pregi della giuria ... è quello di rendere giustizia, non secondo formule stereotipate sancite nei codici, non secondo principii rigidi e inflessibili, non secondo le dottrine e le opinioni di chi può imporre una legge, ma bensì secondo i sentimenti e la coscienza del popolo»; questo è garanzia di una giustizia penale «che dal popolo emana e che il popolo garantisce e difende ... che punisce soltanto chi dal popolo è considerato come turbatore della sua pace e della sua sicurezza».

(2) Cfr. Manna, Codice della privacy: nuove garanzie per i cittadini nel Testo unico in materia di protezione dei dati personali, in Dir. pen. proc., 2004, 22 ss; Catullo, Quando il trattamento illecito dei dati personali può offendere la reputazione, in Riv. pen., 2005, 484 ss.

(3) Picotti, Fondamento e limiti della responsabilità penale dei service-providers in Internet, in Dir. pen. proc., 1999, 384.

(4) Fiandaca-Musco, Diritto penale − Parte generale, Bologna, 2007, 581, che spiega come nel reato omissivo il compimento dell'azione comandata presuppone che il soggetto abbia «la possibilità di agire» nel senso normativamente richiesto; e che, quindi, tale possibilità di agire − sul piano della tipicità della condotta omissiva − va intesa nel senso minimo di possibilità materiale di adempiere al comando; v. anche Cadoppi, Il reato omissivo proprio. II Profili Dogmatici, comparatistici e de lege ferenda, Padova, 1988, 815 ss.

(5) Picotti, La responsabilità penale dei service-providers in Italia, in Dir. pen. proc., 1999, 502, secondo cui per la responsabilità penale del provider può bastare de jure condito il comune dolo, pur nella forma eventuale; Contra De Natale, La responsabilità dei fornitori di informazioni in Internet per i casi di diffamazione on line, in Riv. trim. dir. pen. econ., 2009, 561; Resta, La responsabilità penale del provider: tra laissez-faire ed obblighi di controllo, in questa rivista, 2004, 1728 ss.; con riferimento alla compatibilità tra dolo specifico e dolo eventuale Prosdocimi, Dolus eventualis. Il dolo eventuale nella struttura delle fattispecie penali, Milano, 1993, 174.

(6) Fiandaca, Il reato commissivo mediante omissione, Milano, 1975, 193, si tratterebbe di una posizione di controllo su fonti di pericolo in cui il garante è obbligato ad impedire l'agire illecito del terzo. Secondo l'A. affinché sussista la citata posizione di garanzia sono necessari due requisiti: a) che il terzo deve essere carente dei requisiti necessari a governare in modo responsabile il proprio comportamento; b) e che, proprio a causa di tale stato di incapacità naturale, egli debba sottostare al potere di controllo e vigilanza di un garante. Entrambi i requisiti sembrano non sussistere nel caso sottoposto all'attenzione del Tribunale di Milano, considerando che in giudizio non è stata fornita alcuna prova sull'incapacità degli inserzionisti di Google ad autogovernarsi in maniera responsabile.

(7) Gallo, Appunti di diritto penale. Vol. II. Il Reato. Parte II, L'elemento psicologico, Torino, 2001, 32 ss., che spiega come nei reati commissivi mediante omissione, il non fare rilevante agli effetti penali sarebbe quello immediatamente antecedente lo scadere del termine fissato per legge per porre in essere l'azione prescritta: scaduto inutilmente il quale, si attiva un processo causale che diventa indipendente rispetto ai successivi interventi del soggetto agente.

(8) Cfr. art. 17 d.lg. 9 aprile 2003, n. 70 (codice di commercio elettronico), che disciplina l'«Assenza dell'obbligo generale di sorveglianza» per i c.d. prestatori di servizi della società dell'informazione.

(9) Seminara, La pirateria su Internet e il diritto penale, in Riv. trim. dir. pen. econ., 1997, 71 ss e Spagnoletti, La responsabilità del provider per i contenuti illeciti di internet, in questa Rivista, 2004, 9, 1928 ss.

(10) Trib. Milano 18 marzo 2004, in questa Rivista, 2004, 1713 ss.

(11) Nella motivazione della sentenza, il Tribunale, nel riportare la linea accusatoria dei PM, spiega come la posizione di garanzia a carico di Google «derivante da un obbligo giuridico contenuto nella legge sulla privacy» sarebbe «causativa di un obbligo «preventivo» di controllo sui video caricati sul sito».

(12) Pioletti, Causalità (rapporto di), Dig. disc. pen., aggiornamento, 2008, 91, nt. 70.

(13) Sugli aspetti contraddittori della sentenza in commento cfr. Pezzella, Google Italia, diffamazione e riservatezza: il difficile compito del Provider (e del giudice), in questa Rivista, 2010, 2254 ss.

(14) Donini, Imputazione oggettiva dell'evento. «Nesso di rischio» e responsabilità per fatto proprio, Torino, 2006, 106 e 131 che introduce la seguente regola di giudizio: per conoscere le vere conseguenze giuridicamente rilevanti della condotta colposa attiva (o dell'omissione dolosa) «occorre accertare il compiuto decorso ipotetico del comportamento alternativo lecito. Se non ci si riesce, vale la regola probatoria del dubbio su un elemento costitutivo del reato: il nesso oggettivo di condizionamento non è provato». L'A. specifica inoltre di non condividere le espressioni più radicali delle teorie dell'aumento del rischio che ravvisano il nesso causale anche quando consti, ex post, che l'azione «omessa», o diligente, avrebbe consentito alcune maggiori possibilità di evitare l'evento. Il risultano apportato da queste teorie è, infatti, «quello di trasformare reati di evento in reati di pericolo, dove l'evento funziona come una sorta di condizione di punibilità».

(15) Gallo, Appunti di diritto penale. Vol. II. Il Reato. Parte I, La fattispecie oggettiva, Torino, 2000, 132.

(16) Risicato, Combinazioni e interferenze di forme di manifestazione del reato. Contributo ad una teoria delle clausole generali di incriminazione suppletiva, Milano, 2001, 453, che spiega come il garante potrà incorrere «in responsabilità penale per il mancato impedimento del fatto illecito altrui solo se tale fatto consista ... nella realizzazione di un reato causale pur di evento posto a tutela di beni di rango elevato, quali la vita e l'incolumità individuale o pubblica e sempre che lo Hintermann abbia il potere di impedire il verificarsi dell'evento lesivo». Secondo questa interpretazione, quindi, nel caso sottoposto all'attenzione del Tribunale di Milano non potrebbe ravvisarsi la responsabilità di Google, considerando che i reati perfezionabili da parte del terzo inserzionista non riguardano né la vita, né tantomeno l'incolumità individuale o pubblica.

(17) Pagliaro, Il reato, in Trattato di diritto penale, diretto da Grosso - Padovani - Pagliaro, Milano, 2007, 109; Pagliaro, Causalità e diritto penale, in Cass. pen., 2005, 1050, così argomenta: «Che il volere di un certo evento possa essere realizzato anche con il semplice astenersi dall'intervenire nel mondo esterno, è proposizione che risponde a verità solo quando il soggetto tende a quell'evento o come fine ultimo o come mezzo necessario per conseguire il fine ultimo. Se, invece, l'evento è rappresentato dall'agente come conseguenza necessaria o possibile del fatto che egli, per un fine diverso dall'attuazione di quell'evento, non compie una certa attività muscolare, il verificarsi dell'evento stesso per lo svolgimento naturale di altri processi causali non rappresenta la proiezione esterna del significato inerente al valore del soggetto. In breve: non realizza un suo volere che abbia ad oggetto l'evento A chi, mirando all'evento B, rimanga inattivo»; Eusebi, Appunti sul confine tra dolo e colpa nella teoria del reato, in Riv. it. dir. proc. pen., 2000, 1094; Cadoppi, Il reato omissivo proprio. II Profili dogmatici, comparatistici e de lege ferenda, Padova, 1988,1032.

(18) Risicato, Combinazioni e interferenze di forme di manifestazione del reato. Contributo ad una teoria delle clausole generali di incriminazione suppletiva, cit., 456.

(19) Contento, Corso di diritto penale, Bari, 1998, 482.

(20) Cfr. Fiandaca-Musco, Diritto penale —Parte generale, cit., 619 ss.

(21) Wróblewski, Il sillogismo giuridico e la razionalità della decisione giudiziale (1974), in Aa.Vv., L'analisi del ragionamento giuridico. Materiale ad uso degli studenti,

a cura di Comanducci - Guastini, I, Torino, 1987, 297, che intende per «giustificazione esterna» la giustificazione delle premesse del sillogismo decisionale.

(22) Hassemer, Diritto giusto attraverso un linguaggio corretto? Sul divieto di analogia nel diritto penale, in Ars Interpretandi, 1997, 194, secondo cui «un buon rimedio contro un esercizio giurisdizionale che violi le leggi consiste proprio nell'osservazione critica da parte di un'opinione pubblica vigile, interessata ed informata»; v. anche Comanducci, Il ragionamento giudiziale: lineamenti di un modello, in Interpretazione e diritto giudiziale. I Regole, metodi, modelli, a cura di Bessone, Torino, 1999, 66 secondo cui, nelle moderne società democratiche, l'attività interpretativa «è attività sottoposta a molteplici controlli, alcuni dei quali istituzionalizzati, altri diffusi. Non ultimo, sembra essere abbastanza efficace il potere dell'opinione. Interpretazioni cervellotiche o inusitate andrebbero incontro a pesanti reazioni di disapprovazione e rigetto sociali. (...) L'opinione ... funziona da strumento di controllo nei confronti delle interpretazioni più bizzarre»; Catullo, Il diritto di critica come strumento di democrazia, in Cass. pen., 2008, 2849 ss.

(23) Questa argomentazione è significativamente indiziante del convincimento del Tribunale di Milano di voler ricostruire un fatto doloso attraverso le categorie della colpa. Sul punto v. Resta, La responsabilità penale del provider: tra laissez-faire ed obblighi di controllo, cit., 1728, che spiega come nell'individuazione delle responsabilità dei service provider per omessi controlli si rischia «di trasformare surrettiziamente una fattispecie legislativamente prefigurata sul modello doloso, in un'esangue ipotesi colposa».

(24) Inedito perché le due sentenze citate dal Tribunale di Milano introducono principi diversi da quelli sostenuti da quest'ultimo.

(25) Indeterminato perché il service provider com'è responsabile di illecito trattamento dei dati personali per non aver fornito ai propri inserzionisti corretta informazione in merito agli elementi costitutivi del reato de quo, così potrà essere responsabile di qualsiasi altro reato commesso da un proprio uploader se non risulta che gli abbia fornito corretta informazione in merito alla normativa da quest'ultimo violata. Sul punto vedi Fiandaca, Il reato commissivo mediante omissione, cit., 197.

(26) Superfluo perché le informazioni che il service provider dovrebbe fornire correttamente al propri inserzionisti riguardano gli obblighi penali imposti dalla legge, la necessità di rispettarli, i rischi che si corrono non ottemperandoli, ossia riguardano aspetti normativi che l'ordinamento presume essere già conosciuti da tutti i consociati (art. 5 c.p.).

(27) Inutile perché non è assolutamente certo che una precisa e puntuale informazione da parte del service provider in merito ai contenuti normativi di cui sopra sia idonea a impedire che gli inserzionisti commettano reati.

(28) Habermas, Prefazione alla nuova edizione (1990) di Storia e critica dell'opinione pubblica (1962), Bari, 2006, XLI, cita il libro di Meyrowits, No Sense of Place, Oxford, 1985, per spiegare come nella società dell'elettronica e dell'informazione, alla stessa stregua di quella primitiva dei cacciatori e dei raccoglitori, è diventato più difficile sia mantenere separati i luoghi, sia distinguere le sfere sociali. Queste difficoltà, tuttavia, rendono più egualitarie i ruoli dei maschi e delle femmine, dei bambini e degli adulti, dei capi e dei seguaci.

Google Italia, diffamazione e riservatezza:
il difficile compito del provider (e del giudice)

di Vincenzo Pezzella (*)

1. Premessa

Molto si è discusso e si discuterà ancora sulla sentenza con cui il giudice monocratico del Tribunale di Milano il 24 febbraio 2010 ha condannato i responsabili di Google Italy e di Google Inc, in concorso, tra loro, per il reato di cui all'art. 167 d.lg. 30 giugno 2003, n. 196 del (il cosiddetto codice della *privacy*), mentre li ha mandati assolti per il concorso in diffamazione ai danni della onlus Vivi Down.

La reazione di Google alla sentenza di Milano era più che attesa (1). Come quella dei *blogger* e dei siti specializzati in tecnologie di mezzo mondo, altrettanto negativa (2). E anche quella della stampa statunitense (3). Ma pochi si sarebbero immaginati che contro la condanna dei tre dirigenti di *Googl*e arrivassero in prima battuta parole assai dure ed ufficiali dall'ambasciatore statunitense a Roma, David Thorne (4).

Va detto che l'ambasciatore statunitense, dopo le prime dichiarazioni, è parso tornare sui suoi passi precisando come quello sui modi e limiti dell'utilizzo di Google «è un dibattito importante» perché quello attuale «è un momento in cui tutti stiamo imparando come affrontare i problemi giuridici che sorgono dalle nuove tecnologie» (5).

Poi, però, tornava alla carica, dagli Stati Uniti, lo stesso Governo Usa, con l'assistente segretario di Stato per la democrazia, i diritti umani e il lavoro, Michael Posner, che nel corso di un'audizione presso la commissione del Senato statunitense che si occupa delle leggi che regolano la libertà su *Internet* commentava essere «deprimente, per non dire altro, che le autorità italiane abbiano cercato di imporre ai rappresentanti di una compagnia privata una censura preventiva dei contenuti» (6)

In termini di preoccupazione, dopo la lettura del dispositivo, si esprimeva anche l'ex Garante della privacy Stefano Rodotà (7). E il *clou* della spettacolarizzazione mediatica della pronuncia si aveva con la partecipazione degli stessi soggetti istituzionali del processo al pubblico dibattito (8).

Poi, alla lettura della motivazione, non sono mancate le critiche anche da parte dei giuristi. E di certo chi si attendeva già in primo grado l'enucleazione di principi giuridici in grado di dire una parola chiara sui compiti del *provider* e sulla possibile sussistenza di una sua posizione di garanzia rispetto alla lesione dell'altrui reputazione o della *privacy* è rimasto deluso (9).

Le 108 pagine della motivazione del giudice milanese, infatti, indugiano in gran parte sulla descrizione dei ruoli e dei compiti all'interno della struttura di *Google* e alle modalità di pubblicazione dei video, mentre solo nella parte finale (da pag. 85 in poi) si traggono le conseguenze sul piano giuridico di tale orga-

---

(*) in *Giurisprudenza di Merito*, 2010, 2232.

nizzazione, prima che il giudice si lasci andare a delle «*considerazioni finali*» che, invero, paiono assai poco giuridiche e, in quanto tali, mal collocate all'interno di un provvedimento giudiziario.

Il compito affrontato dal giudice milanese non era, tuttavia, dei più agevoli, in primo luogo perché, rimessa la querela da parte dei rappresentanti legali del minore, è venuta meno l'imputazione che maggiormente meritava attenzione: la diffamazione nei confronti del ragazzino protagonista suo malgrado del video.

Ciò nondimeno, come si avrà modo di dire, il giudice ha motivato sulla possibile sussistenza anche di tale reato. In *primis*, rilevando condivisibilmente come la remissione di querela da parte del minore «esclude solo la configurabilità del fatto (in termini di responsabilità) nei confronti degli imputati in relazione alla parte lesa in questione, ma non incide sugli elementi costitutivi del capo d'imputazione e, in particolare, sulla ricostruzione dello stesso così come prospettato». E, in secondo luogo, perché era rimasta in piedi l'analoga contestazione di reato in danno della *onlus* Vivi Down.

Ebbene, proprio la contestazione del reato di diffamazione aveva lasciato sperare che si potesse giungere, stante la peculiarità del caso, ad un qualcosa in più, alla luce del diritto vigente, in termini di affermazione di principi giuridici applicabili a casi simili, rispetto ad una sentenza che, per espressa e ripetuta affermazione dell'estensore, si pone in attesa che sia poi il legislatore ad intervenire con una «buona legge» sull'argomento.

C'era il fondamento normativo perché ciò avvenisse già oggi?

Per dare una risposta a tale non semplice quesito va detto che, da sempre, chi quotidianamente è chiamato a giudicare un reato di diffamazione si trova ad essere partecipe di una rincorsa, inevitabilmente perdente, rispetto all'affermarsi delle nuove tecnologie. A tale rincorsa egli partecipa, infatti, con uno strumentario normativo, qual è quello di cui agli artt. 595 c.p. del 1942 e della l. n. 47 del 1948 sulla stampa, che era stato pensato per un sistema di veicolazione dell'informazione che vedeva nella carta stampata il suo momento di maggiore diffusività.

Si è ricordato in altra sede (10), come l'istituto della diffamazione sia stato quello interessato nell'ultimo mezzo secolo dal maggior numero di progetti di riforma - almeno un paio per ogni legislatura - arenatisi in una logica di veti contrapposti.

Di fronte a ciò, per tutti gli anni Settanta e Ottanta e per parte degli anni Novanta, lo sforzo maggiore degli interpreti è stato teso a verificare quante e quali di quelle previsioni pensate per la carta stampata potessero trovare applicazione rispetto a quello che era lo strumento emergente della comunicazione: la televisione.

Sembrava essere stato raggiunto un momento di buona certezza del diritto, dopo che la Cassazione si era pronunciata su questioni fondamentali, come nel 2001 sull'intervista (11) e nel 2008 su quella televisiva in particolare (12). Poi, però, c'è stata l'esplosione di *Internet*, uno strumento che ha modificato in maniera impensabile tempi e modi della diffusione agli altri delle notizie. E quindi

ha creato problemi fino a qualche anno impensabili di possibile lesione dell'altrui reputazione (13).

A fronte di ciò il quadro normativo è rimasto più o meno invariato. Ed anzi la situazione si è per certi versi ingarbugliata. Mentre le fonti di riferimento, fino a qualche decennio fa, erano infatti i codici penale e civile e la legge sulla stampa, oggi occorre tener conto di un altro diritto che è andato prepotentemente affermandosi negli ultimi decenni, che è quello sulla *privacy*, che ha trovato la sua codificazione in varie leggi succedutesi nel tempo (l. n. 675 del 1996, d.lg. n. 171 del 1998 e d.lg. n. 196 del 2003).

Può accadere, pertanto, di trovarsi oggi di fronte a casi e situazioni in cui non si faccia questione di una possibile lesione della propria reputazione, e quindi di un'avvenuta diffamazione, ma di una lesione del proprio diritto alla *privacy*. O, come nel caso di cui alla sentenza in commento, di entrambi.

2. Il caso google-vivi down

Il caso all'esame del giudice monocratico milanese - che ha proceduto, su richiesta degli imputati, nelle forme del giudizio abbreviato condizionato all'escussione del teste Jeremy Doig - è ormai noto ai più, anche per avere avuto, come detto, grande risalto sui *mass media* generalisti.

Il 24 maggio 2006 alcuni studenti dell'Istituto Tecnico di Torino girarono in classe un video dal contenuto davvero spregevole (e viene da chiedersi dove fossero gli insegnanti mentre ciò accadeva).

Le immagini, infatti, mostrano uno studente, mentre uno sferra qualche pugno e qualche calcio ad un compagno affetto da sindrome di Down, mentre altri stanno ad assistere compiaciuti, un'altra è intenta a riprendere la scena con la videocamera e un altro ancora a disegnare sulla lavagna il simbolo delle SS e a fare il saluto fascista.

I ragazzi scherniscono lo sfortunato compagno, poi rivolgono la loro attenzione all'improvvisata cineoperatrice: «Salve, siamo dell'associazione Vivi Down, un nostro mongolo si è cagato addosso e mò non sappiamo che minchia fare perché l'odore di merda ci è entrato nelle narici».

Tirano anche degli oggetti all'indirizzo del compagno che, per ripararsi, perde gli occhiali e si china affannosamente per cercarli, tra l'indifferenza del resto della classe.

Addirittura, ad un certo punto, la ragazza che gira il video irrompe in scena e dice: «Aspetta, rifatelo, non è venuto».

Immagini, insomma, da far rabbrividire.

Tra l'8 e il 10 settembre il video viene caricato da una minore (giudicata separatamente) su Google Video e vi rimane per due mesi, venendo visualizzato 5500 volte e - particolare non indifferente, ad avviso di chi scrive - viene collocato al primo posto tra i video più divertenti e al ventinovesimo posto tra quelli più scaricati.

Il 5 novembre 2006 - come si ricorda anche nella sentenza in commento - è un *blogger*, tal Alessandro D'Amato, a denunciare sul sito *www.ilcannocchiale.it*, la presenza del video su Google Video.

Non si sa se il *blogger* abbia inviato anche una segnalazione a Google Video sulla inopportunità della presenza del filmato, come afferma, o se la sua segnalazione sia stata correttamente recepita.

Di certo c'è che il giorno dopo tale Silvia Barabino richiede la rimozione del video tramite il Centro di assistenza Google.

Il 7 novembre analoga richiesta viene dalla Polizia Postale di Roma. E finalmente, quello stesso giorno, il video viene rimosso.

I genitori del ragazzo e i legali rappresentanti dell'associazione sporgono, però, querela. E nasce, *in primis*, un procedimento penale a carico della minore che aveva inserito il video *on line* e poi quello a carico dei legali rappresentanti di Google Italia e di Google Inc. deciso con la sentenza in commento.

Il primo reato ipotizzato è quello di diffamazione, sia in danno del minore che dell'associazione Vivi Down.

La responsabilità dei legali rappresentanti del *service provider* viene ipotizzata con riferimento all'art. 40 comma 2 c.p., per avere consentito, senza alcun controllo preventivo sul suo contenuto, che il video venisse immesso on line per la successiva diffusione a mezzo *Internet* attraverso le pagine del sito *http//video.google.it*

Secondo la prospettazione accusatoria in capo a tali soggetti vi era, dunque, un obbligo di garanzia di impedire l'evento lesivo dell'altrui reputazione, che veniva individuato nell'avere consentito che «venisse immesso per la successiva diffusione a mezzo *Internet*, attraverso le pagine del sito *http://video.google.it* e senza alcun controllo preventivo sul suo contenuto, un filmato in cui persone minorenni, in concorso tra loro, pronunciando la seguente frase «(...)» e ponendo in essere numerosi altri atti vessatori nei confronti di un loro coetaneo disabile, ledevano i diritti e le libertà fondamentali nonché la dignità degli interessati» (così testualmente il capo d'imputazione).

Con una ardita costruzione giuridica che il giudice non ha avallato in sentenza tale obbligo di garanzia veniva individuato con riferimento a tre norme del codice della *privacy* del 2003: gli artt. 13, 17 e 26 (14).

Gli imputati venivano rinviati a giudizio, in concorso tra loro, anche per il reato di cui all'art. 167 commi 1 e 2 d.lg. 30 giugno 2003, n. 196 (il cosiddetto codice della *privacy* nella sua più recente stesura) «perché, in concorso tra loro e nelle circostanze di fatto di cui al precedente capo, al fine di trarne profitto per il tramite del servizio Google Video (in relazione al quale Google Italy s.r./ beneficia degli indotti pubblicitari degli inserzionisti), procedevano al trattamento dei dati personali in violazione agli artt. 23, 17 e 26 stesso d.lg., con relativo nocumento per la persona interessata (...) In Milano, 8 settembre 2006 (data del video *upload*)».

Vi era poi, originariamente, una terza imputazione, relativa ad una falsa procura speciale, che il giudice milanese, evidenziata l'assenza di connessione ri-

spetto agli altri due reati, ha stralciato, provvedendo ad una declaratoria d'incompetenza territoriale ai sensi dell'art. 23 c.p.p. e rimettendo gli atti al P.M. presso il giudice competente (il Tribunale di Roma).

Nelle more del procedimento, il minore veniva risarcito, per cui veniva rimessa la querela e il giudice operava una pronuncia d'improcedibilità nei confronti degli imputati ai sensi degli artt. 469 e 129 c.p.p. per la diffamazione che vedeva il giovane disabile parte lesa.

Nel corso dell'udienza il giudice rigettava poi le questioni d'incompetenza territoriale sollevate dai difensori, sul presupposto che il più grave tra i reati connessi contestati (quello di cui all'art. 167 d.lg. n. 196 del 2003) era stato commesso in Milano, dove ha sede la società Google Italy indicata nel capo d'imputazione come responsabile dei comportamenti incriminati.

In realtà - va detto subito - suscita non poche perplessità la motivazione con cui il Tribunale di Milano ha ritenuto che vi sia stato un trattamento di dati personali anche in Italia da parte di Google Italia e non già solo da parte della statunitense Google Inc., il che avrebbe escluso la giurisdizione italiana.

Il ruolo attivo nel trattamento dei dati personali da parte di Google Italia viene, infatti, collegato alla circostanza che tale società, attraverso il sistema *AdWords* ed il riconoscimento di parole chiave, aveva sicuramente - secondo quanto si legge nella sentenza in commento - la possibilità di collegare, attraverso la creazione di *link* pubblicitari, le informazioni riguardanti i clienti paganti alle schermate di Google Video. E quindi in qualche modo di gestire, indicizzare e organizzare anche i dati contenuti in quest'ultimo sito, di fatto trattando i dati contenuti nei video caricati sulla piattaforma di Google Video, dei quali quindi viene ritenuta responsabile quanto meno ai fini del codice della *privacy*.

Le perplessità sono legate al fatto che, ai fini della competenza territoriale in materia di codice della *privacy*, viene riconosciuto alla società italiana un comportamento attivo che non si capisce come non sia stato poi valorizzato ai fini di una correità di tipo commissivo nella diffamazione. E in tal senso, se è vero che il giudice era vincolato alla prospettazione accusatoria, che ipotizzava una responsabilità di tipo omissivo, in relazione ad una posizione di garanzia condivisibilmente ritenuta insussistente, ben avrebbe potuto lo stesso ritenere il fatto diverso da come descritto nel decreto che aveva disposto il giudizio e disporre con ordinanza la trasmissione degli atti al pubblico ministero, per l'ulteriore corso, ai sensi del comma 3 dell'art. 521 c.p.p.

Ma sul punto ci si soffermerà più specificamente, in seguito

Quanto alla competenza per territorio in materia di diffamazione a mezzo *Internet* il giudice monocratico milanese si colloca nell'alveo della giurisprudenza di legittimità consolidatasi sul punto (15) ricordando come «... deve rilevarsi che il reato di diffamazione a mezzo *internet* (reato per così dire presupposto rispetto a quello contestato *sub* B) deve ritenersi commesso in modo contestuale con la semplice immissione del contenuto diffamatorio nella rete di connessione telematica denominata *internet*, a nulla rilevando che tale dato sia percepito

prima in un luogo piuttosto che in un altro; in tal senso, e di conseguenza, non può ritenersi percepito a Roma piuttosto che in un altro luogo il nocumento che la norma richiede come condizione di punibilità del fatto, se tale nocumento sia conseguenza di una comunicazione telematica a mezzo internet».

«In estrema sintesi - si legge ancora nella sentenza in commento -non appare rilevante che la prima persona identificata con certezza nella vicenda in questione sia stata una persona a Roma: sia la commissione del reato di diffamazione che la conseguente commissione del reato di illecito trattamento dei dati avvenuti tramite *internet*, non possono considerarsi commessi in un luogo per il solo fatto che in quel luogo l'offesa viene percepita; essendo la percezione dell'offesa un dato rilevante per la commissione del reato di cui all'art. 595 c.p., ma non dirimente ai fini della competenza territoriale».

3. Diffamazione, privacy e internet: due filosofie a confronto

Il problema che si è trovato ad affrontare il giudice nella sentenza in commento è quello con cui si va misurando la giurisprudenza di merito degli ultimi anni. E le risposte che stanno dando i tribunali italiani sono diverse e spesso contraddittorie.

Non crea problemi l'affermazione di responsabilità di chi introduca su *Internet* un contenuto - audio, video o scritto - lesivo dell'altrui reputazione o dell'altrui *privacy*.

Tali soggetti - com'è avvenuto nel caso che ci occupa per la minore che aveva operato l'*upload* dell'orribile video che vedeva oggetto di vessazioni il coetaneo disabile - vanno incontro a sicura responsabilità, penale e civile, indipendentemente dal mezzo che utilizzano per veicolare il loro messaggio lesivo dell'altrui diritto.

Su questo la giurisprudenza, sin dall'avvento di *Internet*, non ha mai nutrito alcun dubbio.

Ciò che crea, invece, problemi, è la verifica di come figure di responsabilità specificamente pensate per mezzi d'informazione diversi possano trovare applicazione anche per *Internet.*

È il caso, ad esempio, per quel particolare tipo di responsabilità per fatto altrui che l'art. 57 c.p. prevede per il direttore del giornale (16). O per la responsabilità solidale dell'editore.

Come si diceva, le risposte sono contraddittorie. E così, dopo che nel 2006 il Tribunale di Aosta aveva affermato l'equiparabilità del *blogger* al direttore di un giornale (17), la Corte d'Appello di Torino, il 23 aprile 2010, con una sentenza di cui quando questo contributo va in stampa si attendono le motivazioni, ha affermato il principio contrario.

E, ancora, la Cassazione si è pronunciata di recente nel senso di ritenere che gli interventi dei partecipanti ad un *forum* di discussione non possono rientrare nel concetto di stampa o di prodotto editoriale (18).

Tuttavia, come si è più ampiamente evidenziato in altra sede (19), la Suprema Corte ha valutato allo stato i *forum* di discussione. E null'altro. In altri ter-

mini, dall'affermazione di inapplicabilità delle guarentigie in materia di stampa a tale forma di dialogo telematico non può desumersi alcuna implicita affermazione che altro sia stampa. E nemmeno può operarsi un'affermazione a carattere estensivo che riguardi i *blog* o, ancora più in generale, i siti *web.*

Il sito *web* è una scatola. Per valutarne il contenuto - e quindi anche l'eventuale assimilabilità, nel bene e nel male, alla normativa sulla stampa - andrà analizzato di volta in volta cosa c'è dentro.

Su *Internet e* i suoi rapporti con diritti fondamentali, quali quello alla libera manifestazione del pensiero e quello alla tutela del proprio onore e della propria reputazione, dunque, non mancano in questi anni le pronunce giurisprudenziali.

E lo stesso legislatore non manca di prestare attenzione alla materia, anche se le tante proposte di legge e disegni di legge che si sono succeduti nel corso delle ultime legislature, soprattutto in materia di diffamazione, sono rimasti tali, non riuscendo ad essere approvati, bloccati in una logica di veti contrapposti trasversale agli stessi schieramenti politici.

Ciò è accaduto, però, anche perché, quando si parla di *Internet*, gli stessi giuristi sembrano perdere di vista il riferimento normativo e le regole del diritto per lasciarsi coinvolgere da quella che pare ormai diventata una sorta di guerra di religione.

Da un lato ci sono i fautori del *web* come luogo di massima espressione della libertà del singolo. E che quindi avversano ogni intervento legislativo o qualsivoglia interpretazione giurisprudenziale che propenda per un qualche controllo, preventivo o successivo, da parte di terzi dei contenuti che vengono immessi.

Dall'altro c'è chi individua come preminente il pericolo che un eccessivo permissivismo possa costituire il viatico per creare quella che lo stesso giudice estensore della sentenza in commento definisce «la sconfinata prateria di *Internet*, dove tutto è permesso e niente può essere vietato, pena la scomunica mondiale del popolo del web».

4. Il dibattito in dottrina sulla responsabilità dell' internet service provider

In dottrina è stato in più occasioni messo in rilievo come, fino ancora alla metà degli anni Novanta, non esistesse giurisprudenza significativa sulla responsabilità per la diffusione di notizie e messaggi attraverso *Internet*, se non negli Stati Uniti d'America (20).

Si è ricordata in altra sede, cui si rimanda (21), la condivisibile affermazione secondo cui «nel mondo di *Internet*, le caratteristiche proprie del mezzo di trasmissione delle comunicazioni e dei messaggi rende ardua anche l'identificazione dei vari soggetti» per cui «se è vero che ogni messaggio ha un autore, è anche vero che molto spesso tale autore resta sconosciuto, non solo a tutti gli altri utenti della Rete, ma anche alla stessa organizzazione che diffonde quel messaggio, si tratti di imprese di *on line services* o di fornitori di *bullettin board*». E «meno che mai è possibile individuare con certezza l'autore dei messaggi. che vengono diffusi attraverso le *chat lines*» (22).

Altro Autore ha sottolineato come vada guardato con attenzione il dibattito dottrinale sull'argomento sviluppatosi negli Stati Uniti in quanto si tratta del Paese «che, per intuibili ragioni, s'è più occupato, sia a livello d'elaborazione teorica, sia a livello di *law in action*, del problema della diffamazione *on line*, anche in forma anonima» (23).

Tale Autore evidenzia come «l'osservatore continentale, che rivolge lo sguardo oltreoceano, scorge un terreno solcato da una sottile linea d'ombra, che lo divide pressoché a metà» in quanto «in termini cronologici (....), i motivi dell'elaborazione statunitense degli ultimi dieci anni risultano scanditi da un importante provvedimento legislativo, il *Communications Decency Act* del febbraio 1996, a sua volta parte di una riforma più complessiva, che ha investito, con il Telecommunications Act,, l'intero sistema americano delle telecomunicazioni» (24).

Quanto all'inquadramento della figura dell'*internet service provider* e alla sua possibile punibilità a titolo di concorso come autore del reato di divulgazione in rete di contenuti illeciti, veniva condivisibilmente rilevato in dottrina già oltre un decennio or sono come la stessa «si limita a situazioni marginali, ove a tale soggetto sia attribuibile la paternità dei dati in questione o almeno la loro riconducibilità, qualora egli agisca come un moderatore di *newsgroup* o di una *mailing list* e quindi provveda al controllo dei messaggi pervenuti e decida in ordine alla successiva disponibilità di essi per gli utenti del servizio» e che «l'utilizzazione dello schema della responsabilità concorsuale risulta invece consentita nella ipotesi in cui sia dimostrabile che il *provider* abbia consapevolmente fornito l'accesso a dati illeciti da altri immessi in rete; situazione anche questa in grado di assumere una valenza assai limitata, a causa della difficoltà sia di provare il dolo del provider in riferimento ad un reato non ancora verificatosi, sia di derivare la sua responsabilità dalla consapevolezza sopravvenuta in ordine ad un reato già perfezionatosi nei suoi elementi essenziali» (25).

Va aggiunto che la quantità di dati veicolati rende impossibile, di fatto, al *provider* un controllo preventivo su quanto riversato in rete attraverso il *server* da lui gestito e quindi la scarsa praticabilità, in teoria, della strada di una sua responsabilità per colpa.

In termini fortemente critici verso una possibile applicabilità al *provider* di una forma di responsabilità analoga a quella prevista per il direttore del giornale si è espresso anche chi ha sottolineato come «l'art. 57 c.p. sia un ingiustificato residuo che appartiene ad un'epoca e ad un contesto storico ormai superati» in quanto «nel primo dopoguerra la stampa periodica aveva contenuti limitati, effettivamente controllabili da un unico soggetto, ed anche gli strumenti tecnici a disposizione, per la loro lentezza, consentivano una verifica reale della pubblicazione» (26).

Lo stesso Autore rilevava come già negli anni il panorama fosse profondamente mutato, con i contenuti delle testate giornalistiche che avevano subito un notevole incremento in proporzione diretta con l'avanzamento tecnologico che aveva consentito l'aumento notevole delle pagine e dei contenuti di ciascuna

pubblicazione, la simultanea pubblicazione in diverse regioni o province del giornale, anche con inserti di cronaca locale destinati alla sola diffusione periferica. E già ciò aveva talmente incrementato i contenuti che la materiale capacità di controllo di un unico soggetto appariva irrealizzabile o meramente virtuale.

La questione si pone in termini accentuati - veniva ancora notato - per le figure professionali di *Internet* «i cui contenuti sono esponenzialmente più vasti e soprattutto continuamente mutevoli, ciò che rende impraticabile qualsiasi imposizione di controllo, sia umano sia - all'attuale stato del progresso tecnologico - automatizzato» derivandone che «il principio d'inesigibilità assurge (...) a criterio guida della soluzione negativa che esclude - in termini di politica criminale - la legittimità costituzionale (in relazione al principio di colpevolezza) dell'introduzione di fattispecie penali proprie degli operatori telematici impositive di obblighi di controllo penalmente sanzionati sui contenuti delle trasmissioni diffuse e dei dati immessi da terzi».

Sviluppando tale tesi taluno ha ritenuto possibile una responsabilità penale a titolo di colpa del gestore del sito per quanto su di esso pubblicato, ma sempre escludendo la possibilità di estenderla al *service provider* o al *webmaster*.

È stato affermato in proposito che ciò vale «a meno che il provider assuma volontariamente l'obbligo di filtrare e controllare preventivamente il materiale inviato in rete per mezzo del suo *server*, infatti, un tale obbligo non avrebbe fondamento giuridico, non derivando da alcuna disposizione di legge» (27). Secondo tale Autore «non sarebbe possibile, peraltro, individuare una posizione di garanzia, in quanto, a differenza di quanto si verifica in relazione al titolare di un singolo sito, il dovere di controllo si presenterebbe, di fatto, inattuabile» in quanto «per fare un esempio facilmente intuibile, sarebbe come pretendere che l'Ente Poste controlli il contenuto dei plichi e dei pacchi trasmessi per suo tramite, o la Telecom il tenore delle telefonate effettuate con le sue linee telefoniche».

5. La pronuncia milanese nel solco dei precedenti giurisprudenziali in materia

Nella giurisprudenza italiana, del problema della possibile sussistenza di una responsabilità penale degli *Internet provider* (in quel caso per la fattispecie delittuosa di cui all'art. 600-*ter* comma 3 c.p.), si è occupato per primo il Tribunale di Milano nel 2004 (28).

Il caso vedeva imputato l'intestatario di un sito, strutturato secondo le peculiarità ed il meccanismo dei motori di ricerca telematici, attraverso il quale lo stesso si limitava a fornire un mero collegamento ipertestuale (il cosiddetto *link*) ad altro sito *Internet*, mediante il quale venivano diffuse e rese disponibili in rete immagini a contenuto pedopornografico, accessibili dunque a chiunque si collegasse a tale ultimo spazio virtuale, selezionasse specifici sottomenu ed infine risolvesse un semplicissimo enigma.

In quel caso, dunque, l'imputato si era limitato a svolgere un'opera di mero supporto tecnico formale nella divulgazione di materiale (illecito) da altri (pre-

cisamente: il c.d. *content provider*, «ospitato» sul sito dell'imputato) immesso in rete, mettendo invero a disposizione il proprio *server* per la ricezione di tali dati.

Ebbene, secondo il Tribunale di Milano, che assolse l'imputato, i proprietari delle infrastrutture di telecomunicazione (c.d. *network provider*), i fornitori di accessi (c.d. *access provider*) ed i fornitori di servizi (c.d. *service provider*), non possono ritenersi corresponsabili dei reati commessi da coloro che utilizzano i loro servizi (c.d. *content provider*) per mera omissione di controllo, in quanto, da una parte, non hanno un obbligo giuridico di evitare l'evento, e dall'altro, per la struttura stessa della rete, non hanno la possibilità concreta di esercitare un efficace controllo sui messaggi ospitati sul proprio sito.

Nell'occasione si affermò anche che non può nemmeno ritenersi una responsabilità dei medesimi soggetti a titolo di dolo eventuale, ogni qualvolta non vi siano specifici elementi che consentano di ricondurre nella loro sfera di conoscibilità una specifica attività illecita commessa per loro tramite e ciò per la struttura aperta di *Internet*, che rende in astratto possibile immissioni costanti, autonome e non controllabili sugli spazi gestiti dal *server*.

Nello specifico, già allora il tribunale meneghino si pose il problema che «per sostenere la responsabilità a titolo di omissione del *service* o *host provider* occorre affermare a suo carico un obbligo giuridico di impedimento (in questo caso non già dell'evento ma della stessa condotta illecita del *content provider*) e quindi da un lato una sua posizione di garanzia e dall'altro lato una possibilità effettiva di controllo preventivo sul contenuto dei messaggi».

Ma tale posizione di garanzia - osservò allora come oggi il Tribunale di Milano - non è ravvisabile nel diritto vigente, stante «la assenza di una previsione specifica in tal senso e la non applicabilità in via analogica - *in malam partem* - degli artt. 57 e 57-*bis* c.p. (riguardanti il direttore della stampa periodica ed anche l'editore e stampatore nel caso di anonimità o non imputabilità dell'autore degli scritti illeciti)».

«Né la posizione di garanzia può argomentarsi sostenendo l'esercizio precedente da parte di detto *provider* di un'attività pericolosa -sosteneva ancora il Tribunale di Milano nel 2004 - in quanto tale non può considerarsi la sua offerta di uno spazio web e l'apertura di un *link* con un determinato sito che rappresenta un'azione consentita e del tutto neutra per il diritto penale».

Già in quella pronuncia si osservava poi, condivisibilmente, come non fosse ravvisabile la possibilità concreta di esercitare un efficace controllo sui messaggi ospitati sul proprio sito visto l'enorme afflusso dei dati che transitano sui *server* e la possibilità costante di immissione di nuove comunicazioni anche attraverso collegamenti alternativi, proprio per la struttura aperta di *Internet* che non rappresenta alcun unitario sistema centralizzato, ma una possibilità di molteplici connessioni fra reti e *computer* diversi.

La conseguenza fu anche allora quella di non poter fondare un giudizio di responsabilità del *service* e *host-access provider* sotto il mero profilo omissivo.

Quella sentenza, però, offriva uno spunto di riflessione interessante per casi come quello di cui alla sentenza oggi in commento. Si leggeva ancora, infatti, nella pronuncia milanese del 2004 che «d'altra parte si potrebbe sostenere che anche il *service provider* divulga o comunque agevola la divulgazione di dati illeciti» e si precisava che «perché si possa configurare un contributo causale all'illecito del *content provider* da parte del *server* occorre che quest'ultimo si sia inserito nella divulgazione del messaggio con un *quid pluris* rispetto alla sua solita attività, con una interazione con detto sito» e che «deve inoltre verificarsi se il dolo *dell'access* e/o *service provider* abbia ad evidenziarsi attraverso le modalità di svolgimento del servizio da lui prestato (e cioè se si riscontri un dolo di partecipazione od un'oggettiva possibilità di impedire la commissione del reato di cui abbia avuto comunque notizia)» (29).

In dottrina venne rilevato in sede di commento alla pronuncia milanese che «ai fini del riconoscimento della sussistenza di un obbligo giuridico di impedimento dell'evento in capo al *service* (od, a fortiori, all'*host provider*) appare necessario individuare nella funzione dallo stesso svolta la titolarità di una posizione di garanzia, nonché l'esigibilità di un controllo preventivo, da parte dell'*Internet provider*, in ordine alla liceità dei contenuti dei messaggi e delle informazioni trasmesse all'interno dello spazio virtuale» (30).

Lo stesso Autore rilevava, peraltro, come «l'intrinseca diversità dei requisiti dei tradizionali mass media rispetto a quelli dei canali telematici di informazione - caratterizzati dall'assenza di fisicità del mezzo di trasmissione, nonché dalla costante modificabilità dei contenuti veicolati, suscettibili di continue integrazioni ad opera di utenti operanti dall'esterno del sito di riferimento - dimostra peraltro in maniera inequivocabile la natura analogica (e non già meramente estensiva) di ogni applicazione della disciplina dei reati commessi con il mezzo della stampa all'ipotesi di comunicazioni illecite online» e perciò «benché diverse pronunce giurisprudenziali abbiano esteso alle c.d. «testate telematiche» la disciplina amministrativa o civilistica inerente gli illeciti commessi con il mezzo della stampa, pertanto equiparando, ai fini del regime giuridico applicabile, gli organi di stampa ai siti *Internet*, siffatta operazione esegetica appare preclusa, in materia penale, dai principi di stretta legalità e di tassatività della norma incriminatrice».

Altro Autore, sempre in sede di commento alla sentenza del Tribunale di Milano del 2004, rilevò come «la soluzione adottata - esclusione di un'automatica e necessariamente accessoria responsabilità del provider per l'altrui reato - appare sostenuta da una corretta esegesi della normativa vigente e risulta equilibrata anche nell'ottica politico-criminale» (31)

Nel rilevare come su tale crinale «si muovono le tentazioni di introdurre - in via interpretativa o legislativa - forme di responsabilità del provider per i contenuti illeciti da altri immessi nella rete» il medesimo Autore sviluppava una serie di condivisibili argomentazioni che meritano di essere ricordate.

Veniva infatti rilevato come costituissero ineludibile sfondo di soluzioni contrapposte a quelle del tribunale di Milano le delicate problematiche che le

comunicazioni attraverso *Internet* pongono e come da un canto la telematica avesse rivelato «una vocazione criminogena, quale agevole strumento di commissione per una notevole e differenziata serie di reati (dalla pedopornografia, alla violazione del diritto di autore, ai reati tipicamente informatici, alle truffe commerciali)» e dall'altro si palesasse «un'accentuata difficoltà probatoria ed investigativa per l'individuazione dell'autore del reato».

Veniva già evidenziato all'epoca dal Corrias Lucente - e oggi ciò è reso ancora più sostenibile alla luce delle avanzate tecnologie - come il reo potesse «godere e contare sulla possibilità di conservare l'anonimato». Scriveva infatti tale Autore nel 2004: «è sufficiente rilevare che il computer che si collega in rete è identificabile attraverso l'indirizzo IP (*Internet* protocollo) composto da nome, numeri e codici, strutturati secondo sequenze predeterminate. Se tale sistema è destinato a garantire l'identificazione del computer, è ormai evidente che esistono strumenti capaci di ostacolare o mascherare l'identificazione del computer o del singolo utente. Inoltre, va notato che attraverso l'IP si può (seppure con le difficoltà evidenziate) identificare il computer, ma non ancora la persona che lo abbia utilizzato a scopo illecito: ciò che risulta impervio nel caso di elaboratori aziendali condivisi da più dipendenti e nell'ipotesi in cui al provider vengano fornite false generalità».

Perciò - si concludeva - «dinanzi alla possibilità che il reo resti ignoto ed il reato impunito è parsa a taluno allettante (e le incriminazioni lo confermano) l'ipotesi di riversare la responsabilità su un soggetto agevolmente identificabile: l'operatore professionale di *internet*, ipotizzando forme di responsabilità automatica ed accessoria rispetto a quelle proprie dell'autore del reato. Da tale impostazione rifugge la sentenza, che esclude la correttezza di soluzioni che estendano automaticamente o trasferiscano la responsabilità sugli operatori di *internet* per i contenuti da altri inseriti nella rete» (32).

Nel solco dell'impostazione del Tribunale di Milano si mosse tre anni dopo una interessante pronuncia del Tribunale civile di Lucca (33).

A rivolgersi in via cautelare al tribunale toscano era stata una società commerciale per ottenere, a cura e spese di un'altra società, la rimozione di alcuni messaggi a suoi dire diffamatori perché mettevano in cattiva luce alcun prodotti commercializzati dalla ricorrente.

Tali messaggi erano pubblicati su un *newsgroup* non moderato *(it.comp.reti.wireless*) da un indirizzo IP risultato assegnato alla società chiamata in giudizio di cui si chiedeva anche la contestuale «cessazione» dell'utilizzo.

La società convenuta si attivava immediatamente, per quanto di sua competenza, sospendendo l'utilizzo dell'indirizzo IP sopra indicato, circostanza che però di per sé non era risolutiva del problema prospettato dalla società ricorrente posto che, trattandosi di indirizzo dinamico, esso veniva assegnato di volta in volta, in via automatica, ai vari utenti che si connettevano tramite il servizio e dunque non era idoneo ad impedire ulteriori connessioni da parte dell'autore dei messaggi con numeri IP diversi. Essendo in ogni caso la società convenuta nell'impossibilità materiale di rimuovere i messaggi diffamatori dal *newsgroup*,

in quanto tale operazione era di pertinenza esclusiva di Google, veniva chiamata in causa anche Google Italia srl.

Quest'ultima, a sua volta, non vi provvedeva ritenendosi estranea ai fatti e indicando Google Inc., con sede in California, unica società legittimata a farlo in quanto responsabile del motore di ricerca e dei relativi servizi, incluso quello di accesso e gestione del *newsgroup* in questione.

Il Tribunale di Lucca, tuttavia, rigettava il ricorso, non solo escludendo la responsabilità di Google Italia srl, ma anche di Google Inc., sostenendo che la società resistente si era «limitata a fornire la connessione alla rete e l'operatore che consente agli utenti di accedere ai *newsgroups* (riconducibile nella specie a Google) non può essere ritenuto responsabile per i messaggi che passano attraverso i propri elaboratori in quanto si limita a mettere a disposizione degli utenti lo spazio virtuale dell'area di discussione e non ha alcun potere di controllo e di vigilanza sugli interventi che vi vengono man mano inseriti; diversamente si verrebbe ad introdurre una nuova ed inaccettabile ipotesi di responsabilità oggettiva, in aperta violazione alla regola generale di cui all'art. 2043 c.c. che, come è noto, fonda la responsabilità civile sulla colpa del danneggiante».

Del resto, secondo quanto argomentato dal giudice toscano, in linea con tale impostazione è il d.lg. n. 70 del 2003 che sancisce l'assenza dell'obbligo generale di sorveglianza del provider sulle informazioni che trasmette o memorizza né prevede a carico di questi un obbligo di ricercare circostanze che indichino il compimento di atti illeciti.

Peraltro la conclusione del Tribunale di Lucca era che «indubbio che la responsabilità per i contenuti dei messaggi è, in linea astratta, attribuibile solo agli autori degli stessi» occorreva rilevare per completezza come, nel merito, «non vi fossero allo stato elementi concreti per ritenere che i messaggi in questione avessero una natura diffamatoria - sostanziandosi essi in giudizi sulle caratteristiche squisitamente tecniche dei prodotti (...) (e dunque manifestazione del diritto di critica) inseriti in un forum, e dunque in linea con i toni informali che caratterizzano lo scambio diretto di opinioni su *Internet*» (34).

La sentenza in commento si pone nel solco degli unici due precedenti italiani di cui si è detto.

Il giudice milanese, quasi a volerne rafforzare la portata, ripete la stessa identica frase in due passaggi della sentenza, a pag. 95 e a pag. 103: «non esiste, a parere di chi scrive, perlomeno fino ad oggi, un obbligo di legge codificato che imponga agli ISP un controllo preventivo della innumerevole serie di dati che passano ogni secondo nelle maglie dei gestori o proprietari dei siti web, e non appare possibile ricavarlo *aliunde* superando d'un balzo il divieto di analogia *in malam partem*, cardine interpretativo della nostra cultura procedimentale penale».

6. Il codice del commercio elettronico del 2003 e i vari tipi di internet service provider

Non è possibile, tuttavia, non associarsi a quanti hanno ritenuto la pronuncia milanese in commento un'occasione mancata per meglio addentrarsi nella qualificazione di un *internet service provider* qual è Google.

Soprattutto perché sarebbe stato lecito attendersi, al di là delle tante considerazioni *de iure condendo*, che da parte del giudicante venisse maggiormente esplicitato il proprio pensiero circa la collocazione del caso in oggetto, e dei soggetti processuali coinvolti, rispetto alla pur perfettibile - ma allo stato è l'unica che abbiamo - disciplina che ne differenzia ruoli e responsabilità, e cioè quella sul commercio elettronico del 2003.

La stessa Procura di Milano - va detto - ha escluso *ab initio*, nel caso in esame, una possibile applicabilità di tale normativa, in virtù delle clausole di salvaguardia relative alla disciplina sulla *privacy* contenute nella direttiva comunitaria n. 31/2000 sull' *e-commerce* (35). Tuttavia - è stato acutamente rilevato (36) - «è evidente che gli Stati membri siano chiamati a garantire la contestuale applicazione delle due discipline -*privacy* ed *e-commerce* - e non già semplicemente -come sembrerebbe erroneamente ritenere la Procura di Milano - a far sì che la disciplina sulla privacy prevalga sistematicamente su quella in materia di *e-commerce* di modo che, ad esempio, tutti gli intermediari della comunicazione debbano perdere tale loro qualifica soggettiva ed assumere quella di titolari del trattamento in ogni ipotesi nella quale la loro attività abbia ad oggetto dati personali». Ne consegue, per tale Autore, condivisibilmente, che il senso delle clausole di salvaguardia in questione «sia più semplicemente e realisticamente», quello di chiarire che la disciplina sull'*e-commerce* «non vada applicata in luogo di quella sulla *privacy* nelle aree di possibile sovrapposizione, ma piuttosto in concorso con essa» e che «in altre parole, un intermediario della comunicazione rimane tale anche quando tratta dati personali e se tali dati sono nella disponibilità giuridica e fattuale dell'utente che è libero di aggiornarli e rimuoverli - così come avviene nel caso di *upload* di un video su qualsivoglia piattaforma UGC - non vi è alcuna ragione per trasformare l'intermediario in titolare di un trattamento che, in realtà, esso non gestisce se non da un punto di vista strettamente tecnico» (37).

Eppure, a voler sintetizzare la tesi portata avanti dalla pubblica accusa - che, come è stato acutamente rilevato, se fatta propria dal giudice sarebbe stata «ancor più dirompente di quanto non sia stata la decisione del Tribunale» (38) Google Italy avrebbe dovuto essere condannata, per diffamazione e violazione della privacy, in quanto si tratterebbe di una particolare figura di *host provider* - definito *host* attivo - improntato ad un chiaro fine lucrativo per massimizzare il quale avrebbe consentito una disinvolta inserzione *on line* di contenuti audiovisivi leciti e illeciti.

La Procura, dunque, di fatto operava una classificazione di Google Italia tra i vari tipi di *internet service provider*, anche se poi finiva per ritenere inapplicabile la normativa in materia di commercio elettronico in ragione della specifica clausola di salvaguardia a favore della legge sulla *privacy*, non ritenendo di aderire all'interpretazione di cui si è detto poc'anzi.

E invece quella normativa andava probabilmente tenuta in maggior considerazione. Sia dalla pubblica accusa che dal giudice.

Come si ricordava in precedenza della materia dei profili di responsabilità per gli operatori di *Internet* si è occupata la direttiva n. 31 del 2000 del Parlamento europeo «sul commercio elettronico» («relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico nel mercato interno»), che ha trovato attuazione nel nostro Paese prima con la legge delega 1 marzo 2002, n. 39 e poi attraverso il d.lg. 9 aprile 2003, n. 70 in vigore dal 14 maggio 2003.

Con tale intervento legislativo sono state fissate le condizioni per riconoscere la responsabilità del provider nell'ambito del commercio elettronico.

È stato condivisibilmente sottolineato in proposito dalla dottrina (39) che le soluzioni adottate ed i criteri introdotti manifestano, tuttavia, capacità di applicazione generalizzata «per la ragionevolezza e la praticabilità loro sottesi» e come «la normativa si innesta in un quadro generale che ribadisce la libertà della telematica e che fornisce la cornice di riferimento anche per la riflessione penalistica».

Altri ha tuttavia evidenziato, in termini critici, di essere «deluso e, soprattutto, preoccupato soprattutto per un motivo: con una tecnica di redazione legislativa di bassissimo livello, il nostro legislatore si è limitato ad un vero e proprio "copia e incolla" del (necessariamente generico) testo italiano della direttiva, senza il benché minimo intervento di adattamento ai nostri principi giuridici» (40)

La direttiva europea e la legge di attuazione, nel solco tracciato dalla dottrina, hanno previsto specifici obblighi e responsabilità (civili) per gli operatori di *internet*, attraverso una tipizzazione di responsabilità per fatto proprio.

A proposito della responsabilità del provider il d.lg. 9 aprile 2003, n. 70 (in G.U. 14 aprile 2003, suppl. ord. n. 61) prevede quattro norme.

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

In sede di commento all'intervento legislativo *de quo* è stato sottolineato come in tale norma «l'irresponsabilità è collegata al ruolo passivo ed automatico svolto dall'operatore» e come «alcune delle condotte che danno luogo alla responsabilità possono tradursi, in termini penalistici, in attività di concorso commissivo (ad esempio, può esservi riconducibile l'attività di selezione delle informazioni che implichi la conoscenza dei contenuti illeciti e, dunque, la loro volontaria diffusione, comportando la sussistenza delle componenti della fattispecie concorsuale» (41).

Ed è proprio questo il punto che, come si avrà modo di dire, può fornire uno spunto di riflessione sul caso affrontato nella sentenza in commento.

L'art. 15 d.lg. n. 70 del 2003 regola l'attività di *caching* (memorizzazione temporanea, automatica ed intermedia per attuare il successivo inoltro a richiesta dei destinatari) prevedendo che «1. Nella prestazione di un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, il prestatore non è responsabile della memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta, a condizione che: a) non modifichi le informazioni; b) si conformi alle condizioni di accesso alle informazioni; c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore; d) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni; e) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione. 2. L'autorità giudiziaria o quella amministrativa aventi funzioni di vigilanza può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse».

In relazione a tale norma è stato condivisibilmente rilevato come «soltanto taluni dei comportamenti fonte della responsabilità civile sono trasferibili sul piano penalistico» in quanto «la norma (...), tipicizza la diligenza del provider, e delinea ipotesi colpose, raramente configuranti illecito penale» (42).

L'art. 16 disciplina l'attività di *hosting* (memorizzazione duratura delle informazioni per renderle disponibili in rete), che costituisce «l'attività più penetrante è regolata in modo più severo, perché il *server* non svolge un ruolo meramente passivo e la memorizzazione stabile accresce (seppure non rende automatica) le possibilità di conoscenza del materiale illecito» (43).

La norma prevede che: «1. Nella prestazione di un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto

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

Secondo la lettera *a*) di tale disposizione, dunque, vi è una rilevante differenza fra l'effettiva conoscenza (che integra evidentemente anche corresponsabilità penali per le informazioni costituenti reato) e «la conoscenza di meri fatti che rendano manifesta l'illiceità dell'informazione» rispetto alle quali è introdotta l'eloquente limitazione alle azioni risarcitorie. Si potrebbe così ritenere che per la responsabilità penale è necessario il dolo diretto (l'effettiva conoscenza) mentre ipotesi dolose di grado inferiore non avrebbero rilevanza. E perciò si è sostenuto che la previsione legislativa comporti l'estensione della responsabilità civile anche al caso (penalmente irrilevante) in cui il prestatore non si sia accorto di fatti o circostanze indicativi della manifesta illiceità dell'informazione, ricostruendo così in chiave di colpa professionale la responsabilità civile dell'*hosting provider*.

La norma in tal senso è stata ritenuta «fondamentale perché richiede l'effettiva conoscenza dei contenuti illeciti, e contribuisce a limitare il ricorso al dolo eventuale in chiave incriminatrice» (44).

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

Dunque, la norma fa proprio un principio generale (corrispondente a quello affermato nella sentenza in commento e già prima in quelle di cui di è detto del Tribunale di Milano del 2004 e del Tribunale di Lucca del 2007) che i *provider*, nel prestare i servizi di trasporto, memorizzazione temporanea e *hosting* non hanno un obbligo generale di controllo delle informazioni memorizzate e di ricerca dei reati commessi attraverso la rete.

Vista nell'ottica del giudice civile tale previsione fissa un chiaro «paletto» rispetto alla possibilità per il *provider* di fare ricorso a criteri di imputazione meramente oggettivi, assimilabili a quelli previsti dagli artt. 2050 e 2051 c.c. ed impone di inquadrare la responsabilità del *provider* in termini di colpa professionale.

Nell'ottica penalistica - che in questa sede maggiormente interessa - sancisce da parte del legislatore il riconoscimento dell'insussistenza in capo al *provider* di una posizione di garanzia, capace di integrare il presupposto applicativo dell'art. 40 cpv. c.p.

L'art. 17, al comma 2, impone, tuttavia al *provider* obblighi di cooperazione e di informazione dell'autorità giudiziaria delle attività illecite scoperte o sulle quali si svolgono accertamenti giudiziari, ma la norma non indica le conseguenze dell'omissione o dell'inottemperanza che, dunque, allo stato appaiono penalmente perseguibili con riferimento al reato di favoreggiamento.

A proposito del comma 1 dell'art. 17 è stato sottolineato in dottrina che esso non introduce «nulla di nuovo rispetto all'ordinamento esistente», ma che «la disposizione è importantissima perché consente di stabilire che qualsiasi diversa prescrizione (per esempio, a proposito della lotta alla pedofilia) sarebbe contraria alle disposizioni comunitarie, oltre che al senso comune» (45).

La legge sul commercio elettronico del 2003 ha dunque animato il dibattito circa una possibile applicabilità dell'art. 40 comma 2 c.p., e dunque circa la sussistenza, in capo al prestatore, di un obbligo giuridico «di garanzia di impedire l'evento» (evento coincidente con il reato commesso da terzi).

Ciò perché, come è stato ricordato (46) «il decreto in commento non prevede ipotesi di reato specifiche (abbozza un precetto, ma tace su eventuali sanzioni di carattere penale), mentre nel nostro ordinamento non è previsto un generico obbligo, in capo al semplice cittadino, di denunciare o, addirittura, impedire la commissione dei reati (...) in buona sostanza, non è punibile la mera connivenza».

In relazione all'impianto complessivo della normativa è stato da più parti evidenziato come, in buona sostanza, ad analizzare il testo i fornitori di servizi finiscono per non avere alcuna responsabilità per i contenuti immessi in rete, a condizione che non intervengano in alcun modo sui contenuti immessi in rete, il che è già ampiamente previsto dal nostro ordinamento (e da qualsiasi altro ordinamento di un paese democratico).

È stato, però, condivisibilmente evidenziato come «tuttavia la formulazione delle norme è tale da ingenerare non poche perplessità in relazione alla natura degli interventi dei fornitori di servizi, perché è noto che le attività di trasmis-

sione e instradamento delle informazioni comportano sempre qualche forma di "intervento" che potrebbe rientrare tra le cause di non esenzione della responsabilità» per cui pare «ovvio che, ai fini dell'attribuzione di una responsabilità, il giudice indagherà su quello che i giuristi chiamano "l'elemento soggettivo dell'illecito", dovrà cioè stabilire se l'intervento del *provider* sui contenuti sia una mera operazione tecnica o se vi sia l'intenzione di influire in qualche modo sui contenuti stessi: solo in questo caso si potrà parlare di responsabilità del fornitore» (47).

Si temeva, dunque che l'intervento legislativo del 2003 potesse aprire la strada ad una giurisprudenza di maggior rigore in termini di possibile responsabilità penale dell'*internet service provider.*

Un grido d'allarme in tal senso era stato lanciato dalla *Associazione per le libertà nella comunicazione elettronica interattiva* (ALCEI) (48), che aveva sottolineato la pericolosa linea di tendenza emergente soprattutto a livello europeo, dove «dietro le formule "buoniste" e le astratte dichiarazioni di principio contenute nelle direttive europee 2000/31/CE e 2001/29/CE (...) - si nasconde il pericoloso mutamento dei principi giuridici sulla responsabilità dell'*internet provider* e, più in generale, dei fornitori di servizi *internet*» ed aveva evidenziato come «il *provider* viene, di fatto, trasformato in un giudice-poliziotto, che per evitare di essere chiamato a rispondere in prima persona del comportamento illecito degli utenti, sarà costretto ad esercitare censure, filtraggi e controlli più o meno palesi su quanto accade nei propri *server*».

E tale preoccupazione era stata condivisa anche da chi in dottrina aveva rilevato come «l'esperienza insegna che disposizioni così generiche costituiscono un pericolo non trascurabile: non è comunque positivo che un'assenza di responsabilità sia sancita da un giudice al termine di un'istruttoria o addirittura di un processo, laddove una norma più chiara eviterebbe all'origine l'intervento dell'autorità giudiziaria» (49).

Alla luce della pronuncia in commento, tuttavia, tale preoccupazione sembrerebbe essere infondata.

Il giudice monocratico milanese, infatti, non opera alcun riferimento alla legge sul commercio elettronico, neppure per escluderne l'applicabilità, secondo la tesi sostenuta dalla pubblica accusa.

Si legge, invece, nella sentenza in commento, che poco varrebbe la distinzione operata da PM e difensori tra *host provider* e *content provider*, nel senso evidente di ritenere che quanto alla disciplina sulla *privacy* intermediari della comunicazione (*host provider*) e non intermediari (*content provider*) sarebbero soggetti ai medesimi obblighi e responsabilità.

Per giungere a tale affermazione, tuttavia, il Tribunale di Milano pare introdurre un assioma extragiuridico, quello già richiamato secondo cui «non esiste in materia una zona franca» e soprattutto «non esiste nemmeno la «sconfinata prateria di *internet*» dove tutto è permesso e niente può essere vietato, pena la scomunica mondiale del popolo del web».

Eppure in altro punto della sentenza lo stesso Tribunale di Milano sembra prendere una posizione chiara circa la classificazione di Google riconoscendo che «è ... ovvio che l' *hoster* attivo o il *content provider* che dir si voglia avrà certamente un livello di obblighi e di comportamenti più elevato di quello di un semplice *host provider* o *service provider* o *access provider*: lo rende inevitabile il suo diventare *dominus* di dati che, per il solo fatto di essere organizzati e quindi selezionati e quindi "appresi", non sono più il flusso indistinto che non si conosce e che non si ha l'obbligo di conoscere».

Però - secondo quanto di legge ancora a pag. 95 della sentenza in commento «tale fatto, non crea una specie di effetto a catena che fa dell'*hoster* attivo automaticamente il corresponsabile di tutti i reati che gli *uploaders* hanno commesso comunicando e caricando i dati in loro possesso» perché «in tutti questi casi varranno, come in effetti valgono, le normali coordinate interpretative e valutative che si usano per ogni tipo di reato che il legislatore ha inteso codificare nel codice penale o nelle leggi complementari, sia da un punto di vista oggettivo che soggettivo».

«Nel caso in esame - scrive ancora il giudice monocratico milanese - se è ben vero che un *hoster* attivo (come nel caso Google Italy) ha sicuramente più elementi per poter riconoscere l'esistenza di un reato commesso da un singolo *uploader*, ed ha, inoltre, sicuramente degli obblighi che la legge gli impone per il trattamento dei dati sensibili dei soggetti che vengono "caricati" sul suo sito web, è altrettanto vero che non può essere imposto (perché irrealizzabile) allo stesso un obbligo generale e specifico di controllo su tutti i dati "sensibili" caricati (obbligo impossibile) se non altro, perché si imporrebbe ad un terzo la preventiva conoscenza di tutti i dati personali e particolari di tutte le persone che ogni momento "transitano" sul web)».

Quello che invece il Tribunale di Milano ritiene si possa e si debba imporre al *provider* è «un obbligo di corretta informazione agli utenti dei conseguenti obblighi agli stessi imposti dalla legge, del necessario rispetto degli stessi dei rischi che si corrono non ottemperandoli (oltre che) naturalmente, l'obbligo di immediata cancellazione di quei dati e di quelle comunicazioni che risultassero correttamente segnalate come criminose».

7. La (contraddittoria rispetto all'assoluzione per diffamazione) condanna per il reato di cui all'art. 167 del Codice della privacy

Punto nodale della pronuncia in commento, secondo lo sviluppo di tale tesi, è quello in cui si afferma che Google Italy sarebbe responsabile di violazione della disciplina sulla *privacy* perché, nell'ambito di un'attività svolta con finalità lucrativa, non avrebbe avvertito in maniera sufficientemente chiara la ragazzina che ha caricato *on line* il video della necessità di prestare attenzione al rispetto della *privacy* di colui che ne era, suo malgrado, il protagonista.

Scrive, infatti, il giudice monocratico milanese a pag. 96 della sentenza in commento che: «Non costituisce condotta sufficiente ai fini che le legge impone, «nascondere» le informazioni sugli obblighi derivanti dal rispetto della leg-

ge sulla *privacy* all'interno di «condizioni generali di servizio» il cui contenuto appare spesso incomprensibile, sia per il tenore delle stesse che per le modalità con le quali vengono sottoposte all'accettazione dell'utente» ed aggiunge che «tale comportamento, improntato ad esigenze di minimalismo contrattuale e di scarsa volontà comunicativa, costituisce una specie di «precostituzione di alibi» da parte del soggetto/web e non esclude, quindi, una valutazione negativa della condotta tenuta nei confronti degli utenti».

Il reato per cui si è pervenuti ad un'affermazione di penale responsabilità è quello di cui all'art. 167 d.lg. 30 giugno 2003, n. 196 (codice della *privacy*), sul trattamento illecito di dati personali (50).

Ebbene, appaiono assolutamente condivisibili le perplessità avanzate da chi (51), in dottrina, ha rilevato: «Francamente - ed a prescindere da qualsivoglia considerazione giuridica che si fa persino fatica ad intessere in relazione a tale conclusione - trovo tale passaggio, pure determinante, contraddistinto da una buona dose di formalismo giuridico o se preferite «ipocrisia ideologica»: si può davvero ipotizzare che se Google nelle proprie condizioni generali di utilizzo del servizio avesse avvertito, in caratteri più grandi e magari in grassetto, una bambina di dodici anni dell'esigenza di assicurarsi il consenso al trattamento dei dati personali del bambino disabile protagonista del video caricato, questa vi avrebbe provveduto*?*»

È stato, d'altro canto, sottolineato anche come «la motivazione, peraltro, non dice quali criteri avrebbero dovuto essere osservati nell'informativa per ritenerla, invece corretta: si limita a constatare che era insufficiente e intenzionalmente non era stata adeguatamente evidenziata (...) Google, in pratica, avrebbe scientemente inserito informazioni relative agli obblighi in materia di *privacy* nei propri servizi solo a fini di cautela legale ma, in concreto, per il giudice non erano sufficienti a informare in modo effettivo l'utente» (52).

È assolutamente da fare propria - e su ciò va sgombrato il campo da qualunque dubbio - la ritenuta insussistenza, nella sentenza in commento, di un obbligo di garanzia in capo all'*internet service provider* e la conseguente assoluzione operata dal giudice milanese per il delitto di diffamazione.

Non si può, tuttavia, non sottolineare la contraddizione che pare emergere nella stessa pronuncia laddove, per contro, si afferma che c'era un obbligo di garanzia derivante dalla necessità di informare in maniera chiara ed evidente chi inseriva i filmati dei contenuti della legge sulla *privacy* e sulla possibile lesione dei diritti dei terzi. E che da tale obbligo, non pienamente adempiuto fa derivare la condanna per il reato di cui all'art. 167 d.lg. n. 196 del 2003.

Il punto è quello già evidenziato in precedenza: si ritiene che, se fosse stato correttamente adempiuto tale obbligo la dodicenne che ha inserito *on line* il raccapricciante filmato si sarebbe determinata a non violare la *privacy* del compagno disabile?

Sembrerebbe di sì. Ma poi lo stesso giudice milanese perviene ad una sentenza di assoluzione per la diffamazione scrivendo che «pur ammettendo per ipotesi che esista un potere giuridico derivante dalla normativa sulla *privacy* che

costituisca l'obbligo giuridico fondante la posizione di garanzia, non vi è chi non veda che tale potere, anche se correttamente utilizzato, certamente non avrebbe potuto 'impedire l'evento diffamatorio. In altre parole anche se l'informativa sulla privacy fosse stata data in modo chiaro e comprensibile all'utente, non può certamente escludersi che l'utente medesimo non avrebbe caricato il file video incriminato, commettendo il reato di diffamazione».

Ebbene, non pare perciò avere torto chi ha rilevato come sia «difficile seguire la coerenza logica prima ancora che giuridica che lega i due passaggi appena richiamati della sentenza» (53)

7. Conclusioni: e se ci fosse una responsabilità di tipo commissivo?

Si è appena detto delle perplessità che suscita l'avere visto, in qualche modo, riconosciuta la sussistenza di una posizione di garanzia dell'*internet service provider* in relazione alla lesione dell'altrui *privacy* e non per quel che concerne la diffamazione.

In realtà, pare condivisibile, l'affermazione operata dal Tribunale di Milano nella sentenza in commento (e prima ancora dallo stesso Tribunale di Milano nel 2004 e da quello di Lucca nel 2007) secondo cui non può ritenersi sussistente alcun obbligo preventivo in capo al *service provider* di controllo circa i contenuti di quanto viene immesso in rete.

Il Tribunale di Milano, in altri termini, alla luce del tipo di imputazione su cui era chiamato a giudicare, con riferimento all'art. 40 comma 2 c.p., non poteva che pervenire, in relazione al contestato concorso nella diffamazione, ad una sentenza di assoluzione. Salvo non fare ricorso, come si diceva all'inizio, alla possibilità di rimessione degli atti al Pm con un'ordinanza *ex* art. 521 comma 3 c.p.p.

E non si tratta - va chiarito - di una scelta di campo di tipo *pro-Internet*, anche se non può sottacersi l'ovvia considerazione che, diversamente opinando, stante la difficoltà tecnica di tale controllo «a monte», verrebbe meno *Internet* stessa. O, in ogni caso, ci troveremmo di fronte ad un *web* diverso da quello che abbiamo conosciuto sino ad oggi, privo di immediatezza nella veicolazione dei suoi contenuti. E perciò destinato probabilmente ad un lento declino.

Condivisibile è anche l'auspicio manifestato nella sentenza in commento - e non solo (54) - a che il legislatore intervenga sulla materia con una buona legge, che fissi dei chiari "paletti" e al contempo dia delle certezze agli operatori. Del resto, negli ultimi anni, come già ricordato, non sono mancate in Parlamento le proposte che hanno animato il dibattito tra gli addetti ai lavori (55).

Un intervento normativo, tuttavia, non potrà evidentemente imporre al *service provider* un controllo preventivo su quanto viene immesso in rete.

Certo, potrà operarsi anche sul versante di una maggiore visibilità degli avvisi ai terzi delle potenzialità lesive dell'altrui *privacy* di quanto vanno ad immettere *on line.* Ma si tratterebbe solo di un dato formale, laddove, come già si evidenziava, è assolutamente condivisibile l'assunto di chi ha rilevato che, in un caso come quello del video di cui alla sentenza in commento, non sarebbe stata

certamente una migliore informazione sulla tutela dell'altrui *privacy* che avrebbe verosimilmente indotto la dodicenne a non rendere pubblico *on line* il video.

Il piano su cui deve auspicabilmente intervenire il legislatore è invece quello della fissazione di un obbligo di tempestiva rimozione dei contenuti, indipendentemente dalla richiesta di chi si senta leso nei propri diritti o delle autorità.

E tale obbligo dovrà essere tanto più stringente e da ottemperare in tempi brevi quanto più evidente si palesi, nei contenuti immessi in rete, una lesione dell'altrui diritto.

Varrà forse la pena di spiegarsi meglio sul punto.

Se viene immesso in rete un video in cui un soggetto critichi, ad esempio, un amministratore pubblico, accusandolo di avere operato secondo interessi propri e non secondo quelli della collettività in relazione ad una determinata scelta politica o amministrativa, può essere accettabile che la non facile valutazione circa la portata diffamatoria di tali affermazioni e/o la sua eventuale scriminabilità sotto il profilo dell'esercizio del diritto di critica politica non possa prescindere da una valutazione che debba essere operata dalle autorità competenti, eventualmente compulsate dal soggetto che si sente leso nella propria reputazione. E perciò non parrebbe accettabile, in termini di libertà di comunicazione e di espressione, imporre o prevedere che sia il *service provider* a dover rimuovere il video.

Cosa diversa, però, è se quello stesso video si palesi *ictu oculi* diffamatorio, ad esempio, dal punto di vista dell'incontinenza verbale del soggetto che opera le accuse. Perchè magari lo stesso si lascia andare ad insulti gratuiti.

È evidente, infatti, che in tal caso, può e deve essere imposto al soggetto che ospiti *on line* il video, di rimuoverlo in tempi brevi.

Ma l'esempio in cui tale obbligo può e deve esserci riguarda proprio un caso come quello esaminato nella sentenza in commento.

Nel caso del video milanese la lesione dei diritti altrui era palese. Si trattava di un video orribile, lesivo dell'altrui dignità, dei diritti del minore coinvolto, della reputazione della *onlus* malamente tirata in ballo dai ragazzi. Per non parlare della morale pubblica, se ancora ce n'è una.

Occorre allora ripartire dall'elaborazione dottrinaria di cui si è detto in relazione all'art. 14 d.lg. n. 70 del 2003.

Ebbene, in tale ottica, pare evidente che in questo caso si può e si deve imporre a chi può farlo un obbligo di tempestiva rimozione di tali contenuti, che prescinda dall'*input* di terzi.

È questo il punto nodale della vicenda in commento.

Ciò che fa maggiormente rabbia non è che dei minori figli di questo tempo degradato abbiano girato e poi messo in rete un video quale quello di cui si è detto. E nemmeno che vi siano state almeno 5.500 persone che l'hanno visto. Ma che il video sia rimasto *on line* due mesi e sia stato rimosso soltanto dopo le denunce e l'intervento della polizia postale.

Ciò doveva e poteva, però, probabilmente, indurre ad una costruzione dell'ipotesi accusatoria di tipo diverso, che prescindesse, com'è avvenuto,

dall'affermazione della sussistenza in capo al *provider* di una posizione di garanzia e di una responsabilità di tipo omissivo.

Il video in questione, infatti, è stato con tutta evidenza «lavorato» dai responsabili di Google. Se è stato inserito tra i video più divertenti e tra quelli più visti, in altri termini, è evidente, che qualcuno ne avrà visionato i contenuti e calcolato il numero degli accessi.

La valenza commerciate di tale attività, su cui pure ci si è soffermati nel corso delle indagini prima e del processo poi, sebbene colori la vicenda, può anche ritenersi di secondo piano.

Di certo c'è stato, però, un *quid pluris* rispetto alla mera tolleranza all'inserimento del contenuto audiovisivo da parte di terzi e alla mancata rimozione.

Ebbene, la responsabilità concorsuale nella diffamazione in capo a chi conosceva i contenuti del video - e l'ha inserito tra i più divertenti - ben potrebbe configurarsi sotto il profilo della causalità agevolatrice.

Va ricordato, infatti, che ai fini della configurabilità della fattispecie del concorso di persone nel reato il contributo concorsuale assume rilevanza non solo quando abbia efficacia causale, ponendosi come condizione dell'evento lesivo - secondo la superata teoria condizionalistica - ma anche quando assuma la forma di un contributo agevolativo, e cioè quando il reato, senza la condotta di agevolazione, sarebbe stato ugualmente commesso, ma con maggiori incertezze di riuscita o di difficoltà. O con un minore effetto lesivo del bene-interesse protetto (56).

La giurisprudenza in materia è ormai pacificamente orientata nel senso di riconoscere il concorso nel reato non solo all'ausilio necessario, ma anche in quello che si limita ad agevolare o facilitare il conseguimento dell'obiettivo finale (57).

Ebbene, non vi è alcun dubbio che con l'immissione del video *on line* e la sua fruibilità da parte degli utenti di Google video la diffamazione nei confronti del minore e dell'associazione Vivi Down si è consumata. Ma di certo l'avere inserito il video nella griglia di quelli più divertenti è un qualcosa che è andato oltre la mera tolleranza di un contenuto immesso da altri. Ed ha certamente facilitato la commissione del reato, aumentando smisuratamente la potenzialità lesiva della reputazione dei soggetti coinvolti.

Del resto, nella sentenza in commento, viene ricordata l'importante pronuncia della Suprema Corte sul contestato sito di *peer to peer www.thepiratebay.org*, dove si è affermato che concorre nel reato di diffusione mediante la rete *Internet* di un'opera dell'ingegno protetta dal diritto d'autore (art. 171-*ter* comma 2, lett. a-*bis*) il titolare del sito *web* che, portando a conoscenza degli utenti le «chiavi di accesso» e le informazioni in ordine alla reperibilità, in tutto o in parte, dell'opera, consente agli stessi lo scambio dei *file* relativi mediante il sistema di comunicazione «*peer to peer*» (58).

Nella pronuncia del Tribunale di Milano in commento si evidenzia come dovrebbe ritenersi corresponsabile del reato (nel caso di specie quello di cui

all'art. 167 codice della *privacy*) quel tipo di *internet service provider che* «non si limiti a fornire un semplice rapporto di interconnessione, ma, gestendo i dati in suo possesso, ne divenga in qualche modo dominus e quindi titolare del trattamento».

Ebbene, il giudice monocratico milanese non confuta tale tipo di impostazione accusatoria, ma afferma che la stessa «da un lato sembra richiedere un livello di approfondimento probatorio forse troppo elevato (quando un ISP può con certezza definirsi un *hoster* attivo? quando può ritenersi esaurita la ricerca di quel *quid pluris* di cui parla la S.C.?) dall'altra esclude dal novero dei potenziali responsabili tutte le numerose platee degli *host provider* che (...) non sembrano poter sfuggire alle ricadute concorsuali delle condotte di reato evidenziate».

Tale affermazione non pare condivisibile.

Dire che la possibilità di un concorso (nel caso commissivo) nel reato da parte dell'*internet service provider* è difficile da provare, non significa non andare a verificare, di volta in volta, se tale prova c'è.

Occorre allora andare a leggere la motivazione della sentenza n. 49437 del 2009 in cui i giudici di legittimità affrontano proprio il problema del se alla condotta delittuosa sia estraneo, o meno, il titolare del sito che mette in comunicazione gli utenti i quali commettono l'illecito con l'attività di *uploading* (59).

E la condivisibile conclusione cui i giudici di Piazza Cavour pervengono è che «se il sito web si limitasse a mettere a disposizione il protocollo di comunicazione (quale quello *peer-to-peer*) per consentire la condivisione di file, contenenti l'opera coperta da diritto d'autore, ed il loro trasferimento tra utenti, il titolare del sito stesso sarebbe in realtà estraneo al reato».

«Però - si legga ancora nella sentenza n. 49437 del 2009 - se il titolare del sito non si limita a ciò, ma a qualcosa di più, ossia indicizza le informazioni che gli vengono dagli utenti, che sono tutti potenziali autori di *uploading*, sicché queste informazioni (i.e. chiavi di accesso agli utenti periferici che posseggono, in tutto o in parte, l'opera), anche se ridotte al minimo, ma pur sempre essenziali perché gli utenti possano orientarsi chiedendo il downloading di quell'opera piuttosto che un'altra, sono in tal modo elaborate e rese disponibili nel sito, ad es. a mezzo di un motore di ricerca o con delle liste indicizzate, il sito cessa di essere un mero "corriere" che organizza il trasporto dei dati. C'è un *quid pluris* in quanto viene resa disponibile all'utenza del sito anche una indicizzazione costantemente aggiornata che consente di percepire il contenuto dei file suscettibili di trasferimento».

Il passaggio conseguente è che «a quel punto l'attività di trasporto dei file (file *transfert*) non è più agnostica; ma si caratterizza come trasporto di dati contenenti materiale coperto da diritto d'autore. Ed allora è vero che lo scambio di file avviene da utente ad utente *peer-to-peer*), ma l'attività del sito web (al quale è riferibile il protocollo di trasferimento e l'indicizzazione di dati essenziali) è quella che consente ciò e pertanto c'è un apporto causale a tale condotta

che ben può essere inquadrato nella partecipazione imputabile a titolo di concorso di persone *ex* art.110 c.p» (60).

È evidente che non è la stessa cosa indicizzare dei file di opere coperte da diritto d'autore al fine di favorirne lo scambio *peer to peer* e classificare un video, come accaduto nel caso che ci occupa, tra i più visti e i più simpatici. E forse la situazione non è comparabile neanche se si tiene conto di eventuali link pubblicitari a contenuti ospitati a pagamento dal *server*.

Tuttavia la sentenza n. 49437 del 2009 apre la strada ad una riflessione giuridica il cui approdo non pare scontato. E rispetto al quale non sfugge, naturalmente, la necessità di valutare poi, caso per caso, la sussistenza del necessario elemento psicologico, soprattutto laddove la fattispecie contestata sia punibile esclusivamente a titolo doloso.

Occorrerà, tuttavia scandagliare e valutare anche la possibile sussistenza di profili di dolo eventuale.

In tal senso la già citata sentenza del Tribunale di Milano del 2004 (61) era parsa un passo più avanti rispetto alla pronuncia in commento, in quanto l'analisi del tribunale in quell'occasione non si era arrestata alle considerazioni relative allo stato della normativa, ma si era estesa a verificare la configurabilità di una la responsabilità concorsuale per il diverso profilo commissivo.

Nella sentenza del 2004 si era anche dato conto della tesi che il *service* e l'*access provider* forniscono un ineludibile contributo causale alla realizzazione del reato altrui. E soprattutto si era affrontato il delicato tema della valutazione della componente psicologica della fattispecie concorsuale.

La sentenza, in particolare, escluso il dolo diretto, analizzava il tema per il profilo del dolo eventuale, escludendone la configurabilità automatica ogniqualvolta non vi fossero specifici elementi che consentissero di ricondurre nella attività del *provider* una specifica attività illecita commessa per il suo tramite.

In assenza di tali elementi - secondo la pronuncia del Tribunale di Milano del 2004 - si finirebbe per equiparare il dolo eventuale a un dolo *in re ipsa*.

La tesi non pare condivisibile, soprattutto alla luce degli ulteriori sviluppi giurisprudenziali e dottrinari in materia di dolo eventuale.

Ma da quell'analisi, forse, più che dalle attuali considerazioni circa la «*prateria di Internet*», occorre ripartire per valutare i possibili profili di responsabilità del *service provider* in casi giudiziari come quello in commento, in attesa che il legislatore intervenga - se lo farà - con una buona legge.

NOTE

(1) Come ricorda Gatti, Con la polarizzazione su libertà e responsabilità Internet ancora alla ricerca di regole condivise, in Guida dir., 2010, f. 25, 8 per i responsabili legali di Google la sentenza è stato «un attacco ai principi fondamentali di libertà sui quali è stato costruito Internet». Viene nel medesimo scritto ricordato anche che: «I manager italiani della multinazionale hanno sostenuto che i tre dirigenti «non hanno avuto nulla a che fare con il video in questione, poiché non lo hanno girato, non lo hanno caricato, non lo hanno visionato». Hanno anche ribadito che se viene meno il principio che la re-

sponsabilità dei contenuti è esclusivamente di chi li carica in rete, cade di fatto la possibilità di offrire servizi su Internet».

(2) Vedasi per tutti www.guidoscorza.it «Google c. Vividown:condannati i ferrovieri!»

(3) Cfr. www.nytimes.com del 26 febbraio 2010 When american and european ideas of privacy collide.

(4) Affermava il 24 febbraio 2010 in un comunicato alla stampa l'ambasciatore Thorne: «Siamo negativamente colpiti dall'odierna decisione di condanna di alcuni dirigenti della Google Inc. per la pubblicazione su Google di un video dai contenuti offensivi. Pur riconoscendo la natura biasimevole del materiale non siamo d'accordo sul fatto che la responsabilità preventiva dei contenuti caricati dagli utenti ricada sugli Internet service provider». Nel suo comunicato, Thorne faceva poi diretto ed esplicito riferimento alla posizione del governo Usa, diventata netta dopo il caso della censura in Cina, che aveva coinvolto proprio Google: «Il principio fondamentale della libertà di Internet è vitale per le democrazie che riconoscono il valore della libertà di espressione e viene tutelato da quanti hanno a cuore tale valore - aggiungeva Thorne -. Il Segretario di Stato Hillary Clinton lo scorso 21 gennaio ha affermato con chiarezza che Internet libero è un diritto umano inalienabile che va tutelato nelle società libere. In tutte le nazioni è necessario prestare grande attenzione agli abusi. Tuttavia, eventuale materiale offensivo non deve diventare una scusa per violare questo diritto fondamentale» (da www.corriere.it).

(5) Cfr. www.espresso.repubblica.it del 2 marzo 2010 e www.wallstreetitalia.com.

(6) Così su www.repubblica.it del 2 marzo 2010 ove si dà conto che lo stesso Posner aggiungeva nell'occasione: «Siamo chiaramente preoccupati per le ramificazioni che questa sentenza potrebbe avere a livello globale». E, dopo aver sottolineato come a suo avviso i dirigenti di Google «quando sono stati informati del contenuto, hanno agito in modo appropriato e malgrado questo sono finiti nel mirino del governo» concludeva con tono vagamente minaccioso: «Si tratta di un caso molto importante sul quale dobbiamo rispondere e vigilare molto da vicino».

(7) Cfr. l'intervista dal titolo Google, l'allarme di Rodotà: Sentenza non diventi censura, in www.repubblica.it del 25 febbraio 2010, in cui Rodotà afferma: «L'Italia aveva assunto un ruolo di punta nel dibattito internazionale affermando che internet non richiede strumenti di tipo penalistico, ma una Costituzione, un "Internet Bill of Rights". Nell'ultimo periodo, il governo ha abbandonato questa linea, manifestando iniziative di tipo censorio. Ora questo clima potrebbe essere rafforzato da una lettura sbrigativa della sentenza e anche da un'eventuale motivazione del tribunale che non tenesse conto della natura della rete. Ogni giorno su YouTube o su Facebook vengono introdotti centinaia di migliaia di contenuti, e questo esclude possibilità di controlli preventivi come quelli previsti su stampa, radio e tv».

(8) Cfr. «Caso Google, la replica della Procura» in www.espresso.repubblica.it del 2 marzo 2010 e Il giudice della sentenza Google ci spiega che, per essere più libero, Internet ha bisogno di regole in www.ilfoglio.it del 16 aprile 2010.

(9) Assai critico in tal senso Scorza, Una sentenza piccola piccola, in www.guidoscorza.it e in www.puntoinformatico.it, che scrive «Condivido il richiamo a Shakespeare con il quale il Giudice ha scelto di concludere la propria "fatica" ma in un senso sensibilmente diverso: la Sentenza minaccia di produrre uno "scontro tra culture" e rimette in discussione principi di diritto sui quali riposano gran parte delle dinamiche della comunicazione online sulla base di poco più che considerazioni di - peraltro dubbio - buon senso e, in ogni caso, più da buon padre di famiglia e/o da dispensatore di precetti morali che da interprete del diritto».

(10) Pezzella, La diffamazione. Reponsabilità penale e civile, Torino, 2009, 95 ss.

(11) Cass., sez. un., 16 ottobre 2001 n. 37140, Galiero, in Cass. pen., 2002, 8, 98; Giust. pen., 2002, 4, 2, 222; Riv. pen., 2001, 12, 98, Ced Cass., n. 219651.

(12) Cass., sez. V, 23 gennaio 2008, n. 3597, Colacito, in Cass. pen., 2008, 12, 4649, Ced Cass., n. 238872.

(13) Per una disamina delle principali questioni vedasi Pezzella, La diffamazione. Responsabilità penale e civile», cit., 399 ss.

(14) Si legge, infatti, nell'imputazione: «Obbligo giuridico ex art. 40 comma 2 così individuato: «omettevano - ciascuno nella rispettiva qualità - il corretto trattamento di dati personali come prescritto dal d.lg. 30 giugno 2003, n. 196 (e altresì più volte sollecitato dall'Autorità Garante per la protezione dei dati personali, dopo la conclusione del procedimento di cui al successivo capo C, in data 22 marzo 2006, 9 maggio 2006 e 3 luglio 2006)ed in particolare: - dall'art 13, difettando del tutto l'informativa sulla privacy - visualizzabile in italiano dalla pagina iniziale del servizio Google video, in sede di attivazione del relativo account al fine di porre in essere l'upload dei files - in ordine a quanto prescritto dal comma 1 della richiamata norma e, per essa, del valido consenso di cui all'art. 23 comma 3; - dall'art. 26, riguardando altresì dati idonei a rivelare lo stato di salute della persona inquadrata; - dall'art. 17, per i rischi specifici insiti nel tipo di trattamento omesso nell'ipotesi di cui al presente procedimento, non attivandosi Google Italy S.r.l. neppure in tal senso- tramite il prescritto interpello- presso l'Autorità Garante. Trattamento omesso - anche in relazione alle concrete misure organizzative da apprestare, idonee alla sua successiva attuazione - fin dalla rase antecedente alla effettiva localizzazione dei servizio Google Video sulla pagina http://video.google.it (di fatto avvenuta in data 12 luglio 2006), non avendo né i due rappresentanti legali di Google Italy s.r.l, né il responsabile del progetto Google Video.(durante le numerose conference-call per la definizione delle modalità operative con il personale di Google Italy S.r.l. assegnato al progetto) né tantomeno il Global Privacy Counsel di Google Inc. affrontato la problematica relativa alla protezione dei dati personali che sarebbero stati trattati in relazione a Google Video, che invece veniva volutamente lanciato come servizio di "libero accesso" dopo una attenta analisi del mercato italiano (confluita nel documento Google Video: preliminary analisis of italian market peculiarities - redatto, su indicazione del DESIKAN, dal personale di Google Italy S.r.l. assegnato al progetto Google Video - nel quale la consolidata presenza di siti internet italiani che offrivano esclusivamente video d qualità veniva indicata come punto di criticità per diventare leader nel mercato dei video on line)».

(15) Più ampiamente sul punto Pezzella, La diffamazione. Responsabilità penale e civile, cit., 437 ss.

(16) Vedasi Pezzella, La diffamazione. Responsabilità penale e civile, cit., 205 ss.

(17) Trib. Aosta 1 giugno 2006, n. 553, in D&G, 2006, 31, 78.

(18) Cass. sez. III, sent. n. 10535 del 10 marzo 2009, ADUC, in www.penale.it.

(19) Cfr. Pezzella, La diffamazione. Responsabilità penale e civile, cit., 431.

(20) De Martini, Telematica e diritti della persona, in D. Inf, 1996, 855 ricorda come i casi esaminati dai giudici di questo Paese (Cubby Ine. v. Compuserve Inc., S.D.N.Y., 1991; Stratton Oakmont Inc. v. Prodigy Servìees Co., S.C. Nassau County, 1995; Stern v. Delphi Internet Serrices Corp., S.C.N.Y. County, 1995) si sono conclusi con l'affermazione della totale assenza di responsabilità per il. contenuto dei messaggi e delle notizie diffuse in capo alle organizzazioni che, anche professionalmente e con spirito commerciale, diffondono « on line services», che sono tutte state equiparate dal punto di

vista della responsabilità al distributore di un mezzo di comunicazione di massa, piuttosto che all'editore

(21) Pezzella, La diffamazione. Responsabilità penale e civile, cit., 402 ss.

(22) Così De Martini, Telematica e diritti della persona, cit., 855 il quale rileva come sia altrettanto difficile individuare con certezza se e chi sia l'editore di un determinato messaggio. Secondo tale Autore: «La responsabilità. dell'editore, così come - nei paesi ove essa esiste - la responsabilità del direttore del mezzo di comunicazione di massa, si fonda sulla possibilità di un controllo editoriale sul contenuto del messaggio diffuso. Sia pure attraverso percorsi logici diversi, che sono in gran parte motivati dalle differenze di disciplina positiva delle varie legislazioni, i vari sistemi giuridici individuano una responsabilità dell'editore fondamentalmente in una sorta di «culpa in vigilando», consistente nell'aver omesso il controllo dovuto sul contenuto e sulla legittimità di pubblicazione di una notizia lesiva della personalità di qualcuno. Nella realtà di Internet, sia che si tratti della trasmissione di notizie on line, sia che si tratti di consentire l'accesso a informazioni e notizie conservate e memorizzate su uno specifico computer, ovvero in una banca dati, anche le imprese che forniscono «on line services» (che sono quelle che sembrano più assomigliare ad un vero e proprio editore) non possono che sfuggire ad una simile identificazione, in virtù della circostanza fondamentale che nessuna di tali imprese è in condizione di esercitare, né di fatto esercita alcun controllo sul contenuto dei messaggi diffusi, e sul contenuto delle notizie memorizzate in banche dati. o in appositi "depositi"».

(23) Natoli, La tutela dell'onore e della reputazione in Internet: il caso della diffamazione anonima, in Europa e diritto privato, 441.

(24) Natoli, cit. ricorda come in realtà «anche se la finalità precipua del CDA era di promuovere la decenza in rete e, quindi, essenzialmente di limitare la circolazione di materiale pornografico, può certamente affermarsi, con riguardo ai profili che qui interessano, cioè quelli della diffamazione on line, che il CDA sia diventato, a livello giurisprudenziale, un punto di non ritorno». Ed infatti -secondo lo stesso Autore: «appare significativa la circostanza che dopo l'approvazione del CDA da parte del Congresso non si siano più registrate decisioni conclusesi con una condanna degli internet providers in casi che affrontassero questioni di diffamazione. Un simile esito, d'altronde, era del tutto prevedibile se si tiene presente che, come la gran parte dei commentatori americani non ha mancato di notare, il CDA ha rappresentato, senza troppi fronzoli, una graziosa concessione fatta dal Congresso alla potente lobby dei provider americani».

(25) Seminara, La responsabilità penale degli operatori in Internet, in D.Inf, 1998, 751 ove si sottolinea che «appare comunque chiaro che la ridotta capacità operativa dei due criteri ora esaminati potrebbe indurre verso la costruzione di una responsabilità colposa del provider conseguente alla violazione di un obbligo giuridico di impedire eventi illeciti, similmente a quanto già dispone l'art. 57 c.p. per il direttore o vicedirettore responsabile in tema di stampa periodica rispetto ai reati commessi con il mezzo della pubblicazione». Secondo tale Autore, però, se è vero che già all'epoca taluni interventi giurisprudenziali apparivano voler estendere ai giornali c.d. telematici la disciplina amministrativa della stampa o affermare una equiparazione tra gli organi di stampa e i siti Internet, tuttavia «il tentativo di estendere analogicamente la normativa penale vigente in tema di stampa è destinato inesorabilmente a infrangersi sul principio di legalità, giacché l'art. 1 l. 8 febbraio 1948, n. 47 tassativamente stabilisce che "sono considerate stampe o stampati, ai fini di questa legge, tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici, in qualsiasi modo destinate alla pubblicazione"».

(26) Corrias Lucente, Ma i network providers, i service providers e gli access providers rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che gestiscono?, in questa Rivista, 2004, 2526.

(27) Russo, Internet, libertà di espressione e regole penali: spunti di riflessione a margine di una pronuncia in tema di diffamazione», in Foro it., 2000, 2, 664.

(28) Trib. Milano 18 marzo 2004, in questa Rivista, 2004, 1713.

(29) Trib. Milano 18 marzo 2004, in questa Rivista 2004, 1714 ove si legge anche che «non appare invece soddisfacente un'impostazione della responsabilità del server con riferimento alla categoria del dolo eventuale ogni qualvolta non vi siano specifici elementi che consentano di ricondurre nella sua sfera di conoscibilità una specifica attività illecita commessa per suo tramite e ciò, come si è già detto, per la struttura aperta di Internet (che rende in astratto possibile immissioni costanti, autonome e non controllabili sugli spazi gestiti dal server laddove lo stesso anche per il tipo di servizio gestito non abbia potuto applicare alcuna tutela rispetto a dette immissioni). In assenza di detti elementi si finirebbe per equiparare il dolo eventuale a un dolo in re ipsa».

(30) Resta, La responsabilità penale del provider: tra lasseiz faire ed obblighi di controllo, in questa Rivista, 2004, 1719 secondo cui «con riferimento alla questione dell'eventuale sussistenza di una posizione di garanzia in capo all'operatore della realtà virtuale osserva giustamente il tribunale di Milano come, de lege lata, essa non possa essere fondata su alcuna specifica norma giuridica, né tanto meno, stante il divieto di analogia in malam partem delle norme (lato sensu) incriminatrici, sulla base di un'applicazione analogica della disciplina dettata, dagli art. 57 e 57-bis c.p., in materia di responsabilità penale dell'editore, del direttore, del vice-direttore e dello stampatore (nel caso di stampa non periodica ed in presenza di pubblicazioni illecite i cui autori siano ignoti o non imputabili), per i reati commessi con il mezzo della stampa». «Ogni operazione ermeneutica in ipotesi volta ad applicare alla fattispecie in esame la disciplina relativa agli illeciti commessi con il mezzo della stampa - osservava lo stesso Autore - si risolverebbe infatti nella violazione del suddetto divieto di analogia delle norme incriminatrici, sconfinando ben oltre la massima estensibilità esegetica del dettato normativo di cui all'art. 1 l. 8 febbraio 1948, n. 47, che dispone espressamente doversi considerare "stampe o stampati, ai fini di questa legge, tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici, in qualsiasi modo destinate alla pubblicazione"».

(31) Corrias Lucente, Ma i network providers, i service providers e gli access providers rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che gestiscono?, in questa Rivista, 2004, 2526.

(32) Corrias Lucente, Ma i network providers, i service providers e gli access providers rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che gestiscono?, in questa Rivista, 2004, 2524.

(33) Trib. civ. Lucca 20 agosto 2007, in www.dirittodellinformatica.it; www.intertraders.eu.

(34) Trib. civ. Lucca 20 agosto 2007, in www.dirittodellinformatica.it; www.intertraders.eu.

(35) Il Considerando 14 di tale direttiva prevede che l'applicazione della stessa debba «essere pienamente conforme ai principi relativi alla protezione dei dati personali, in particolare per quanto riguarda le comunicazioni commerciali non richieste e il regime di responsabilità per gli intermediari».

(36) Scorza, Oltre Google c'è di più. L'equilibrio tra diritto alla privacy e il principio di non responsabilità degli intermediari, la libertà di espressione. Riflessioni sulle

spiegazioni della Procura in attesa delle motivazioni della sentenza Vividown, in www.guidoscorza.it.

(37) Scorza, Oltre Google c'è di più. L'equilibrio tra diritto alla privacy e il principio di non responsabilità degli intermediari, la libertà di espressione. Riflessioni sulle spiegazioni della Procura in attesa delle motivazioni della sentenza Vividown, cit.

(38) Scorza, Una sentenza piccola piccola, in www.guidoscorza.it e in www.puntoinformatico.it, cit.

(39) Corrias Lucente, Ma i network providers, i service providers e gli access providers rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che gestiscono?, cit., 2528.

(40) Minotti, Responsabilità penale: il provider è tenuto ad attivarsi?, in www.interlex.it, 5 maggio 2003.

(41) Corrias Lucente, Ma i network providers, i service providers e gli access providers rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che gestiscono?, cit., 2528.

(42) Corrias Lucente, Ma i network providers, i service providers e gli access providers rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che gestiscono?, cit., 2529, il quale sottolinea come la fattispecie concorsuale può tuttavia «risultare integrata dall'inottemperanza all'ordine di rimozione o disabilitazione dell'informazione costituente reato, sussistendo, nel caso del mantenimento in rete, le componenti oggettiva e soggettiva del concorso».

(43) Così ancora Corrias Lucente, Ma i network providers, i service providers e gli access providers rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che gestiscono?, cit., 2529.

(44) Corrias Lucente, Ma i network providers, i service providers e gli access providers rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che gestiscono?, cit., 2529.

(45) Cammarata, Sotto torchio gli operatori della rete, in www.interlex.it, 10 aprile 2003 il quale sottolinea la novità e la legittimità della disposizione, non senza evidenziare, però, come «naturalmente si dovrà in qualche modo provare che, in un dato momento, il prestatore era "a conoscenza di presunte attività o informazioni illecite" (qui si dovrebbe riaprire un discorso già fatto: per il nostro ordinamento, non esiste l'informazione "illecita"; illecito può essere solo un comportamento)». Resta comunque il problema di capire -secondo l'acuta osservazione di tale Autore- su quali basi il provider possa valutare la presunta illiceità di un comportamento.

(46) Minotti, Responsabilità penale: il provider è tenuto ad attivarsi?, cit.

(47) Cammarata, Sotto torchio gli operatori della rete, in www.interlex.it, cit.

(48) ALCEI 19 giugno 2002, in www.interlex.it.

(49) Cammarata, Sotto torchio gli operatori della rete, in www.interlex.it, cit.

(50) L'art. 167 d.lg n. 196 del 2003 prevede che: «1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli artt. 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'art. 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi. 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli artt. 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni».

(51) Scorza, Una sentenza piccola piccola, cit.

(52) Così Berlingieri, Sentenza Google, la condanna è incoerente, in www.apogeonline.com la quale rileva che «nella sentenza si legge, infatti che «tale comportamento, improntato ad esigenze di minimalismo contrattuale e di scarsa volontà comunicativa, costituisce una specie di «precostituzione di alibi» da parte del soggetto». A tale Autrice si deve peraltro il condivisibile spunto di riflessione su «quale valore giuridico debba darsi in concreto alle condizioni o termini di servizio che siamo abituati ad accettare ogni volta che sottoscriviamo un servizio web, ma che molto di rado vengono effettivamente letti e compresi», problema che «in sentenza è appena accennato e certamente avrebbe meritato un ulteriore approfondimento non solo per la sua centralità - vista la rilevanza che ha assunto in motivazione - nel caso di specie, ma anche per l'intrinseco valore di una riflessione sul dibattito in relazione al rapporto reale che esiste tra consenso prestato tramite il clic sul pulsante «Accetto» e consapevolezza del contenuto e del significato delle clausole che sono accettate con quel clic».

(53) Così Scorza, op. cit., che afferma. «mi sfugge probabilmente qualcosa ma, l'impressione, è che a pag. 96 il Giudice abbia ritenuto che se Google avesse dato correttamente l'informativa la ragazzina non avrebbe caricato il video incriminato mentre a pag. 104 si mostri convinto del contrario ovvero che lo avrebbe comunque caricato».

(54) In tal senso Melzi D'eril - Vigevani, Nelle motivazioni di condanna della sentenza violazione della privacy per mancato consenso, in Guida dir., 2010, 25, 23 secondo cui: «Il caso esaminato palesa anche l'opportunità di un intervento del legislatore che rafforzi gli obblighi di controllo sull'identificazione di chi scrive o immette filmati in rete; disegni con maggiore chiarezza l'obbligo di notice and takedown, specificando quali segnalazioni siano sufficienti a porre in capo al provider l'obbligo di rimozione dei contenuti illeciti; adatti la normativa sul commercio elettronico alle nuove forme di comunicazione sorte nell'ultimo decennio, ragionando sulla qualificazione giuridica di soggetti quali i motori di ricerca o i social network. Il tutto nel rispetto del principio cardine della normativa italiana e comunitaria sul commercio elettronico, ovvero l'insussistenza di un obbligo generale di sorveglianza e nella consapevolezza che il diritto di parola si esercita liberamente intingendo il pennino nell'inchiostro, ma anche caricando un filmato sulla piattaforma di una multinazionale della comunicazione».

(55) Cfr. sul punto Pezzella, La diffamazione. Responsabilità penale e civile, cit., 237.

(56) Cfr. Cass., sez. IV, sent. n. 24895 del 22 maggio-26 giugno 2007, Di Chiara, in Ced Cass., n. 236853; conf. Cass., sez. I, sent. n. 5631 del 17 gennaio-5 febbraio 2008, in Ced Cass., n. 238648.

(57) Cfr. Cass., sez. IV, sent. n. 6664 del 28 gennaio 1993-7 luglio 1993, Mangani, in Ced Cass, n. 195476.

(58) Cass., sez. III, sent. n. 49437 del 29 settembre-23 dicembre 2009 P.M. in proc. Sunde Kolmisoppi e altri, in Ced Cass., n. 245935.

(59) Nella sentenza n. 49437 del 2009 i giudici di legittimità precisano anche che «la circostanza che la condotta di partecipazione sia stata posta in essere all'estero fa venir meno la giurisdizione del giudice nazionale laddove una parte della condotta comune abbia avuto luogo in Italia (cfr. Cass., sez. V, 9 luglio 2008 - 20 ottobre 2008, n. 39205, secondo cui, in caso di concorso di persone nel reato, ai fini della sussistenza della giurisdizione penale del giudice italiano e per la punibilità di tutti i concorrenti, è sufficiente che nel territorio dello Stato sia stata posta in essere una qualsiasi attività di partecipazione da parte di uno qualsiasi dei concorrenti; cfr. anche Cass., sez. V, 17 novembre 2000 - 27 dicembre 2000, n. 4741, che ha affermato che il giudice italiano è competente

a conoscere della diffamazione compiuta mediante l'inserimento nella rete telematica Internet di frasi offensive e/o immagini denigratorie, anche nel caso in cui il sito web sia stato registrato all'estero, purché l'offesa sia stata percepita da fruitori che si trovino in Italia».

(60) Cass., sez. III, sent. n. 49437 del 29 settembre-23 dicembre 2009 P.M. in proc. Sunde Kolmisoppi e altri, in Ced Cass., n. 245935 che sul punto richiama: Cass., sez. II, 17 giugno 1992 - 16 luglio 1992, n. 8017, secondo cui l'attività di chi concorre nel reato ex art. 110 c.p. può essere rappresentata da qualsiasi forma di compartecipazione o contributo di ordine materiale o psicologico a tutte o ad alcune delle fasi di ideazione, organizzazione ed esecuzione della condotta illecita; Cass., sez. I, 14 febbraio 2006 - 2 maggio 2006, n. 15023, secondo cui la partecipazione al reato può consistere anche in un apporto che soltanto agevoli la condotta illecita; Cass., sez. IV, 22 maggio 2007- 26 giugno 2007, n. 24895, secondo cui anche il mero «contributo agevolatore», che, se di «minima importanza», dà luogo all'attenuante di cui all'art. 114 c.p., comunque consente l'imputazione a titolo di concorso nel reato; infine anche Cass., sez. VI, 28 giugno 2007 - 30 luglio 2007, n. 30968, sulla responsabilità a titolo di concorso del direttore responsabile di un sito web ove era stata effettuata la pubblicazione di un atto amministrativo a carattere riservato

(61) Trib. Milano 18 marzo 2004, in questa Rivista 2004, 1714.

Il caso google - vivi down quale emblema del difficile rapporto degli internet providers con il codice della privacy

di Rocco Lotierzo (*)

1. La questione decisa

Il caso su cui è intervenuto il Tribunale di Milano è noto e raccapricciante: alunni di una scuola in un empito di "creatività cinematografica" avevano filmato - senza chiedergli alcun tipo di permesso - un compagno disabile mentre lo sottoponevano a varie angherie e soprusi di loro gusto.

Il filmato poi era stato immesso sul sito di *Google Video*, allora concorrente di *Youtube*.

Giudicata separatamente la posizione dei ragazzi minorenni, il processo di Milano riguardava esclusivamente quattro soggetti apicali, investiti di diversi ruoli nell'ambito di società della galassia *Google Inc.*, i quali dovevano rispondere, in concorso tra loro, del delitto di diffamazione mediante omissione ai danni del giovane e della associazione Vividown, nonché di trattamento illecito dei dati personali relativi al solo ragazzo videoripreso.

Per la prima imputazione è intervenuta sentenza assolutoria. Invece, per il delitto di trattamento illecito dei dati personali, il giudice di merito è pervenuto alla condanna con motivazioni, che, condivisibili o meno, costituiscono senz'altro la pietra miliare per discutere d'ora innanzi di responsabilità dell'ISP (*internet service provider*) per fatti che ledono la *privacy* degli individui.

Perciò, le considerazioni che verranno esposte saranno relative soltanto al capo della sentenza che riguarda il delitto p. e p. dall'art. 167 cod. *privacy*, mentre è preferibile lasciare ad altri e più autorevoli interventi la trattazione anche della parte che concerne l'assoluzione per il delitto di diffamazione (1).

2. Le ragioni della decisione

Ha ritenuto il tribunale che, al di là della dibattuta qualificazione del *PROVIDER GOOGLE ITALY* (se *CONTENT* oppure *HOST PROVIDER*, come rispettivamente sostenuto da accusa e difesa), esso attuasse senza ombra di dubbio una attività di trattamento di dati personali in una qualsiasi delle numerosissime forme indicate dall'art. 4, comma 1, lett. *A)*, cod. *PRIVACY*. Pertanto, indiscutibile doveva ritenersi il suo assoggettamento alle disposizioni di cui all'intero d.lg. n. 196/2003.

L'indagine del tribunale era rivolta a stabilire, in primo luogo, se su *Google* gravasse l'obbligo di reperire direttamente presso l'interessato il consenso al trattamento; in secondo luogo, se sempre su *Google* incombesse un obbligo di verifica preventiva di tutti i contenuti inseriti in Rete attraverso il servizio concretamente offerto (pubblicazione di video).

Il giudice di merito ha dissentito rispetto ad entrambe le ipotizzate soluzioni, considerando inesigibili le condotte adempienti. Tuttavia, ha evidenziato come

---

(*) in *Cassazione Penale*, 2010, 3994.

fosse innegabile che sul *Provider* incombesse un distinto obbligo ovvero quello di corretta e puntuale informazione ai terzi che consegnavano il video (e, quindi, i dati) con specifico riferimento alle norme "che concernono la necessità di procurarsi l'obbligatorio consenso in ordine alla diffusione di dati personali sensibili".

Perciò, in sentenza può leggersi che, chiaramente, non può sussistere responsabilità *ex* art. 167 cod. *privacy* allorché "il *Provider* utilizzi e diffonda dati che egli in buona fede debba o possa considerare come lecitamente raccolti da altri", ciò in quanto non può esigersi, in capo a chi fornisca un semplice servizio di interconnessione, un pervasivo controllo rispetto ad ognuno dei dati inseriti nel sistema. Tuttavia, non può andare esente da responsabilità colui il quale effettui il trattamento di dati senza il prescritto consenso qualora venga provata la piena consapevolezza della sua mancanza, in quanto derivata da precisi indici rivelatori, uno dei quali è senz'altro l'inadempimento rispetto all'obbligo di informazione sopra tratteggiato.

3. Il delitto di trattamento illecito dei dati personali

Prima di svolgere alcun tipo di riflessione in ordine alle motivazioni per cui il Tribunale di Milano è giunto alla condanna, pare opportuno indicare le coordinate normative all'interno delle quali esso si è trovato ad operare.

Queste sono fornite, essenzialmente, dall'art. 167 cod. *privacy*, il quale testualmente prevede che: "1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni".

Non è chi non veda come la norma incriminatrice in commento definisca la fattispecie astratta attraverso il richiamo ad altre norme di "disciplina" (2) contenute nello stesso codice. Per altro verso, essa non appare catalogabile tra le norme penali cc.dd. in bianco, atteso che il contenuto del precetto penale non si esaurisce nella richiamata norma disciplinare, venendo, invece, integrato dal disposto dell'art. 167 cod. *privacy* stesso, che, oltre al coefficiente psicologico del dolo specifico, prevede una particolare condizione obiettiva di punibilità (il nocumento) (3).

Tale tecnica di redazione della fattispecie penale suscita, peraltro, non poche perplessità (4), atteso che il rinvio a norme esterne a quella penale dispiega un campo applicativo assai esteso e, soprattutto, di difficilissima delimitazione.

Il punto è chiaro sol che si veda quali e quanti siano i comportamenti prescritti dalle disposizioni richiamate.

Si pensi, ad esempio, al contenuto dell'art. 130 cod. *privacy*, che regolamenta l'invio di comunicazioni indesiderate.

Il fulcro della disposizione è senz'altro rappresentato dal comma 1, che fa esplicito divieto di invio delle comunicazioni in parola senza il consenso dell'interessato.

Tuttavia, ulteriore prescrizione dello stesso art. 130 cod. *privacy* è quella del comma 5, che vieta l'invio del c.d. *spamming* camuffando l'identità del mittente.

E, ancora, vi è il comma 4, che, nell'ambito di una relazione commerciale "aperta", legittima l'invio di comunicazioni non sollecitate, relative a prodotti e servizi analoghi ad uno già acquistato dall'interessato, sempre che l'invio venga accompagnato dalla comunicazione in ordine "alla possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente".

Ora, considerato che l'art. 167 cod. *privacy* opera un rinvio integrale allo stesso art. 130, pare che una qualsiasi di tali violazioni conduca alla consumazione del reato, fatta salva la venuta ad esistenza del dolo specifico di fattispecie - che difficilmente mancherà in ipotesi di comunicazioni a scopo commerciale - e del nocumento.

Certamente, la previsione della condizione obiettiva di punibilità può ben servire a modulare l'erogazione della sanzione penale, dal momento che la suprema Corte ha affermato che dall'ambito della nozione di nocumento "devono essere senza dubbio escluse le semplici violazioni formali ed irregolarità procedimentali, ma anche quelle inosservanze che producano un *vulnus* minimo all'identità personale del soggetto ed alla sua *privacy* come su definite sia nell'aspetto negativo sia positivo e non determinino alcun danno patrimoniale apprezzabile" (5).

Eppure, nonostante una concezione sostanzialistica della condizione obiettiva di punibilità, è immaginabile che in un gran numero di casi il trattamento dovrebbe considerarsi illecito anche essendovi alla base una violazione di minimo rilievo quale quella sanzionata dal comma 4 dell'art. 130 cod. *privacy*.

La situazione che ne deriva, oltre a suggerire qualche riflessione di politica criminale di cui si fa grazia, pone un serio interrogativo relativo alla tenuta dell'art. 167 cod. *privacy* rispetto ai principi di tassatività e determinatezza delle fattispecie incriminatrici (6), tanto più che il discorso proposto in merito all'art. 130 va proiettato sulle ben quindici norme disciplinari cui la fattispecie penale fa espresso rinvio.

Ciò premesso, ai limitati fini dell'analisi della pronuncia in commento, l'attenzione va appuntata esclusivamente sugli artt. 23 e 26 del codice, atteso che il tribunale, per ritenere consumato il reato di trattamento illecito di dati personali, ha fatto riferimento esclusivamente alla violazione delle norme in questione.

Dall'art. 23, applicabile ai soli trattamenti effettuati da soggetti privati od enti pubblici economici, possono enuclearsi i seguenti precetti:

1. il trattamento di dati personali altrui è vietato senza il consenso dell'interessato;

2. il consenso ha da essere valido ovvero esso va espresso liberamente, in relazione a uno specifico trattamento, documentato per iscritto e, infine, preceduto dall'informativa resa all'interessato nei termini di cui all'art. 13 del codice;

3. il consenso va manifestato in forma scritta quando il trattamento concerne dati sensibili.

L'art. 26, coerentemente, limitando la sua sfera applicativa ai dati sensibili (7), prevede che:

1. i trattamenti che riguardano tali dati possano avvenire lecitamente, salve le eccezioni di cui ai commi 3 e 4, soltanto col consenso scritto dell'interessato e previa autorizzazione del Garante;

2. i dati idonei a rivelare lo stato di salute non possano essere diffusi.

Al lume di siffatti riferimenti normativi pare, in primo luogo, che erroneamente il giudice estensore non abbia approfondito il giudizio attorno alla tipologia dei dati divulgati (le immagini videoriprese del ragazzo), restando indifferente rispetto alle sollecitazioni di accusa e difesa, volte a far stabilire se si trattasse di dati relativi allo stato di salute o meno (8). Appare, infatti, di tutta evidenza che, qualora si fosse optato per la soluzione positiva, ogni successiva valutazione in ordine alle caratteristiche del consenso prestato dai ragazzi che avevano fornito il video sarebbe risultata superflua, dal momento che per i dati idonei a rivelare lo stato di salute vige un divieto assoluto di loro diffusione anche in presenza del consenso dell'interessato (art. 26, comma 5, cod. *privacy*).

In secondo luogo, la lettura delle stesse norme lascia ben comprendere come, non avendo il tribunale operato quella valutazione, assolutamente dirimente, la traccia di tutto il discorso motivazionale dovesse giocoforza consistere nella analisi del consenso effettivamente prestato al *provider* che aveva consentito la diffusione del video.

4. Il trattamento di dati raccolti presso terzi e gli obblighi di un internet service provider

Un punto su cui la sentenza in commento vuole apparire molto netta è il seguente: non esiste un obbligo preventivo di controllo da parte del *PROVIDER* riferito ai dati immessi dagli utenti.

Invece, ciò che, secondo il tribunale, non può negarsi è che lo stesso soggetto sia tenuto a precisamente informare gli utenti sugli obblighi derivanti dalla legislazione in materia di protezione dei dati personali.

Orbene, pare che proprio questo nella fattispecie sia il terreno d'incontro con la problematica del consenso, visto che ad esser contestata ai responsabili del *Provider* era la mancanza di una idonea informativa a coloro che avevano inviato il video circa l'obbligo di premunirsi del consenso dell'interessato.

Merita, a questo punto, un breve cenno la regolamentazione normativa del trattamento di dati raccolti presso soggetti diversi dall'interessato. Questo deve esser preceduto, in primo luogo, da un'informativa resa ai terzi che comunicano il dato; poi, da un'informativa resa all'interessato all'atto della registrazione dei dati o della loro comunicazione (art. 13, commi 1 e 4, cod. *privacy*). Di tutta evidenza, allora, che anche tali trattamenti debbano tendenzialmente ottenere il consenso dell'interessato al dato, salve ovviamente le ipotesi di cui all'art. 13, comma 5, cod. *privacy*, che prevede, tra l'altro, un esonero dall'obbligo di informativa all'interessato quando essa "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" (art. 13, comma 5, lett. *c)*, cod. *privacy*).

Dalla rapidissima disamina della disciplina del caso concreto si può evincere che il principio del consenso rappresenta un caposaldo dei trattamenti che avvengono in ambito privato. Tuttavia, esso non può avere applicazioni parossistiche, dovendo recedere a fronte di situazioni in cui l'obbligo non è esigibile.

Il punto è di non poco interesse nella fattispecie che ci occupa, atteso che, in definitiva, ad essere in discussione era un comportamento omissivo rispetto all'obbligo sancito dall'art. 13 cod. *privacy*, intimamente connesso con quello di ottenere il consenso dell'interessato (9).

Quel che rappresenta il *novum* della sentenza in commento è, però, il fatto che il tribunale non abbia rimproverato la mancanza di una informativa all'interessato, bensì la mancata prospettazione a coloro che inviavano il video dei rischi giuridici collegati alla condotta che ponevano in essere.

Orbene, la ricostruzione del reato in questi termini, pur se ricca di spunti di interesse, non pare condivisibile.

Invero, se appare corretto senz'altro il ragionamento in punto di inesigibilità della richiesta di consenso diretta all'interessato, a non convincere è la pretesa di un adempimento non richiesto da alcuna disposizione del codice della *privacy*, atteso che l'art. 13, comma 1, nel disciplinare il contenuto dell'informativa riguardante il trattamento, non fa alcun cenno ad avvisi circa l'obbligo di rispettare il codice stesso (10). E si comprende bene la scelta del legislatore, dal momento che il titolare del trattamento certamente non può farsi divulgatore di precetti legislativi, vigendo il principio, in ambito penalistico anche testualmente affermato dall'art. 5 c.p., di presunzione di conoscenza della legge. Peraltro, si rifletta a come la soluzione prospettata dal giudice di Milano, oltre a non trovare conferma nel dettato del codice, costituirebbe probabilmente uno strumento inidoneo allo scopo professato tra le righe (impedire divulgazioni di dati senza il consenso dell'interessato).

Urge, allora, un ritorno al punto di partenza ovvero ai rapporti intercorrenti tra gli artt. 167 e 23 del codice.

Ancora una volta, dalla lettura delle norme si distillano elementi indispensabili alla soluzione del caso concreto. Non è in discussione, infatti, che ad esser richiamato dall'art. 167 sia esclusivamente l'art. 23 del codice e non anche l'art.

13, disciplinante, come detto, l'informativa. E, allora, pare possibile concludere che la omissione (o la inadeguatezza) della informativa a terzi, diversi dall'interessato, non possa costituire di per sé reato, atteso che lo stesso art. 23 cod. *privacy*, ai fini della raccolta di un valido consenso, obbliga testualmente all'inoltro della informativa nei confronti del solo interessato, per nulla menzionando altre tipologie di soggetti.

Pertanto, potrebbe invocarsi addirittura la violazione del principio di tassatività laddove si giungesse ad affermare la sussistenza di un reato punibile *ex* art. 167 cod. *privacy* sol perché non si sono adeguatamente informati coloro presso i quali i dati sono stati raccolti.

Ciò premesso al fine di sgombrare il campo da potenziali equivoci, va sottolineato che nella sentenza in commento si propone un discorso diverso e senz'altro di maggior pregio giuridico, affermandosi, in sintesi, che la responsabilità penale del *Provider* deriva dalla consapevolezza della mancanza del consenso, desunta dal fatto che la informativa ai terzi che comunicavano il dato era inadeguata, in quanto manchevole delle avvertenze suindicate. In altre parole, seppur testualmente nella decisione si parli di "piena consapevolezza", pare che alla fattispecie contestata sia stato applicato il coefficiente psicologico del dolo eventuale (l'indifferenza e, quindi, l'accettazione del rischio che un consenso dell'interessato non vi sia).

Sulla specifica argomentazione: non sembra condivisibile che un indice, assunto quale rivelatore del dolo, possa esser derivato dalla violazione di un precetto non esistente sul piano normativo; e, tanto meno, che costituisca un fatto scontato che persone per cui vige la presunzione di conoscenza della legge decidano di violarla (11). Del resto, si noti come in sentenza venga, nel caso concernente la diffamazione, affermato che "anche se l'informativa sulla *privacy* fosse stata data in modo chiaro e comprensibile all'utente, non può certamente escludersi che l'utente medesimo non avrebbe caricato il *file* video incriminato ...". Dunque - *a contrario* -, anche ponendosi nell'ottica del tribunale, come poter escludere che l'indifferenza rispetto alla illiceità del trattamento operato dai ragazzi (per mancanza del consenso), vi sarebbe stata anche in caso di formalistico ossequio ai dettami della sentenza stessa (l'invio di una informativa "blindata")?

Ma il *punctum dolens* non è neppure precisamente questo: è piuttosto che, parlando di consapevolezza della natura illecita del precedente trattamento di dati, non appare più corretto concepire il reato in forma "monosoggettiva" (12) e cioè disgiunta dalla condotta dei ragazzi che avevano caricato il video.

Si rifletta a come sia lo stesso tribunale a considerare inesigibile per il *Provider* l'adempimento dell'obbligo di richiedere il consenso all'interessato, nonché quello di preventivo controllo dei contenuti immessi dagli utenti.

Ora. Ben si comprende che la consapevolezza da parte del *Provider* circa la mancanza del consenso dell'interessato non potrebbe non essere valorizzata. Tuttavia, ferme restando le riserve sulla effettiva correttezza della operazione che quella consapevolezza fa discendere dalla insufficienza della informativa a

terzi, merita considerazione anche un diverso dato: è un fatto che ad essere in discussione non sia la mancanza di un consenso che avrebbe dovuto richiedere il *Provider* - ipotesi esclusa dal tribunale -, bensì quella di un consenso che avrebbe dovuto esser raccolto dagli utenti.

Vien da chiedersi, allora, se la omissione di una condotta dichiaratamente inesigibile e rientrante nel dominio di altri (la richiesta del consenso all'interessato), prima di qualsiasi valutazione in ordine all'elemento psicologico di fattispecie, potesse essere ricondotta alla consumazione "monosoggettiva" del reato di cui all'art. 167 cod. *privacy*. In altre parole, preso atto di come la condotta penalmente rilevante implichi una violazione disciplinare nei termini descritti dall'art. 23 cod. *privacy*, *quid juris* allorquando la violazione sia imputabile a soggetti diversi da quello a cui si tratta di applicare la norma penale?

Pare di poter rispondere che l'altruità della condotta escluda l'accesso all'applicazione della norma penale e, quindi, qualsiasi discorso in ordine alla sussistenza del dolo, peraltro qui evocato nella forma del dolo eventuale: si tratta del rispetto del principio di tassatività oltre che di quello di colpevolezza.

La ricostruzione del delitto di cui all'art. 167 proposta dal tribunale sarebbe stata teoricamente più compatibile con l'elevazione di una contestazione nella forma del concorso mediante omissione nel reato commissivo altrui, ipotesi non formulata dalla pubblica accusa, che in maniera molto lineare reclamava che non vi era stata da parte del *Provider* alcuna richiesta del consenso.

A giustificare una contestazione riguardante l'omesso impedimento del reato altrui, poteva esservi il fatto che la condotta del *Provider*, attraverso il dispiegamento di mezzi tecnici, aveva realizzato la più larga diffusione di dati già illecitamente trattati dai minori, che, pur potendo richiedere il consenso al ragazzo ritratto, avevano omesso di farlo (13).

A questo punto, non può sottacersi che il delitto di cui all'art. 167 cod. *privacy* è privo di evento naturalistico, di modo che secondo taluni mal si adatta a una contestazione formulata come sopra (14).

Qualora, però, si riuscisse a superare l'impasse dogmatico, chiaramente preclusivo di ogni ulteriore analisi, andrebbe ancora appurato se nel caso di interesse sussisteva una posizione di garanzia del *Provider*, "definibile come uno speciale vincolo di tutela tra un soggetto garante ed un bene giuridico, determinato dalla incapacità - totale o parziale - del titolare a proteggerlo autonomamente" (15).

Ebbene, in argomento, si osserva come certamente non si ravvisi alcuna posizione di garanzia all'interno delle disposizioni dell'art. 13 cod. *privacy*, atteso che, come già segnalato, esse non prevedono in capo al titolare del trattamento alcun obbligo di invitare i terzi al rispetto della legge. Del resto, quel che può assumere rilevanza non è tanto la prescrizione di un determinato comportamento, quanto la sussistenza di un obbligo giuridico di impedire l'evento (16), che, a sua volta, non può esser disgiunto da un potere di controllo (17). All'opposto, nella fattispecie, dalla posizione del *Provider*, non poteva esercitarsi alcun dominio rispetto alle condotte degli utenti.

Per non dissimili motivazioni, deve escludersi che la posizione di garanzia possa trovare la propria fonte in altre disposizioni; tanto meno, nel d.lg. 9 aprile 2003, n. 70, dal momento che l'art. 17, comma 1, dello stesso provvedimento sancisce che "nella prestazione dei servizi di cui agli artt. 14, 15 e 16, 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". Vero è che gli artt. 14, 15 e 16 d.lg. n. 70/2003 introducono obblighi progressivamente più onerosi in considerazione della tipologia del *Provider*. Vero è anche che le stesse disposizioni hanno sancito che l'intermediario è comunque tenuto:

1. ad informare l'autorità giudiziaria e quella di vigilanza in merito ad attività illecite "riguardanti un suo destinatario del servizio della società dell'informazione";

2. a fornire alle 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".

E vero è, infine, che, all'inadempimento di taluni obblighi, l'art. 17, comma 3, d.lg. n. 70/2003 ricollega una forma di responsabilità civile dell'intermediario.

Tuttavia, precisato che non è in discussione la responsabilità del *Provider* per la immissione di contenuti propri, né quella a titolo di concorso mediante azione nel reato commesso dagli utenti, è assolutamente condivisibile l'affermazione di chi sostiene che tali obblighi non appaiono sufficientemente qualificati per potersi concepire quali obblighi di impedire l'evento (18) - *rectius*: il reato dell'utente -. Ciò perché essi dovrebbero giocoforza presupporre un potere di controllo rispetto all'illecito agire di terzi, di cui il *Provider* certamente non può dirsi munito (19). Anzi, la grandissima mole di dati e informazioni gestite dagli intermediari consentono di sollevare più di un dubbio in ordine alla generale esigibilità di siffatto controllo (20), correttamente esclusa dallo stesso estensore della sentenza in commento.

Per concludere: certamente, l'esistenza di diverse tipologie dei prestatori di servizi della società dell'informazione (21) non permette di svolgere un discorso esaustivo perché valido per ognuno di essi. Nondimeno, appare principio ragionevole e perciò da applicare quello secondo il quale la responsabilità del *Provider* "per materiali immessi interamente ed autonomamente da altri deve ancorarsi necessariamente ad un'effettiva (previa) conoscenza del contenuto illecito, nonché ad una concreta rappresentazione della possibilità di realizzazione del fatto di reato e accettazione del rischio (e, dunque, in tal senso volizione) del fatto medesimo, non essendo sufficiente una generica "conoscibilità" delle informazioni diffuse per suo tramite" (22).

5. Brevi considerazioni finali

Con i giusti limiti di una sintesi, possono, alla fine, trarsi alcune conclusioni in ordine alla disciplina del caso pratico, peraltro forse molto meno isolato di quanto la giurisprudenza in argomento lascerebbe immaginare.

Una rapidissima nota a margine, tuttavia, non può non riguardare la scelta di perseguire e condannare determinati soggetti.

Tutte le considerazioni sopra esposte hanno visto quale termine di riferimento il *Provider* - ente impersonale, giuridicamente variamente strutturato -, che evidentemente non può esser tenuto penalmente responsabile di alcunché stante il principio di personalità della responsabilità penale stessa.

Rimarcato che neppure il d.lg. 8 giugno 2001, n. 231 prevede alcuna forma di responsabilità dell'ente in dipendenza della commissione di illeciti penali previsti dal codice della *privacy*, va qui soltanto evidenziato che ogni discorso concernente la colpevolezza, in generale, e il dolo, in particolare, dovrebbe giocoforza tener conto del fatto che un controllo da parte dei singoli - persone fisiche si presentava di ancor più difficile attuazione.

Ciò detto, va, come all'esordio, riconosciuto al tribunale di Milano il merito di avere emesso una sentenza che ha chirurgicamente individuato un problema tentando di risolverlo a diritto vigente, mentre, per altro verso, invocava, probabilmente a ragione, una "buona legge" in materia. Gli argomenti utilizzati sono acuti e di alto spessore giuridico e costituiranno sin da ora una "base" per qualsiasi discussione concernente la responsabilità di un *Provider* per fatti di illecito trattamento dei dati personali. Tema, questo, tutt'altro che accademico visto che il dibattito anche "meta-giuridico" sulla decisione di Milano ha fatto scorgere come gli interessi in gioco siano di rango costituzionale: da un lato, la libertà di manifestazione del pensiero (art. 21 Cost.), esercitata e coltivata nelle forme rese accessibili dalla potenza dei nuovi *media*; dall'altro, il diritto alla protezione dei dati personali, quale manifestazione del diritto alla *privacy*, che è radicato tra i diritti inviolabili consacrati nell'art. 2 Cost.

È, allora, facile accorgersi di come da un insoluto giuridico possano derivare conseguenze abnormi a tutto detrimento di uno dei valori in discussione. Per esser ancora più chiari: le prospettive che si disegnano all'orizzonte appaiono non incoraggianti, atteso che, da un lato, può immaginarsi una intensificazione dei controlli in Rete da parte dei *Providers* (ad es. con la predisposizione di filtri malamente calibrati); dall'altro, per la eccessiva onerosità degli adempimenti imposti dalle norme, potrebbe verificarsi un abbandono di attività non particolarmente remunerative.

Pur a fronte di siffatti rischi, tuttavia, i motivi già segnalati *supra* non consentono di ritenere corretta la interpretazione del contesto normativo fornita dal tribunale, tanto più se si pongono i paletti posti dal medesimo giudicante in merito alla inesigibilità della richiesta diretta di consenso all'interessato.

A tal proposito, pare che la rinuncia ad analizzare lo specifico termine di riferimento per il giudizio di responsabilità (il *Provider*) abbia condotto a formulare il principio di cui in massima, con la conseguenza che in taluni casi si finisce per ridurre anche troppo gli adempimenti del *Provider*.

E, invero, si rifletta a come, rispetto a un *Provider* di contenuti (23), probabilmente l'esonero dall'obbligo di verificare "in proprio" la esistenza del consenso dell'interessato al trattamento appaia ingiustificato ove si considerino le capacità conoscitive e operative che lo stesso detiene riguardo ai contenuti del sito *web*.

Al contrario, per gli *Host Provider* la capacità di controllo è inferiore sicché appare incongruo che, in presenza di un elemento aspecifico (l'informativa priva degli avvertimenti indicati dal tribunale) - che non consente di ricondurre alla sfera di sicura conoscibilità del *Provider* l'altrui attività illecita per il suo tramite commessa -, possa fondarsi la responsabilità di un soggetto attingendo alla categoria del dolo eventuale, e ciò per la particolare struttura di *Internet*, ovvero di una rete aperta cui si può apportare materiale in modo non controllabile (24).

In altre parole, l'applicazione del principio indicato in sentenza, mentre facilita fin troppo l'operato di alcuni, invece, almeno ai fini di un giudizio di responsabilità penale, si rivela troppo gravosa per altri.

La questione che resta sul tappeto è ancora quella correttamente individuata dal tribunale: *quid juris* quando colui che effettua il trattamento dei dati personali è un *Provider* che li ha raccolti presso terzi, i quali non hanno richiesto il consenso dell'interessato?

Rispetto a tale quesito pare - pur nel condivisibile auspicio che sopravvenga una specifica disciplina - che il *quantum* degli adempimenti richiedibili al *Provider* debba tener conto delle sue effettive potenzialità di controllo del contenuto immesso dagli utenti.

D'altra parte, meriterebbe approfondimento un dato: lo strumento penale, in casi come quello all'attenzione del Tribunale di Milano, oltre ad esigere accertamenti defatiganti, manifesta tutta la sua inidoneità rispetto alla esigenza di tutelare la riservatezza dell'interessato. Auspicabile è, pertanto, che prendano piede forme di tutela civilistica quale quella apprestata dall'art. 15 cod. *privacy*, che, oltre ad esser più efficienti sotto il profilo risarcitorio, non devono pagare un pesante prezzo alle esigenze di tipicità e, addirittura, introducono una inversione dell'onere della prova attraverso il richiamo all'art. 2050 c.c.

NOTE

(1) V. CORRIAS LUCENTE, La pretesa responsabilità penale degli intermediari di contenuti su internet, in Dir. inf., 2009, n. 1, p. 91 ss., che, già al momento in cui fu resa nota la formulazione della contestazione, si soffermava diffusamente proprio sulla configurabilità giuridica della diffamazione ipotizzata dagli inquirenti.

(2) Ad inquadrare in tali termini la fattispecie, è, tra gli altri, DEL CORSO, Art. 167 cod. privacy, in La protezione dei dati personali: commentario al D.lgs. 30 giugno 2003, n. 196, Codice della privacy, a cura di Bianca e Busnelli, Cedam, 2007, p. 2054 ss.

(3) In primis, a classificare così la previsione del nocumento, Sez. III, 28 maggio 2004, Barone, in Dir. inf., p. 461 ss.; conforme, Sez. III, 26 marzo 2004, Modena, ivi, 2005, p. 499. Del medesimo avviso, in dottrina, MANNA, Commento al "Codice della privacy", in Dir pen. proc., 2004, n. 1, p. 23 ss., il quale sostiene che, stante la previsione normativa del dolo specifico, il nocumento - che coinciderebbe con una parte di quell'elemento (il recare ad altri un danno) - non può considerarsi evento del reato, ben-

sì condizione obiettiva di punibilità. Dissenziente, invece, CORRIAS LUCENTE, La nuova normativa penale a tutela dei dati personali, ne Il codice dei dati personali. Temi e problemi, a cura di Cardarelli, Sica e Zeno Zencovich, Giuffrè, 2004, p. 644 s., che, tra l'altro, fa rilevare come la considerazione del nocumento quale condizione obiettiva di punibilità possa fare nascere una notevole discrasia in tema di elemento soggettivo per il caso di dolo specifico di profitto, laddove l'effetto dell'azione (il nocumento), se classificato quale condizione obiettiva di punibilità, si porrebbe al di fuori del fuoco del dolo.

(4) Del tutto condivisibili quelle di DEL CORSO, Art. 167, cit., p. 2056 s.

(5) Sez. III, 28 maggio 2004, Barone, ult. cit.; in tali termini anche Sez. V, 14 ottobre 2009, Genchi, in Riv. pen., 2010, n. 1, p. 47.

(6) Dubbio sollevato da CASELLI LAPESCHI, Sub art. 167, nel Codice in materia di protezione dei dati personali, a cura di Cassano e Fadda, Ipsoa, 2004, p. 710; nonché da PLANTAMURA, La tutela penale dei dati personali, in Dir. inf., 2007, p. 657 s.

(7) Secondo il disposto dell'art. 4, comma 1, lett. d), cod. privacy, sono dati personali sensibili quelli "idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale".

(8) La difesa, in particolar modo, sosteneva che, essendo la vittima autistica, e non affetta da sindrome di Down, i dati che rivelavano tale sua condizione non riguardavano lo stato di salute.

(9) Cfr. PATTI, Art. 11. Consenso, in Tutela della privacy, in N. leggi civ., 1999, p. 364, per cui l'informativa all'interessato costituisce "imprescindibile garanzia" della effettività del consenso. Nonché CUBEDDU, Art. 13 cod. privacy, in La protezione dei dati, cit., p. 297, secondo la quale il diritto ad esser informato con le modalità di cui all'art. 13 del codice, rappresenta "la premessa logica, non solo di un consenso informato, ma altresì della delimitazione dei diritti dei soggetti interessati e della definizione dell'ambito di tutela connesso al trattamento".

(10) Osservazione proposta da MELZI D'ERIL-VIGEVANI, Nelle motivazioni di condanna della sentenza, violazione della privacy per mancato consenso, in Guida dir., 2010, n. 25, p. 22, per cui l'informativa ex art. 13 cod. privacy "non deve contenere le regole astratte che disciplinano il corretto trattamento, bensì le peculiarità proprie di quello che il singolo titolare ha intenzione di realizzare". Va, altresì, evidenziato come lo stesso Garante per la protezione dei dati personali abbia affermato nel corso di un'intervista, reperibile sul web all'indirizzo http://zambardino.blogautore.repubblica.it/2010/04/16/il-garante-privacy-sulla-sentenza-di-milano-e-sbagliata-ma-ora-bisogna-fare-regole-non-censorie/, che "la sentenza cerca di radicare in ordinamenti che oggi non lo prevedono un dovere qualificato di informativa che non è quello previsto dal codice privacy, ma che nasce dalle caratteristiche proprie di queste tecnologie".

(11) In tema, spunto interessante quello di TORRE, Modelli di tutela penale della privacy in internet, in Dir. pen. proc., n. 2, p. 243, per cui "la incertezza sulla evitabilità dell'evento si riflette sull'elemento soggettivo, che rappresenta il profilo di maggiore criticità della responsabilità concorsuale del Provider".

(12) A esser contestata agli imputati, invero, era la commissione dei reati in concorso tra loro, ma non con i minori che avevano consegnato il video.

(13) La giurisprudenza di legittimità è intervenuta in più occasioni a delimitare i contorni del delitto di illecito trattamento, dipendente dalla mancanza di consenso, ga-

rantendo che, in primo luogo, non si tratti di trattamento per fini esclusivamente personali sottratto all'applicazione del codice (art. 5, comma 3, cod. privacy); in secondo luogo, che non si ricada in una delle fattispecie che, ex art. 24 cod. privacy, esonerano dall'obbligo di raccogliere il consenso dell'interessato. In tali termini, Sez. III, 26 marzo 2004, Modena, cit.; nonché Sez. III, 17 aprile 2004, P., in Dir. inf., 2005, p. 492.

(14) Questa l'opinione di FIANDACA, Il reato commissivo mediante omissione, Giuffrè, 1979, p. 181, secondo cui il giudizio di equivalenza ex art. 40 cpv c.p. va limitato ai reati causali puri sia in caso di realizzazione monosoggettiva sia in caso di concorso di persone. Non difforme la impostazione seguita da RISICATO, La partecipazione mediante omissione a reato commissivo, in Riv. it. dir. e proc. pen., 1995, p. 1267 ss. Al contrario, GRASSO, Il reato omissivo improprio. La struttura obiettiva della fattispecie, Giuffrè, 1983, p. 141; nonché BISORI, L'omesso impedimento del reato altrui nella dottrina e nella giurisprudenza italiane, in Riv. it. dir. e proc. pen., 1997, p. 1340 ss., ritengono che il titolare dell'obbligo di garanzia possa partecipare mediante omissione anche alla consumazione di reati privi di evento naturalistico.

(15) CARCANO, Sub art. 40 c.p., in Codice penale. Rassegna di dottrina e giurisprudenza, di Lattanzi e Lupo, Giuffrè, 2000, p. 31.

(16) V. Sez. IV, 20 aprile 1983, Bruno, in C.E.D. Cass., n. 160990.

(17) V. come, per FIANDACA, Il reato commissivo, cit., p. 196, "la Garantenstellung poggi su di un effettivo potere di signoria su alcune delle condizioni che direttamente conducono all'evento tipico; e ... il suo manifestarsi sotto forma di posizione di controllo su soggetti che costituiscono fonti di pericolo (presuppone), necessariamente, una condizione di incapacità di questi ultimi, tale da escludere o menomare la loro attitudine all'autodeterminazione responsabile".

(18) SPAGNOLETTI, La responsabilità del Provider per i contenuti illeciti di internet, in Giur. merito, 2004, p. 1922 ss.

(19) Secondo SPAGNOLETTI, La responsabilità del Provider, cit., p. 1922 ss., è da respingere anche la ricostruzione secondo cui in capo al Provider sussisterebbe "un obbligo di controllo su una fonte di pericolo, derivante dal potere di organizzazione/disposizione su cose pericolose, poiché quest'ultimo presuppone necessariamente un potere di fatto, una signoria sulla cosa, nel caso di specie difficilmente configurabile".

(20) Cfr. Trib. Milano, 18 marzo 2004, B.G., in http://www.altalex.com/index.php?idnot=7076, per cui non sussiste in capo all'Host Provider alcun obbligo giuridico di controllo del materiale contenuto negli altri siti, controllo che sarebbe, peraltro, probabilmente impossibile (per l'enorme mole di dati) oltre che poco utile, atteso che i dati sono modificabili in qualsiasi momento.

(21) In particolare, il c.d. network provider, fornisce le infrastrutture di telecomunicazione; l'access (oppure host) provider rende disponibile lo spazio web del suo server; il content provider utilizza il servizio, inserendo autonomamente i contenuti sul sito; il service provider consente agli utenti di effettuare il collegamento alla Rete, fornendo solitamente altri servizi supplementari.

(22) SPAGNOLETTI, La responsabilità del Provider, cit., p. 1922 ss.

(23) V. nota n. 20.

(24) V. Trib. Milano, 18 marzo 2004, B.G., cit.

Il caso google-vividown tra protezione dei dati e libertà di espressione on-line

Giovanni Sartor, Mario Viola de Azevedo Cunha (*)

Si esaminerà il caso Google-Vividown, conclusosi in primo grado con la condanna penale di tre dirigenti di Google per illecito trattamento di dati personali, in seguito alla distribuzione on-line di un filmato nel quale un ragazzo disabile veniva maltrattato e insultato da alcuni compagni. Dopo aver illustrato i fatti del caso e il ragionamento del giudice, si svilupperanno alcune considerazioni circa la responsabilità dei fornitori di piattaforme per la distribuzione di contenuti on-line, rispetto ai materiali prodotti e caricati dagli utenti.

1. I fatti del caso.

L'8 settembre 2006 veniva pubblicato sulla piattaforma Google-Videos (1) un filmato nel quale uno studente disabile era maltrattato e insultato da tre compagni, mentre un quarto studente riprendeva la scena con il telefono cellulare e altri dieci osservavano senza intervenire. Più esattamente, lo studente disabile, affetto da autismo e da carenze nell'udito e nella vista, era oggetto di offese verbali e fisiche. In particolare, veniva chiamato "mongolo", termine usato per indicare, con connotazione negativa, soggetti affetti da sindrome di Down. In connessione con l'attribuzione di tale qualifica, nel filmato si faceva riferimento all'associazione Vivi-Down (Associazione italiana per la ricerca scientifica e per la tutela della persona Down). Il filmato, della durata di circa tre minuti, era visto da un elevato numero di persone (era scaricato più di 5000 volte). Per qualche tempo era il filmato più popolare nella categoria "video divertenti".

Alcuni utenti di Google-Videos colpiti dalla natura offensiva del filmato pubblicavano sul sito commenti critici (a partire dall'8 ottobre). Sembra che alcuni frequentatori del sito abbiano apposto al filmato segnalazioni (flagging) negative, e che siano state inviate alcune e-mail di protesta a Google, chiedendo la rimozione del filmato. Tuttavia, dalla sentenza si evince che esiste prova solo di una segnalazione del 5 novembre 2006 e di una richiesta di rimozione del giorno successivo (Google è dichiarata incapace di fornire documentazione relativa a tutti i commenti e segnalazioni sul filmato inseriti su Google-Videos). Il 7 novembre la polizia postale italiana, dopo una comunicazione da parte di un cittadino, richiedeva a Google di eliminare il filmato, che era rimosso il giorno successivo. Pertanto il filmato rimaneva disponibile on-line per circa due mesi dal momento nel quale era stato inizialmente pubblicato (2).

La pubblicazione del filmato originava tre cause distinte. La prima riguardava i quattro studenti che avevano avuto un ruolo attivo nel filmato (i tre che avevano maltrattato il compagno disabile e quello che aveva ripreso la scena). Essi erano identificati grazie alle informazioni fornite da Google − che consentivano di risalire all'indirizzo del computer mediante il quale era stato effettuato

(*) in *Diritto dell'Informazione e dell'Informatica*, 2010, 645.

il caricamento del filmato − ed erano condannati dal tribunale di Torino per maltrattamenti e ingiurie. La seconda causa, ancora pendente a Torino, riguarda l'insegnante e la scuola (per non aver impedito il fatto). La terza causa, quella che qui si considera, riguarda Google, e più esattamente l'affiliata italiana (Google Italy) e i suoi dirigenti.

Quest'ultima causa prendeva avvio dall'azione del Pubblico ministero di Milano, che promuoveva un procedimento penale contro quattro alti dirigenti di Google (David Drummond − già presidente di Google Italy, George De Los Reyes − già membro del consiglio d'amministrazione di Google Italy, Peter Fleisher − consulente di Google per la Privacy in Europa e Arvind Desika − responsabile per il progetto Google-Videos in Europa). Le accuse contro i quattro erano le seguenti: "aver offeso la reputazione" dell'associazione Vividown e dello studente disabile e aver "omesso il corretto trattamento dei dati personali". Quindi da un lato si trattava di "concorso in diffamazione aggravata" (art. 110, 40 comma 2, 385 commi 1 e 3 del Codice penale) e dall'altro di illecito trattamento di dati personali, in particolare attinenti alla salute, a scopo di profitto (art. 167 del Codice in materia di protezione dei dati personali, o più brevemente, Codice privacy). L'associazione Vivi-Down, il Comune di Milano, e il padre dello studente disabile si inserivano nel procedimento quali parti civili, chiedendo il risarcimento dei danni.

La causa veniva decisa il 24 febbraio 2010 dal giudice Oscar Magi (Tribunale ordinario di Milano in composizione monocratica): i quattro dirigenti di Google erano assolti dall'imputazione di diffamazione e tre di essi erano condannati a sei mesi di reclusione (pena sospesa) per illecita elaborazione dei dati personali (3). Tale sentenza stimolava vivaci reazioni, anche al livello internazionale. Nel suo blog Google affermava che la decisione del tribunale milanese attaccava "gli stessi principi di libertà sui quali è costruita l'Internet" (4). L'ambasciatore statunitense in Italia, David Thorne, affermava la propria contrarietà alla tesi che "i fornitori dei servizi dell'Internet siano responsabili per i contenuti caricati dagli utenti" (5), e citando le parole del Segretario di Stato Hillary Clinton, osservava che "l'Internet libera è un diritto umano integrale che deve essere protetto nelle società libere" (6). Molti condividevano l'indirizzo libertario espresso dagli Stati Uniti, e consideravano questa decisione come un tentativo di avviare la censura sull'Internet. Si osservava anzi che tale tentativo che si collegava con le discussioni dei mesi precedenti sulla necessità di intervenire contro la pubblicazione di insulti e minacce verso personalità della politica e dell'economia (in particolare, i blogger erano stati accusati di aver istigato un'aggressione contro il Presidente del Consiglio Silvio Berlusconi) (7).

Altri commentatori approvano la decisione, ritenendo immorale che Google potesse esonerarsi da ogni responsabilità per i danni sofferti da persone innocenti in conseguenza della sua attività commerciale, attività dalla quale Google trae enormi profitti, in particolare mediante la raccolta pubblicitaria (nel 2009 i proventi pubblicitari ammontavano a più di 22 miliardi di dollari) (8). Osservavano che Google aveva i mezzi tecnici per controllare i contenuti ed escludere i

materiali illeciti: evitava tali controlli per ridurre i costi (risparmiando sul personale) e massimizzare i profitti (attraendo il vasto uditorio interessato a contenuti lascivi, sconvenienti, o offensivi). Pertanto, come osservava uno dei pubblici ministeri milanesi, Alfredo Robledo, la decisione non riguardava la censura, ma piuttosto il bilanciamento tra la libertà d'impresa e la dignità della persona (9).

Nei giorni successivi alla decisione, si formulavano diverse ipotesi, on-line e off-line, sui fondamenti giuridici della decisione stessa, finché la motivazione non era rilasciata, il 12 aprile 2010, più di un mese in anticipo rispetto alle attese. Nel presente contributo si esamineranno le principali questioni considerate nella decisione e si illustrerà il ragionamento del giudice prima di sviluppare alcune considerazioni generali su protezione dei dati e libertà di espressione del pensiero.

2. L'assoluzione dell'imputazione per diffamazione.

Il reato di diffamazione, previsto dall'art. 595 del Codice Penale, consiste nell'offendere l'altrui reputazione comunicando con più persone, ed è aggravato dall'uso della stampa o di "qualsiasi altro mezzo di pubblicità" (inclusa quindi la diffusione mediante l'Internet). Dal momento che tutti gli imputati sono stati assolti da tale accusa, è sufficiente dedicare un'attenzione limitata a questa questione, soffermandosi su alcune argomentazioni sviluppate dal giudice.

Una questione preliminare consiste nel fatto che la diffamazione è procedibile solo su querela della parte offesa. Nel caso in esame lo studente (mediante il proprio genitore) si era ritirato dalla causa (in seguito ad un accordo con Google). Tuttavia, il giudice superava l'ostacolo ritenendo che anche l'associazione Vivi-down, quale ente esponenziale degli interessi delle persone affette da sindrome di Down (offese nel filmato) fosse legittimata a proporre la querela.

Passiamo quindi ad esaminare la realizzazione degli elementi del reato di diffamazione. Secondo il pubblico ministero, la responsabilità penale dei dirigenti di Google risulterebbe dal loro comportamento omissivo: i dirigenti avevano l'obbligo giuridico di prevenire la diffamazione esercitando un controllo preventivo sui contenuti caricati sul sito Google-Videos, obbligo a quale essi non avrebbero ottemperato. Data l'esistenza di questo obbligo, l'omissione delle misure preventive contro la diffusione on-line di filmati offensivi equivarrebbe ad aver causato tale diffusione (secondo l'art. 40 del Codice Penale, "Non impedire un evento, che si ha l'obbligo giuridico di impedire, equivale a cagionarlo"). L'esistenza dell'obbligo di controllare e prevenire, deriverebbe dal fatto che Google, secondo il pubblico ministero, non è un mero host provider, non si limita ad ospitare nei propri computer contenuti prodotti da altri, rendendoli accessibili in rete. Al contrario, Google sarebbe un fornitore di contenuti (content provider), su cui grava l'obbligo giuridico di elaborare correttamente i dati personali inseriti in quei contenuti, adempiendo alle norme del Codice privacy. In conclusione, secondo il pubblico ministero la mancata corretta elaborazione dei dati personali (il fatto che fossero caricati e resi disponibili mediante Internet

dati personali al di fuori delle condizioni previste dalla legge) avrebbe causato la diffamazione e quindi i dirigenti di Google, che avrebbero dovuto assicurare la corretta elaborazione dei dati, sarebbero responsabili per il reato di diffamazione.

Il giudice rispondeva che − benché egli si augurasse l'emanazione 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)" − allo stato del diritto vigente doveva riscontrare l'assenza di un obbligo generale di controllo a carico dei fornitori di servizi di hosting (10). Pertanto assolveva gli imputati dall'accusa di diffamazione: poiché Google non aveva l'obbligo di prevenire il caricamento di materiali offensivi sul proprio sito, essa non poteva essere ritenuta responsabile per la diffamazione conseguente alla diffusione di quei materiali. L'argomentazione del giudice solleva alcune perplessità: da un lato egli esprime il desiderio che sia introdotta una responsabilità generale per il mancato controllo, e dall'altro egli afferma che il provider si trova nell'impossibilità di controllare ogni contenuto, cosicché l'obbligazione di esercitare un puntuale controllo preventivo sarebbe inesigibile.

Un'interpretazione coerente di questi enunciati può forse essere la seguente: il giudice auspica che il legislatore introduca un obbligo generale, gravante sui provider, di adottare misure precauzionali, ma tale obbligo − che non potrebbe essere così rigido da richiedere l'esame umano di ogni filmato, ma dovrebbe essere attuabile anche mediante soluzioni automatizzate, almeno in parte − sarebbe sufficiente per affermare una responsabilità per diffamazione nel caso di specie.

È interessante osservare, tuttavia, che il giudice non menziona, come fondamento per l'irresponsabilità del provider, l'esenzione prevista dal Decreto legislativo n. 70 del 9 aprile 2003, che ha attuato la Direttiva europea sul commercio elettronico (11). L'art. 16 di tale decreto riguarda specificamente l'host provider, cioè il fornitore del servizio di hosting, che ospita sul proprio sistema informatico contributi predisposti dal destinatario del servizio, rendendoli accessibili ai terzi. Tale soggetto è esente da responsabilità qualora "*a*) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione; *b*) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso". Inoltre, secondo l'art. 17 dello stesso decreto, il provider non ha né un "obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza", né un "obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite".

Ricordiamo che anche il diritto statunitense prevede esenzioni dalla responsabilità dei provider analoghe a quelle introdotte dalla disciplina europea. Il Communications Decency Act del 1996 (CDA), sezione 230(c), stabilisce, con riguardo alle questioni estranee alla proprietà intellettuale che: "Nessun fornito-

re o utente di un sistema informatico interattivo sarà considerato un editore o autore di qualsiasi informazione fornita da altri" (12). Una più limitata esenzione di responsabilità è prevista per le violazioni del diritto d'autore nel Digital Millennium Copyright Act (DMCA).

Ci sembra che la mancata applicazione dell'esenzione prevista per gli host provider dipenda dal fatto che il giudice ha ritenuto che Google, nell'ambito del servizio Google-Videos, non si limitasse ad ospitare contenuti prodotti da altri, ma estendesse la propria azione alla promozione e all'organizzazione di quei contenuti. Di conseguenza, secondo il giudice (che quindi concorda, su questo punto, con il pubblico ministero), Google, anziché un mero host provider era un fornitore di contenuti (content-provider) che non poteva avvalersi dell'esenzione (13). Come vedremo nel seguito, tale conclusione si fonda sull'osservazione che per Google la messa a disposizione della piattaforma Google-Videos rappresentava un'attività commerciale, e che nell'ambito di tale attività Google stimolava il caricamento, senza controlli, di filmati creati dagli utenti. Pertanto, secondo il giudice, l'inclusione di quei contenuti nel sito e la loro conseguente distribuzione dovrebbero considerarsi risultato dell'attività commerciale di Google, oltre che dell'iniziativa dei suoi utenti.

3. Responsabilità nell'ambito della protezione dei dati: elaborazione di dati personali senza autorizzazione.

Passiamo alla seconda imputazione, quella per la quale i dirigenti di Google sono stati condannati. Si tratta del reato di "*trattamento illecito dei dati*", di cui all'art. 167 del Codice privacy. Tale reato viene commesso quanto taluno "al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali", in violazione di alcune norme del Codice privacy. Tra le ipotesi previste dall'articolo 167 è rilevante soprattutto l'art. 26 secondo il quale i dati personali sensibili possono essere trattati solo quando ricorrano due condizioni: il consenso scritto dell'interessato e l'autorizzazione del Garante. Tra i dati sensibili, a norma dell'art. 4 del Codice privacy rientrano i "dati personali idonei a rivelare lo stato di salute" dell'interessato. Combinando questi elementi otteniamo il reato per il quale i dirigenti di Google sono stati condannati: allo scopo di trarre profitto, essi partecipavano al trattamento del filmato contenente dati sulla salute dello studente disabile, senza il consenso di quest'ultimo (dei suoi rappresentanti legali) e inoltre senza l'autorizzazione del Garante Privacy. Questa condanna solleva alcune importanti questioni giuridiche, che saranno esaminate nelle pagine seguenti:

1. È applicabile al trattamento del filmato la legge italiana sulla protezione dei dati?
2. Conteneva il filmato dati personali, e in particolare dati sanitari?
3. Chi trattava il filmato?
4. Avrebbe dovuto Google richiedere il consenso dello studente disabile al fine di trattarne i dati?

5. Avrebbe dovuto Google informare gli studenti che avevano caricato il filmato circa gli obblighi attinenti alla protezione dei dati?

6. Poteva Google ritenersi responsabile (solo) civilmente?

7. Era Google esonerata dalla responsabilità, quale host-provider?

8. Vi è una specifica esenzione da responsabilità per la libertà di espressione?

Sulla base delle risposte a queste domande cercheremo di sviluppare alcune considerazioni generali in tema della responsabilità dei provider di piattaforme destinate ad ospitare contenuti prodotti dagli utenti, rispetto a questi contenuti.

3.1. È applicabile la legge italiana sulla protezione dei dati?

Il giudice ha dovuto affrontare la questione preliminare attinente alla legge applicabile: si applica la leggi italiana al servizio Google-Videos, che riguarda trattamenti di dati aventi luogo esclusivamente o prevalentemente negli Stati Uniti? Infatti, un trattamento è soggetto alla disciplina italiana solo se è soddisfatta una delle seguenti condizioni (Art. 5 del Codice privacy):

1. Il trattamento è effettuato da soggetto stabilito nel territorio dello Stato;

2. Il trattamento è effettuato da soggetto che, pur non essendo stabilito nell'Unione Europea, impiega strumenti situati nel territorio dello Stato.

Secondo il giudice la prima condizione risultava soddisfatta: il trattamento dei dati attinente a Google-Videos si compieva presso Google Italy, la controllata italiana di Google Inc., stabilita a Milano. Questa conclusione si connette alle seguenti affermazioni (benché manchi un'esplicita argomentazione): a) Google Italy era la "mano operativa e commerciale" di Google Inc; b) Google Italy, come ogni altra controllata da Google, era sostanzialmente una parte del gruppo, che operava in modo unitario, sotto la direzione di Google Inc; c) Google Italy aveva la possibilità di collegare annunci pubblicitari ai filmati, usando il servizio Google-AdWords.

In realtà, risulta che i computer (i server) per la piattaforma Google-Videos fossero collocati negli Stati Uniti, mentre i controlli sui contenuti caricati su tale piattaforma fossero effettuati in Irlanda, attraverso la controllata irlandese di Google Inc. Inoltre, non sembra che l'uso di Google-AdWords fosse controllato da Google Italy, trattandosi di sistema nel quale i collegamenti (link) ad annunci pubblicitari sono effettuati alla base delle scelte degli inserzionisti (le imprese che si avvalgono del servizio Google-AdWords per la propria pubblicità) e quei collegamenti non portano ai filmati, ma collegano la pagina dei filmati al sito web indicato dall'inserzionista.

Forse possiamo interpretare l'argomento del giudice come segue: Google Italy contribuiva ad un processo commerciale che includeva il trattamento dei filmati caricati in Italia. Lo faceva promovendo il servizio Google-Videos e le funzionalità pubblicitarie ad esso afferenti (mediante Google-AdWords). Pertanto, secondo il giudice, Google Italy partecipava al trattamento dei filmati, benché i server che memorizzavano e diffondevano i filmati fossero collocati al di fuori dell'Italia e fossero gestiti da Google Inc. La partecipazione di Google

Italy non sarebbe esclusa dal fatto che tutte le decisioni e i controlli fossero effettuati al fuori dell'Italia, trattandosi di strategia commerciale adottata da Google Inc. per evitare di essere soggetta al diritto italiano.

Ci permettiamo di osservare che il modo in cui è affrontato il difficile tema del diritto applicabile ai trattamenti di dati effettuati all'estero ci sembra essere una delle debolezze di questa decisione, ed è un peccato che il giudice non abbia motivato con maggior chiarezza la propria decisione a questo riguardo. L'incertezza al riguardo è accresciuta dal fatto che il Garante ha affermato che l'elaborazione dei dati effettuata da Google negli Stati Uniti, anche con dati trasmessi da utenti italiani, non è soggetta alla legge italiana (14).

3.2. Conteneva il filmato dati personali, e in particolare dati sanitari?

Assumendo con il giudice che la legge italiana sulla protezione dei dati trovi applicazione (benché, come abbiamo osservato, ciò sembri assai dubbio), dobbiamo considerare se siano soddisfatte le condizione affinché possa essere commesso un reato attinente alla protezione dei dati, cioè se dati personali siano stati trattati in violazione di una norma penale.

In primo luogo dobbiamo esaminare se il filmato comprendesse dati personali, una questione alla quale il giudice non dedica particolare attenzione, assumendo senza argomentare che il filmato contenesse dai personali e in particolare dati sanitari afferenti allo studente disabile. Noi concordiamo con questa conclusione, ma la discuteremo brevemente, non essendo essa così ovvia.

Iniziamo con l'osservare che un filmato contiene dati personali quando raffigura una persona identificabile sulla base delle immagini del filmato e delle informazioni ulteriori (scritte, link, ecc.) associate al filmato stesso. Ciò si verificava nel filmato raffigurante lo studente disabile. Il problema è stabilire se quei dati personali possano essere considerati dati sensibili, essendo atti a rivelare le condizioni di salute dello studente. L'immagine di una persona può rivelare dati sensibili su di essa (le caratteristiche corporee possono rivelare l'origine etnica, l'abbigliamento può indicare la fede religiosa, lo stato fisico può rivelare le condizioni di salute, ecc.), ma sembra assurdo assoggettare ogni immagine atta a rivelare dati sensibili alle regole restrittive che governano i dati sensibili, anche quando l'immagine riveli informazioni che il soggetto non intendeva nascondere, o intendeva perfino comunicare con il proprio aspetto (ad esempio, indossando certi simboli religiosi o politici).

Un'indicazione per affrontare la questione viene dal Gruppo di lavoro ex articolo 29 (15), secondo il quale le immagini distribuite sull'Internet non contengono dati personali sensibili "a meno che non siano esplicitamente usate per rivelare informazioni sensibili sulle persone" (16). Nel caso in esame, tuttavia, possiamo affermare che le immagini intendevano rivelare e diffondere dati sensibili sulla vittima, in quanto gli autori dell'abuso mettevano in risalto nel filmato la condizione di disabile della vittima. Inoltre il titolo del filmato faceva riferimento alle condizioni di salute della vittima (parlando "andicappato", sic). È vero che gli autori attribuivano alla vittima la sindrome di Down, anziché la rea-

le condizione di questa (autismo), ma ciò che importa è l'indicazione di una condizione di disabilità.

3.3. Chi trattava il filmato?

Avendo stabilito che il filmato conteneva dati personali attinenti alla salute dello studente disabile, dobbiamo considerare se quei dati fossero trattati da Google. Ciò può sembrare ovvio, dato l'ampio spettro di operazioni elencate nella definizione del concetto di "trattamento" nell'art. 4, comma 1.a del Codice privacy: "la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati".

Si potrebbe tuttavia adottare una diversa opinione assumendo che il filmato fosse trattato dagli studenti che l'avevano caricato sulla piattaforma Google-Videos e che Google si limitasse a fornire gli strumenti per tale trattamento. È importante, inoltre, distinguere i diversi ruoli del titolare e del responsabile dell'elaborazione dei dati. Secondo il Codice privacy (art. 4, comma f), il primo è il soggetto cui "competono [...] le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati" mentre il secondo è il soggetto "preposto dal titolare al trattamento di dati personali" (art. 4, comma g).

Sembra che gli studenti che hanno caricato il filmato possano essere qualificati come titolari dell'elaborazione, avendo preso l'iniziativa di trattare il filmato, nelle modalità offerte dalla piattaforma Google-Videos. Il Codice privacy (art. 5, comma 3) esclude dalla disciplina della protezione dei dati i trattamenti effettuati "da persone fisiche per fini esclusivamente personali", ma tale esclusione non copre la diffusione dei dati mediante siti accessibili al pubblico senza restrizioni. Ciò è stato affermato dal Gruppo di lavoro ex articolo 29 nella sua opinione sulle reti sociali (social networking): gli utenti di una rete sociale quando vanno al di là di un'attività puramente personale o casalinga (come avviene quando essi usano altre piattaforme tecnologiche per pubblicare dati personale sulla rete) diventano "titolari del trattamento". Pertanto, essi sono soggetti alle norme sulla protezione dei dati, e in particolare hanno l'obbligo di ottenere il consenso delle persone le cui informazioni (o immagini) intendono rendere disponibili sull'Internet (17).

Avendo classificato i "caricatori" (uploader) del filmato come "titolari del trattamento", ci rimane da esaminare la posizione di Google. Google può essere qualificata in tre modi: o è titolare del trattamento, unitamente agli utilizzatori, o è un incaricato, che tratta i dati per conto degli utilizzatori, o è il mero fornitore di strumenti software e hardware impiegati dagli utilizzatori dei suoi servizi. Il giudice ha chiaramente respinto l'ultima opzione, ritenendo che Google sia titolare o almeno responsabile del trattamento. Si può argomentare che tale distinzione non sia rilevante ai nostri fini, dal momento che sia il titolare sia il responsabile del trattamento sono soggetti al Codice privacy. Ci possiamo tuttavia

chiedere se alcune norme sulla protezione dei dati si applichino solo al titolare, e non al responsabile, quando il titolare abbia raccolto i dati trattati. In particolare, in questo caso si potrebbe sostenere che l'obbligo di ottenere il consenso dell'interessato e l'autorizzazione del Garante riguardi il solo titolare, dovendo il responsabile procedere per conto del titolare, sui materiali e sulla base delle istruzioni fornitegli. Pertanto il responsabile dovrebbe essere sanzionato solo per le proprie scelte, non per le scelte che riguardano il solo titolare dallo stesso titolare. Poiché sono stati i titolari (gli studenti) a caricare dati concernenti un terzo, spettava ad essi ottenere il consenso e più in generale rispettare le norme che disciplinano la raccolta dei dati.

3.4. Doveva Google richiedere il consenso dello studente disabile al fine di elaborare i suoi dati?

Secondo il giudice Magi, come abbiamo osservato, Google in collaborazione con gli studenti autori del filmato, trattava illecitamente dati attinenti alla salute, senza il consenso dell'interessato e senza l'autorizzazione del Garante. Il giudice, tuttavia, cerca di evitare una conclusione troppo ampia, cioè la conclusione che il fornitore di una piattaforma per la diffusione di contenuti su Internet commetta un reato ogni qualvolta contenuti illeciti siano pubblicati sulla sua piattaforma, e in particolare, ogni qualvolta informazioni sulla salute siano diffuse senza il consenso dell'interessato. A questo proposito il giudice sviluppa due argomenti.

Il primo argomento consiste nell'osservazione che l'obbligazione di ottenere il consenso non è applicabile al fornitore della piattaforma quando l'utente pubblichi immagini di terzi. Infatti, argomenta il giudice, per adempiere a questa obbligazione, il provider dovrebbe controllare ogni immagine, e dovrebbe rifiutare ogni immagine che contenga dati personali (e in particolare dati sulla salute) qualora non gli sia fornita la prova del consenso di tutti gli individui riconoscibili nell'immagine, consenso che deve essere scritto per i dati sulla salute. Si tratta di comportamento impossibile (data l'enorme quantità di materiali caricati ogni giorno sull'Internet), e quindi inesigibile: il provider sarebbe pertanto esonerato dall'obbligo di ottenere il consenso. Il secondo argomento, anch'esso tratteggiato dal giudice, riguarda il fatto che i dirigenti di Google non potevano sapere che il filmato era stato caricato senza il consenso dell'interessato e quindi non potevano possedere l'elemento soggettivo richiesto dal reato in questione.

Quindi, secondo il giudice Magi, i dirigenti di Google non potevano commettere un reato omettendo di richiedere il consenso allo studente disabile, perché innanzitutto erano esonerati da tale obbligo, e in subordine perché, anche se non fossero stati esonerati, non avrebbero avuto lo stato psicologico richiesto (la conoscenza che il consenso non era stato richiesto).

3.5. Doveva Google informare gli autori del filmato circa la protezione dei dati?

Sulla base di considerazioni sviluppate nel paragrafo precedente, sembra che il giudice avrebbe dovuto escludere la responsabilità penale dei dirigenti di Google, e avrebbe dovuto assolverli dal reato ad essi attribuito. Invece, come vedremo nelle sezioni seguenti, egli trova un modo diverso per giungere ad una conclusione positiva circa la responsabilità degli stessi: tale responsabilità viene fondata sul fatto che il filmato è stato trattato da Google senza adottare adeguate cautele, intese a prevenire la violazione dei diritti dell'interessato e in particolare senza informare adeguatamente i propri utenti (gli studenti che hanno caricato il filmato) dei loro obblighi attinenti alla protezione dei dati (l'obbligo di non pubblicare dati personali, in particolare sulla salute, al di fuori delle condizioni previste dalla legge). È difficile vedere, tuttavia, come questo comportamento omissivo possa fondare una responsabilità penale dei dirigenti di Google, responsabilità che deve fondarsi sulla violazione di un obbligo previsto dalla legge. A questo riguardo sono potenzialmente rilevanti gli obblighi che discendono dall'art. 17 del Codice privacy, attinente all'autorizzazione da parte del Garante, e gli artt. 13 e 16 attinenti all'ottenimento del consenso dell'interessato.

È vero che secondo l'art. 17 del Codice privacy per trattare dati personali attinenti alla salute si deve richiedere un'autorizzazione del Garante, e poi si debbono osservare le precauzioni stabilite dallo stesso. Tuttavia, le precauzioni da osservare, a pena di sanzione penale sono solo quelle stabilite dal Garante. Pertanto Google potrebbe aver violato l'art. 17 solo per non aver ottenuto l'autorizzazione del Garante per il trattamento di dati personali attinenti alla salute, pur sapendo che con ogni probabilità i suoi utilizzatori avrebbero caricato anche dati sulla salute di terzi. Possiamo supporre che Google non abbia richiesto tale autorizzazione ritenendo (e desiderando) che la sua attività di trattamento dati − effettuata mediante server situati negli Stati Uniti − fosse governata esclusivamente dalla legge statunitense. La soggezione di tale attività alla sola legge statunitense era stata affermata dal Garante e ribadita in comunicazioni con Google, e sembra quindi che, anche se si accogliesse la tesi che Google abbia violato l'art. 17, si dovrebbe ritenere che ciò sia dovuto a un errore inevitabile di diritto (l'erroneo assunto che il trattamento sia governato solo dal diritto statunitense), un errore che, secondo una famosa decisione della corte costituzionale (n. 364/1988), esclude la responsabilità penale.

Passiamo a considerare l'obbligo di fornire informazioni sul trattamento dei dati. È vero che l'art. 13, comma 1 del Codice privacy richiede che "L'interessato o la persona presso la quale sono raccolti i dati personali" siano "previamente informati oralmente o per iscritto" sulle modalità del trattamento e sui diritti d'accesso e controllo. Tuttavia, questa disposizione è intesa a fornire all'interessato informazioni che gli consentano di decidere se fornire i propri dati e di esercitare i propri diritti. Tale disposizione non è applicabile al caso qui considerato, nel quale chi caricava i dati su Google-Videos era perfettamente consapevole di come i dati sarebbero stati trattati e distribuiti. Si può sostenere che, come vedremo nella sezione seguente, Google avrebbe dovuto informare gli autori del filmato dell'obbligo di non caricare dati illegalmente, ma

quest'ultimo dovere è distinto dall'obbligo sanzionato penalmente di informare gli interessati circa l'ambito e gli obiettivi del trattamento e circa i loro diritti di accesso.

3.6. Potrebbe Google essere civilmente responsabile (per fatto illecito)?

L'esclusione di una responsabilità penale di Google non impedisce che questa sia responsabile civilmente. Infatti, l'art. 15 del Codice privacy stabilisce che "Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del Codice Civile". Si tratta, come è noto della responsabilità per attività pericolose, che prescinde dalla colpa (pur ammettendo la prova liberatoria di aver adottato tutte le misure idonee a prevenire il danno).

Pertanto, se si potesse provare che gli studenti non avrebbero caricato on-line il filmato qualora fossero stati informati su obblighi e sanzioni attinenti alla protezione dei dati, allora Google potrebbe essere responsabile. Si può certamente convenire che Google avrebbe potuto fornire una migliore informazione ai propri utenti. Come il Gruppo di lavoro ex articolo 29 ha affermato, nella sua opinione relativa alle reti sociali on-line, il fornitore di servizi di social networking dovrebbe "mettere in guardia gli utenti sui rischi per la loro privacy e per quella altrui" e comunicare loro "che inserire dati su terzi può pregiudicare il diritto altrui alla privacy e alla protezione dei dati" e che "se desiderano pubblicare foto o dati riguardanti terzi, dovrebbero farlo solo con il consenso degli interessati" (18).

È vero che Google aveva elencato, tra le condizioni per l'uso di Google-Videos, anche il requisito generico che chi caricava dati avrebbe dovuto rispettare i diritti di ognuno, inclusa la privacy, ma questo riferimento può considerarsi insufficiente, considerando gli specifici rischi attinenti alla privacy connessi con la distribuzione di filmati prodotti dagli utenti.

Pertanto, se si potesse stabilire un collegamento tra la mancata informazione sulla protezione dei dati e il caricamento del filmato, allora Google potrebbe ritenersi civilmente responsabile, ma si tratta di questione che va al di là del tema qui esaminato, la responsabilità penale del provider. È da osservare che il padre dello studente disabile ritirò la propria querela in seguito ad un accordo con Google sul risarcimento del danno, come ricorda il giudice nella motivazione della sentenza (19).

Non si tratterebbe però di responsabilità per la pubblicazione di informazioni illecite, ma di responsabilità per il danno conseguente all'omissione di una fondamentale precauzione. Come vedremo nel seguito, l'obbligo di informare gli utenti sulla protezione dei dati sembra pienamente compatibile con la ratio dell'esenzione dalla responsabilità per gli host-provider: rispettare tale obbligo non richiede interventi censori rispetto alle informazioni ospitate nelle piattaforme on-line.

3.7. È Google esonerata da responsabilità, essendo un fornitore di servizi di hosting?

La difesa di Google ha richiamato l'esenzione dalla responsabilità prevista per gli host provider, affermando che Google, in quanto tale, non sarebbe responsabile per i contenuti forniti dai propri utenti. Per rispondere a questo argomento il giudice discute estesamente quale qualificazione giuridica sia applicabile a Google e in particolare se Google Italy, quale fornitore del servizio Google-Videos, sia un mero host provider o un fornitore di contenuti. Questa distinzione è rilevante in quanto sono esenti da responsabilità solo i fornitori di hosting (non i fornitori di contenuti). Secondo l'art. 14 della Direttiva sul commercio elettronico (e l'art. 16 del Decreto legislativo di attuazione), l'attività dei fornitori di servizi di hosting consiste "nella memorizzazione di informazioni fornite da un destinatario del servizio".

Quando la Direttiva è stata emanata il fenomeno cui essa si rivolgeva (hosting) consisteva prevalentemente in siti web (pagine html e documenti collegati) predisposti dagli utenti. L'host-provider rendeva disponibile il server (spazio disco ed elaboratore) per memorizzare il sito, il collegamento verso l'Internet, e il software (il web-server) per accedere al sito (digitando un nome di dominio o usando un motore di ricerca). Negli ultimi anni il servizio di web-hosting ha subito una radicale trasformazione: i contenuti prodotti dagli utenti sono ora caricati su piattaforme che facilitano la preparazione dei contenuti e la loro pubblicazione in rete (tra i più diffusi: YouTube per i filmati, Facebook per le informazioni personali, Wordpress per i blog, Twitter per brevi messaggi, ecc.). La maggior parte delle piattaforme sono gestite da società commerciali che traggono profitto associando messaggi pubblicitari ai materiali prodotti dagli utenti, spesso (come nel caso di Google) selezionando automaticamente gli annunci sulla base del contenuto di quei materiali. Pertanto, la questione affrontata dal giudice è la seguente: un Internet provider è ancora un mero fornitore di hosting quando il provider abiliti il caricamento di contenuti, la loro preparazione e successiva distribuzione, indicizzi quei contenuti per facilitarne la ricerca, li colleghi a messaggi pubblicitari, e svolga tutte tali attività a scopo di profitto?

La conclusione del giudice è negativa rispetto a questo tipo di soggetto (che chiama hoster attivo), e quindi in concreto rispetto a Google: Google non è un mero host provider, è un "hoster" attivo e pertanto un fornitore di contenuti. Di conseguenza l'esclusione dalla responsabilità prevista dalla disciplina del commercio elettronico non si applicherebbe a Google-Videos (e similmente, non si applicherebbe a YouTube, Facebook, Wordpress, ecc.). Per sostenere questa conclusione il giudice fa riferimento ad una recente decisione (sentenza 49437 del 2009) della Corte di Cassazione che ha affermato la responsabilità penale, per la violazione della proprietà intellettuale, dei titolari di un sito web (il sito svedese Pirate Bay) per lo scambio peer-to-peer di contenuti digitali (scambio che avviene cioè senza che i contenuti siano registrati del sito, il quale si limita a porre in collegamento i computer degli utenti). La Corte di Cassazione ha affermato che fornendo accesso mediante indici ai contenuti nei computer degli

utenti (anziché limitarsi a consentire la comunicazione tra gli utenti stessi) i titolari del sito avrebbero partecipato ai reati commessi dagli utenti.

L'adozione del concetto restrittivo di "host provider" proposto dal giudice Magi avrebbe un ampio impatto, non limitato al tema della protezione dei dati, sulla disciplina dell'informazione on-line: la clausola che esonera dalla responsabilità i fornitori di servizi di hosting non si applicherebbe ai fornitori delle più diffuse piattaforme per la distribuzione di contenuti digitali, fornitori che sarebbero quindi responsabili, in linea di principio, per tutti i contenuti illeciti caricati dai loro utenti. Infatti, per classificare Google come un fornitore di contenuti, il giudice Magi prende in considerazione diversi fattori (che potrebbero facilmente ritrovarsi, mutatis mutandis, presso altri fornitori di piattaforme): Google aveva attivamente stimolato il caricamento dei filmati su Google-Videos; aveva promosso la pubblicazione di contenuti prodotti dagli utenti senza controlli, al fine di superare la concorrenza di altre analoghe piattaforme; aveva attivamente contribuito all'organizzazione dei filmati, indicizzandoli e collegandoli a messaggi pubblicitari.

Questa conclusione contraddice però una recente decisione della Corte di Giustizia dell'Unione Europea (20), preceduta da un'opinione dell'avvocato generale Miguel Poiares Maduro (21). Nella motivazione della decisione (riguardante l'uso di marchi di note imprese per attivare link a informazioni pubblicitarie, e il loro posizionamento nelle risposte fornite dal motore di ricerca di Google), la Corte ricorda che il prestatore di un servizio di hosting ("consistente nella memorizzazione di informazioni fornite da un destinatario del servizio") non può essere ritenuto "responsabile per i dati che ha memorizzato su richiesta di un destinatario del servizio in parola, salvo che tale prestatore, dopo aver preso conoscenza, mediante un'informazione fornita dalla persona lesa o in altro modo, della natura illecita di tali dati o di attività di detto destinatario, abbia omesso di prontamente rimuovere tali dati o disabilitare l'accesso agli stessi". Ricorda altresì la Corte che "il legislatore ha definito la nozione di "servizio della società dell'informazione" come comprendente i servizi prestati a distanza mediante attrezzature elettroniche di trattamento e di memorizzazione di dati, a richiesta individuale di un destinatario di servizi e, normalmente, dietro retribuzione".

Pertanto "la semplice circostanza che il servizio di posizionamento sia a pagamento, che la Google stabilisca le modalità di pagamento, o ancora che essa dia informazioni di ordine generale ai suoi clienti, non può avere come effetto di privare la Google delle deroghe in materia di responsabilità previste dalla direttiva 2000/31". Secondo la Corte la responsabilità può solo riguardare "il ruolo svolto dalla Google nella redazione del messaggio commerciale che accompagna il link pubblicitario o nella determinazione o selezione di tali parole chiave". La responsabilità non può riguardare i contenuti prodotti dagli utenti, qualora il provider svolga un ruolo "meramente tecnico, automatico e passivo, comportante una mancanza di conoscenza o di controllo dei dati che esso memorizza".

Non possiamo qui approfondire il concetto di neutralità, ma ci sembra che contrariamente all'opinione del giudice Magi, per distinguere i fornitori di hosting dai fornitori di contenuti non ci si può basare sulla natura commerciale del servizio fornito, né sul fatto che il caricamento dei materiali e l'accesso ad essi siano oggetto di promozione pubblicitaria, e neppure sul fatto che il servizio sia a pagamento. L'accento deve essere sulla connessione tra il fornitore e l'informazione resa disponibile sul sito, distinguendo il ruolo del fornitore stesso rispetto a diversi contenuti. Pertanto, si potrebbe discutere se, dato il funzionamento di Adwords (che descriveremo nel seguito), Google sia un fornitore di contenuti rispetto ai link pubblicitari attivi presso i suoi servizi, ma certamente non è un fornitore di contenuti (è un mero hoster) rispetto ai filmati caricati autonomamente dagli utenti (anche se gli utenti sono stati motivati da un'iniziativa di marketing promossa da Google).

3.8. Un'esenzione per la libertà di espressione?

Né il giudice né le parti hanno considerato la possibilità di escludere la responsabilità penale nel caso in esame con riferimento alla tutela della libertà della manifestazione del pensiero e dell'espressione artistica (22). A norma dell'articolo 136 e 137 del Codice privacy né il consenso dell'interessato né l'autorizzazione del Garante sono richieste per il trattamento di dati (anche attinenti alla salute) temporaneo finalizzato esclusivamente alla pubblicazione o diffusione occasionale di articoli, saggi e altre manifestazioni del pensiero anche nell'espressione artistica. Pertanto, se il filmato fosse considerato un'espressione artistica (benché aberrante) il reato attribuito a Google non sarebbe stato commesso.

Ovviamente, gli autori del filmato dovrebbero comunque affrontare le imputazione di maltrattamenti, ingiuria e diffamazione, ma non avrebbero commesso alcuna violazione della disciplina sulla protezione dei dati (almeno per quanto riguarda l'illecito trattamento di dati attinenti alla salute). Non svilupperemo ulteriormente questo argomento, che richiederebbe un attento esame di vari aspetti, come i diversi diritti e valori implicati, la minore età dell'interessato, ecc. Tuttavia, speriamo che possa contribuire a illustrare la difficoltà del compito che Google dovrebbe affrontare, se dovesse operare quale guardiano della sua piattaforma per filmati: non solo Google dovrebbe controllare se siano pubblicati dati personali o sensibili, ma dovrebbe anche accertare se non ricorrano le condizioni perché i dati siano comunque pubblicabili, in omaggio alla libertà di manifestazione del pensiero ed espressione artistica.

4. Che cosa manca?

Riassumiamo l'argomento fondamentale del giudice. La mancanza giuridica (e morale) che il giudice attribuisce a Google è la seguente: Google promoveva il caricamento senza restrizioni di contenuti da parte degli utenti, anziché limitarsi a fornire filmati di alta qualità, come facevano alcuni concorrenti. Google sapeva che tale politica avrebbe condotto alla pubblicazione di materiali illegali,

ma l'adottava ugualmente, per conquistare una più ampia quota del mercato, alla ricerca del profitto. Inoltre, sempre a scopo di profitto, Google non adottava misure cautelative che avrebbero potuto prevenire il caricamento di materiali illegali: Google non esercitava alcun controllo preventivo sui materiali caricati, non poneva alcun filtro teso ad identificare materiali potenzialmente dannosi e non informava i suoi utenti (interessati a pubblicare materiali sulla piattaforma) che certi contenuti (in particolare quelli contenti dati personali attinenti alla salute) avrebbero violato la disciplina della protezione dei dati, esponendo chi li pubblicava on-line a sanzioni giuridiche. Pertanto, secondo il giudice, Google deve considerarsi penalmente responsabile per il trattamento di dati attinenti alla salute in mancanza delle condizioni richieste dalla legge (informare l'interessato, ottenerne il consenso, ottenere l'autorizzazione del garante, rispettarne le prescrizioni).

Ci sembra che questo modo di affrontare il tema sottoposto al giudice mostri non solo un discutibile orientamento politico-giuridico, ma anche un'incompleta comprensione degli interessi e dei valori in discussione.

È vero, Google trae profitto dall'attività dei suoi utenti, che pubblicano materiali sulle piattaforme fornite da Google stessa. Attraverso l'opera di centinaia di migliaia di utenti-caricatori Google ottiene la disponibilità di un enorme deposito di filmati, cui accedono centinaia di milioni di utenti-scaricatori. Indicizzando questi filmati e rendendoli accessibili sulla propria piattaforma, Google ottiene grandi profitti. Ciò si realizza principalmente fornendo agli utenti che cercano un filmato due tipi di risultati. Sul lato sinistro dello schermo compaiono i risultati "naturali" della ricerca, cioè i link verso i filmati più rilevanti rispetto all'interrogazione dell'utilizzatore (secondo gli algoritmi del motore di ricerca di Google). Sul lato destro, invece, vengono mostrati link (accompagnati da brevi commenti) di natura pubblicitaria, che rinviano a messaggi pubblicitari o a siti commerciali. Ad esempio, se si effettua una ricerca su YouTube (o Google-Videos) usando la parola "Beatles", a sinistra si trovano link a filmati di canzoni dei Beatles disponibili su YouTube, mentre a destra si trovano link a spettacoli televisivi, a siti dove acquistare film o dischi dei Beatles, ma anche giochi per computer e profumi. Allo stesso modo, se si utilizza invece il termine "Glassworks" (lavori in vetro), al fine di trovare filmati o musiche riguardanti le composizioni di Philip Glass così denominate, si troveranno sul lato sinistro filmati di diversi artisti che eseguono pezzi tratti da Glassworks (con la possibilità di acquisto da negozi on-line, cliccando sull'apposito bottone), mentre a destra si vedranno link che puntano a produttori o venditori di vetri isolanti, ceramiche in vetro, vetri artigianali e artistici, ecc. Similmente, se si usa il termine di ricerca "studente", si rinverranno a sinistra link verso diversi filmati su studenti, per la maggior parte prodotti da studenti (studente divertente, studente sexy, studente arrestato in classe, ecc.) mentre a destra si troveranno link verso corsi universitari, master, offerte di lavoro, e altri prodotti potenzialmente interessanti per gli studenti.

Questi risultati si spiegano considerando che gli imprenditori interessati ad una pubblicità mirata possono acquistare AdWord (parole per la pubblicità) da Google. Ciò significa che essi possono indicare le parole il cui utilizzo nella ricerca attiverà la visualizzazione (a destra dello schermo) dei loro link pubblicitari e l'ammontare che sono disposti a pagare ogni qualvolta un utente clicchi su tali link. In questo modo gli inserzionisti partecipano ad un'asta che determina se il loro link sarà visualizzato, e in quale posizione (chi offre di più otterrà una posizione più elevata nella lista dei link pubblicitari). La posizione del link non è però determinata solo dall'asta, ma anche dalla qualità del messaggio pubblicitario ad esso collegato, misurata da Google sulla base di un insieme di fattori (quante volte il link è utilizzato, la rilevanza dei contenuti collegati al link rispetto all'AdWord acquistata, la qualità delle pagine collegate, ecc.).

Quindi, nel fornire il servizio Google-Videos (ora YouTube) Google è motivata dalla ricerca del profitto, ma il profitto è il risultato di attività condotte dagli utenti, attività che la piattaforma di Google abilita o facilita: grazie al libero accesso alla piattaforma alcuni utenti (solitamente non commerciali) godono della possibilità di pubblicare di materiali on-line, altri della possibilità di scaricare quei materiali, altri infine (commerciali) della possibilità di farsi pubblicità.

È vero, Google trae vantaggio da tali attività, ma ci dobbiamo chiedere se ciò è sufficiente affinché essa sia responsabile per le conseguenze negative di tali attività (ad esempio, diffamazione, violazione del copyright, violazione della protezione dei dati). Un celebre motto giuridico afferma che "cuius commoda eius et incommoda" − chi gode dei vantaggi di un'attività dovrebbe anche sostenere gli svantaggi da essa causati. Seguendo questa idea si potrebbe sostenere, con il giudice Magi, che poiché Google trae profitto dalle attività che essa abilita mediante la propria piattaforma, essa dovrebbe farsi carico delle perdite (delle "esternalità negative") subite da terzi a causa di tali attività, e eventualmente essere soggetta a responsabilità penale quando tali attività fossero penalmente rilevanti.

4.1. Quali "commoda" e quali "incommoda"?

Dobbiamo tuttavia adottare una più ampia visione dei vantaggi e degli svantaggi collegati all'uso di una piattaforma come Google-Videos, una visione che prenda in considerazione le opportunità individuali così come gli effetti sociali.

Il contesto è quello del cosiddetto Web 2.0, cioè dei recenti sviluppi della rete caratterizzati dalla crescente importanza dei contenuti prodotti dagli utenti (user-generated contents). In questo contesto il Web non è solo l'infrastruttura mediante la quale possiamo comunicare, svolgere attività economiche ed amministrative, accedere a contenuti culturali. Il Web è divenuto il luogo nel quale le persone possono esprimersi, costruire le proprie immagini pubbliche, interagire con amici e conoscenti, produrre informazione e conoscenza, partecipare alla cultura e contribuire al dibattito sociale e politico. Ciò si realizza mediante diverse infrastrutture e strumenti software, che abilitano le nuove dimensioni del Web: condividere contenuti (testi, fotografie, filmati, musica), realizzare blog,

commentare contenuti altri, produrre contenuti intellettuali in modo cooperativo, entrare in reti sociali, ecc.

È vero, era possibile caricare contenuti in rete e renderli pubblicamente accessibili già prima dell'avvento del Web 2.0. Fin dai suoi inizi l'Internet consentiva la condivisione di file (file-sharing) e la creazione di gruppi di discussione (basati sulla condivisione di e-mail). Tuttavia le piattaforme del Web 2.0 rappresentano un importante progresso: in combinazione con l'accresciuta efficacia e la più ampia disponibilità degli strumenti informatici per la creatività individuale e per la produzione cooperativa, queste piattaforme hanno enormemente facilitato la partecipazione attiva dei loro utenti. Grazie a tali piattaforme centinaia di milioni di dilettanti (e professionisti) partecipano alla produzione di notizie, software, lavori letterari, fotografie, filmati, ecc. (23). Ciò avviene affidando alla folla degli utenti (crowdsourcing) la produzione di raccolte di contenuti accessibili sul Web (YouTube, Google-Videos, Flickr, Twitter, MySpace, Facebook, ecc.): tali raccolte (e le loro sezioni) uniscono i contributi separati di tanti individui in opere collettive il cui valore d'uso supera largamente il valore dei contributi individuali che tali opere collettive contengono. Sforzi cooperativi più consapevoli caratterizzano i progetti per la produzione di software a sorgente aperta (open source: Linux, Firefox, OpenOffice, distribuzioni Tex and Latex, ecc.), o di opere intellettuali condivise (Wikipedia). Inoltre, le iniziative diffuse, molteplici e diversificate degli utenti del Web si combinano con l'emergere di funzioni tese a filtrare e organizzare l'informazione prodotta, aggregando le scelte dei singoli in risultati che possano essere rilevanti per altri: i blog si organizzano in raggruppamenti (cluster) intorno a centri (hub) significativi, le preferenze individuali vengono aggregate in valutazioni di reputazione, le reazioni degli utenti ai messaggi indesiderati (spam) contribuiscono ai sistemi di filtraggio, i link alle pagine web vengono aggregati in indici di rilevanza (come nel motore di ricerca di Google, che considera più rilevanti le pagine riceventi più collegamenti) (24). Tim O' Really (che ha contribuito a dare il significato oggi in uso al termine "Web 2.0") ha osservato che il Web 2.0 consiste nello sfruttare l'intelligenza collettiva, cioè nel gestire, comprendere, e rispondere a, enormi quantità di dati prodotti dagli utenti (25). Secondo alcuni autori sta emergendo una nuova forma di produzione, la produzione paritetica di contenuti (peer-production of content), che può superare alcune limitazioni delle presenti forme organizzative per le attività economiche (il mercato e l'impresa), favorendo lo sviluppo umano e la cooperazione (26).

In questo contesto, le imprese del Web svolgono un ruolo decisivo: esse operano a scopo di profitto, ma offrono agli individui la possibilità di contribuire alla comunicazione e alla conoscenza, e forniscono informazioni ottenute aggregando i contributi degli stessi individui. Mentre di regola l'impiego della piattaforma è concesso gratuitamente, alcune attività connesse generano reddito: la pubblicità sui siti è fornita a fronte di un corrispettivo da parte degli inserzionisti, le informazioni aggregate risultanti dalle scelte individuali possono essere fornite a pagamento (ad esempio, dati aggregati sulle preferenze dei consumato-

ri, estratti dal comportamento on-line degli stessi, possono essere venduti alle imprese interessate). Di solito gli utenti mettono a disposizione gratuitamente i loro contenuti (senza percepire corrispettivi dal gestore della piattaforma), benché in alcuni casi possa essere fornita una ricompensa agli utenti per partecipare a una raccolta di informazioni o per svolgere lavoro non qualificato.

In questo modo la creatività individuale, motivata dai più diversi interessi, spesso non ispirata da obiettivi commerciali, si combina con l'attività delle società commerciali del Web (Web-companies), tesa al profitto. Questa attività è chiaramente rivolta all'interesse particolare di tali società, ma può tuttavia essere neutrale, nel senso di essere orientata ad abilitare e facilitare l'azione degli utenti (ad esempio fornendo loro l'opportunità di esprimere il proprio pensiero o la propria creatività, di presentarsi al pubblico, di partecipare ad attività commerciali, ecc.) e a fornire informazioni agli utenti stessi, organizzando e aggregando i materiali forniti da questi (ad esempio, costruendo indici di reputazione sugli operatori commerciali del web, o indici di rilevanza per i siti web).

Pertanto l'attività rivolta al profitto dei fornitori delle piattaforme realizza strumenti per la creatività individuale e organizza l'informazione fornita dagli individui in modo che essa divenga conoscenza sociale, sulla base della quale ulteriori servizi possono essere offerti agli individui o alle entità commerciali. Quando la "generatività di Internet" (27) opera nel modo migliore, i contributi individuali sono agevolati da operatori commerciali che competono per attirare gli utenti offrendo loro un più ampio spettro di scelte ed opportunità per la creatività individuale, così come l'accesso a informazioni di interesse. Pertanto può attuarsi un'utile sinergia: gli individui generano una crescente quantità di contenti, e gli operatori commerciali generano migliori servizi per accogliere e aggregare quei contenuti. In questo modo i bisogni individuali, così come i diritti degli individui (libertà di manifestazione del pensiero, di espressione, comunicazione, partecipazione alla cultura) possono realizzarsi in un'economia capace di sostenersi e svilupparsi in un quadro di auto-organizzazione e autoregolamentazione.

4.2. Il problema della responsabilità del provider.

Ovviamente le cose non procedono sempre nel modo idilliaco sopra considerato. Gli operatori commerciali possono adottare iniziative che violano gli interessi (e i diritti) dei loro utenti. In particolare, essi possono violare la disciplina della protezione dei dati raccogliendo o trasmettendo informazioni personali senza il consenso degli utenti, o comunque al di là dei limiti stabiliti dalla legge. Come abbiamo sopra osservato la questione dell'applicazione della disciplina europea sulla protezione dei dati alle informazioni raccolte nell'Unione, ma trattate al di fuori di essa, richiede una chiarificazione da parte delle autorità competenti e del loro coordinamento europeo (Gruppo di lavoro ex articolo 29). Se si applicasse la disciplina europea sulla protezione dei dati, i provider dovrebbero essere responsabili per tutte le violazioni, civili o penali, da essi commesse trattando illegalmente i dati personali degli utenti. Il caso che abbiamo qui con-

siderato, tuttavia, riguarda una questione diversa, cioè la responsabilità dei provider per il trattamento illecito di informazioni su terzi, fornite dai loro utenti.

Come abbiamo visto, il giudice Magi, pur considerando i dirigenti di Google penalmente responsabili per non avere adottato le precauzioni necessarie e in particolare per non aver informato gli autori del filmato circa le loro responsabilità giuridiche, afferma che la legge non potrebbe richiedere ai provider di controllare individualmente ogni contenuto caricato sulla piattaforma: ciò sarebbe impossibile e quindi inesigibile. A nostro parere, è vero che controllare ogni contenuto prima che sia caricato sarebbe estremamente costoso (se tale controllo fosse affidato ad operatore umano), ma tale controllo non sarebbe in linea di principio impossibile, ed esistono tecniche che consentirebbero un controllo automatico pervasivo (anche se non infallibile). Pertanto la supposta "impossibilità di controllare" non spiega adeguatamente l'esenzione dei provider dalla responsabilità per i contenuti prodotti dagli utenti. La ragione dell'esenzione risiede invece nei diritti e negli interessi collettivi ulteriormente implicati nell'uso delle piattaforme on-line: i diritti di libertà degli interessati e i vantaggi sociali che risultano dal libero esercizio di tali diritti. Come si è spesso osservato, stabilire la responsabilità del provider per i contenuti prodotti dagli utenti presuppone che il provider sia autorizzato ad esercitare controlli atti a prevenire la sua responsabilità, cioè, che gli sia conferito il potere di escludere tutti i contenuti la cui pubblicazione potrebbe renderlo responsabile. Il provider diventerebbe allora il guardiano dell'ingresso (gate-keeper) di Internet, ed eserciterebbe un controllo preventivo sulla pubblicazione dei contenuti generati dagli utenti. Di conseguenza, ogni informazione potenzialmente controversa sarebbe probabilmente impedita dall'ottenere la visibilità pubblica. In particolare ogni informazione relativa a terzi sarebbe bloccata preventivamente dal provider, per timore di incorrere in incriminazioni o azioni di responsabilità civile per violazione della disciplina della protezione dei dati (o della proprietà intellettuale). La libertà degli utenti di esprimere le proprie opinione e di partecipare nella creazione della cultura soffrirebbe inaccettabili limitazioni e inoltre si comprometterebbe la "generatività" di Internet (28).

Come abbiamo sopra osservato, il diritto dell'Unione Europea (come il diritto statunitense) ha trovato un ragionevole bilanciamento tra le libertà di Internet e la protezione dei terzi, mediante un sistema a due livelli: i fornitori delle piattaforme sono esonerati dalla responsabilità per i contenuti illegali generati dagli utenti, ma questa esenzione non si applica se il provider non si è attivato dopo essere stato informato dell'illegalità dei contenuti. Si è autorevolmente sostenuto che questo modello dovrebbe trovare applicazione anche alla protezione dei dati, al fine di bilanciare la privacy e la libertà di espressione (29). In Europa si possono avere però dei dubbi sull'applicabilità di questo modello alla protezione dei dati, poiché la Direttiva sul commercio elettronico esclude espressamente (art. 1, comma 5, b) l'ambito della protezione dei dati dalle esenzioni di responsabilità previste per i provider.

A nostro parere questi dubbi possono essere risolti coordinando in via interpretativa, protezione dei dati e disciplina della responsabilità. I fornitori di piattaforme dovrebbero essere pienamente responsabili (senza alcuna esenzione) quando elaborano dati personali sugli utenti che essi hanno richiesto agli utenti stessi o hanno estratto dall'attività on-line di quelli (questi dati dovrebbero essere soggetti a tutte le norme sulla protezione dei dati); al contrario, i provider dovrebbero essere esonerati da responsabilità quando elaborino contenuti caricati dagli utenti e contenenti informazioni su terzi. I provider che indicizzano e rendono disponibili contenuti prodotti e caricati dagli utenti non svolgono infatti il ruolo di titolari del trattamento; essi sono meri responsabili che eseguono le richieste degli utenti (solo questo dovrebbe infatti essere il ruolo fisiologico dell'host provider rispettoso delle scelte dell'utente). Peraltro, in assenza di chiare indicazioni legislative, riteniamo sarebbe opportuno che le autorità competenti rimovessero le presenti incertezze circa l'applicazione della disciplina della protezione dei dati ai provider, sperabilmente seguendo l'indirizzo liberale appena tratteggiato in via interpretativa.

Il diritto italiano mostra una particolare attenzione per l'esigenza di prevenire la censura preventiva da parte dei provider: migliorando la disciplina prevista dalla direttiva europea (che richiede che i provider rimuovano i contenuti illegittimi di cui sono a conoscenza), la legge italiana stabilisce che l'esenzione dalla responsabilità è inapplicabile solo quando il provider abbia omesso di rimuovere i contenuti illegittimi dopo esserne stato richiesto da un'autorità giudiziaria o amministrativa, o non abbia informato una tale autorità dopo aver essere venuto a conoscenza di presunte informazioni illecite (30). Questa disciplina affidata alla competente autorità giudiziaria o amministrativa il compito di stabilire se si debba rimuovere un contenuto ritenuto illegittimo. Quindi il provider è liberato non solo dalla necessità di controllare ogni contenuto caricato sulla piattaforma, ma anche dalla necessità di effettuare difficili ed incerte valutazioni giuridiche per stabilire l'illiceità di particolari contenuti, valutazioni che possono richiedere il bilanciamento di diritti fondamentali.

Nel caso presente, Google ha rispettato la disciplina sulla responsabilità degli host provider, provvedendo a rimuovere il filmato appena richiestane da parte della Polizia Postale italiana. Inoltre ha adempiuto alle richieste della polizia fornendo le informazioni che hanno consentito di identificare gli studenti autori del video, e di condannarli per i reati da essi commessi (maltrattamenti e ingiurie).

Infine il fatto che un provider operi a fini di profitto non esclude l'applicabilità dell'esenzione dalla responsabilità, qualora il profitto risulti dall'abilitare e facilitare l'attività degli utenti. Ciò è stato affermato con chiarezza nella sentenza della Corte di Giustizia dell'Unione Europea sopra menzionata (31), secondo la quale l'esenzione per gli host-provider si applica anche quando il provider mostra link pubblicitari a pagamento, a condizione che il contenuto della pubblicità sia stabilito dall'utente stesso. Invece l'esenzione non si applica ai provider la cui azione vada al di là della "funzione naturale" della piattafor-

ma, cioè, al di là della funzione di abilitare e facilitare le attività degli utenti (pubblicare contenuti, ricercare materiali, o anche farsi pubblicità): i provider sono responsabili quando producono i contenuti o rivolgono il funzionamento della piattaforma verso il proprio interesse immediato (a scapito dell'utente). Finché il profitto del provider si ottiene potenziando le capacità dell'utente, non c'è conflitto tra ricerca del profitto ed esenzione da responsabilità.

5. Conclusione.

Ci sembra che la decisione del giudice Magi sia criticabile sotto diversi aspetti.

Innanzitutto, non approfondisce adeguatamente alcuni presupposti fondamentali della responsabilità penale, e in particolare, l'applicabilità della legge italiana e la presenza dell'elemento psicologico caratterizzante il reato.

In un secondo luogo, non fornisce una precisa analisi del perché l'omessa comunicazione agli utenti-caricatori dei loro obblighi attinenti alla protezione dei dati possa qualificarsi come mancata informativa ai sensi della disciplina della privacy (l'informativa dovendo riguardare gli scopi del trattamento e i diritti di controllo).

In terzo luogo, non coglie il ruolo dei fornitori di piattaforme nel contesto del Web 2.0, ed in particolare la loro funzione abilitante e facilitatrice rispetto alla produzione di contenuti da parte degli utenti.

In conclusione, contro la tesi esposta da giudice Magi, a noi sembra che le limitazioni della responsabilità previste per gli host provider dovrebbero applicarsi anche al trattamento di dati personali contenuti nei materiali prodotti e caricati dagli utenti su piattaforme on-line. Tali limitazioni, come disciplinate dal decreto sul commercio elettronico, forniscono un bilanciamento adeguato anche degli interessi e dei diritti qui considerati. Queste considerazioni non escludono che i provider abbiano il dovere di adottare iniziative volte ad educare gli utenti circa la protezione dei dati. In particolare, i provider dovrebbero essere indotti (anche mediante appropriati provvedimenti del Garante) a fornire ai loro utenti migliori informazioni sull'esigenza di rispettare i diritti dei terzi, come suggerito dal Gruppo di lavoro ex articolo 29. Pensiamo che l'obbligo di adottare tali iniziative sarebbe compatibile la ratio dei limiti della responsabilità degli host provider, perché il suo adempimento non comporterebbe l'imposizione di alcuna censura sugli utenti, ma si limiterebbe a renderli consapevoli dei loro preesistenti doveri inerenti alla protezione dei dati.

NOTE

(1) Google-Videos è un servizio fornito da Google Inc., la celebre impresa statunitense che ha ottenuto un enorme successo grazie alla realizzazione del motore di ricerca Google, utilizzato dalla grande maggioranza dei navigatori di Internet (circa il 70% delle ricerche on-line fanno uso di Google). Tale motore di ricerca è stato affiancato da numerosi altri servizi come la posta elettronica G-Mail, le indicazioni geografiche e gli indirizzi di Google-Maps, le immagini geografiche di Google-Earth, il notiziario Google-News, i testi di Google-Books e Google-Scholar, la piattaforma per foto Picasa, la

gestione di documenti Google-Docs e tante altre funzioni disponibili su Internet. Tali servizi sono forniti gratuitamente all'utilizzatore, poiché i proventi di Google derivano in gran parte dalla pubblicità: quando gli utenti accedono ai servizi, essi ricevono messaggi pubblicitari pagati dagli inserzionisti. Il servizio Google-Videos, il cui impiego è al centro del caso qui esaminato, era stato offerto da Google nel 2005, quale piattaforma per il caricamento on-line e la distribuzione di filmati. Nel 2006 Google acquistava YouTube, il sito web più popolare per la condivisione di filmati on-line. In seguito all'acquisto di YouTube, Google-Videos veniva ad assumere la funzione prevalente di motore di ricerca per filmati, perdendo, a partire dal 2009, le funzionalità attinenti al caricamento e alla distribuzione dei filmati, affidate a YouTube.

(2) Sentenza n. 1972/2010, Tribunale ordinario di Milano in composizione monocratica. Sezione 4 Penale, p. 102/103. Disponibile oltre che in questa Rivista, retro, p. 474 presso: http://speciali.espresso.repubblica.it//pdf/Motivazioni_sentenza_ Google.pdf.

(3) Sentenza n. 1972/2010, p. 108.

(4) The Official Google Blog. `Serious threat to the web in Italy' (2010). Disponibile presso: http://googleblog.blogspot.com/20 10/02/serious-threat-to-web-in-italy.html.

(5) `Statement by Ambassador David Thorne: Ruling in Google Court Case'. Disponibile presso: http://italy.usembassy.gov/viewer/article.asp?article=/file2010 _02/alia/10022205.htm.

(6) Donadi, `Larger Threat is Seen in Google Case' (2010). The New York Times. Disponibile presso: http://www.nytimes.com/2010/02/25/technology/companies /25google.html.

(7) `Berlusconi e il Governo approvano il decreto per controllare Internet'. Disponibile presso: http://revenews.info/berlusconi-e-il-governo-approvano-il-decreto-per-controllare-internet_post10615.html.

(8) Google investor relation. 2010 Financialtables. Disponibile presso: http://investor.google.com/financial/tables.html.

(9) `Caso Google: la replica della Procura' (2010). L'Espresso. Disponibile presso: 0http://espresso.repubblica.it/dettaglio/Caso-Google-replica-la-Procura/2122058.

(10) "Non esiste, a parere di chi scrive, perlomeno fino ad oggi, un obbligo di legge codificato che imponga agli ISP un controllo preventivo della innumerevole serie di dati che passano ogni secondo nelle maglie dei gestori o proprietari dei siti web, e non appare possibile ricavarlo aliunde superando d'un balzo il divieto di analogia in partem, cardine interpretativo della nostra cultura procedimentale penale". Sentenza n. 1972/2010, p. 103.

(11) Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno).

(12) Disponibile presso: http://www.fcc.gov/Reports/tcom1996.txt.

(13) Un giudice francese ha recentemente sviluppato un'argomentazione simile a quella del giudice Magi in un caso riguardante MySpace (una piattaforma per la distribuzione di contenuti on-line), e ha ritenuto che MySpace non fosse un mero host provider, traendo profitti pubblicitari dai filmati caricati dagli utenti. (T.G.I. Paris [réf.], 22 June 2007). VediStrowel, `Google et les nouveaux services en ligne: quels effets sur l'économie des contenus, quels défis pour la propriété intellectuelle. In Strowel e Triaille (a cura di), Google et les nouveaux services en ligne: impact sur l'économie du contenu et questions de propriété intellectelle (Larcier: Bruxelles 2008), p. 44-45.

(14) Vedi Provvedimento del 3 novembre 2009. Garante per la protezione dei dati personali. Disponibile presso: http://www.garanteprivacy.it/garante/doc.jsp?ID =1687662.

(15) Il Gruppo di lavoro ex articolo 29 è un organo consultivo composto dai rappresentanti di tutte le autorità di protezione dei dati degli stati membri, più un rappresentante della Commissione europea. L'autorità britannica di protezione dei dati ha adottato una posizione simile per quanto riguarda il trattamento dei nomi e, in certa misura, anche delle immagini: "Religion or ethnicity, or both, can often be inferred with varying degrees of certainty from dress or name. For example, many surnames are associated with a particular ethnicity or religion, or both, and may indicate the ethnicity and religion of the individuals concerned. However, it would be absurd to treat all such names as "sensitive personal data", which would mean that to hold such names on customer databases you had to satisfy a condition for processing sensitive personal data. Nevertheless, if you processed such names specifically because they indicated ethnicity or religion, for example to send marketing materials for products and services targeted at individuals of that ethnicity or religion, then you would be processing sensitive personal data" in UK Information Commissioner's Office. `The Guide to Data Protection', p. 24. Disponibile presso: http://www.ico.gov.uk/upload/documents/library/ data_protection/ practical_application/the_guide_to_data_protection).

(16) Gruppo di lavoro ex articolo 29: `Parere 5/2009 sui social network on-line', adottato il 12 giugno 2009, p. 8. Disponibile presso: http://ec.europa.eu/justice_home/ fsj/privacy/docs/wpdocs/2009/wp 163_it.pdf.

(17) Gruppo di lavoro ex articolo 29. `Parere 5/2009 sui social network on-line', adottato il 12 giugno 2009, p. 9. Disponibile presso: http://ec.europa.eu/justice_home/ fsj/privacy/docs/wpdocs/2009/wp163_it.pdf.

(18) Gruppo di lavoro ex articolo 29. `Parere 5/2009 sui social network on-line', adottato il 12 giugno 2009. Disponibile presso: http://ec.europa.eu/justice_home /fsj/privacy/docs/wpdocs/2009/wp 163_it.pdf. p. 7.

(19) Il giudice menziona l'accordo come indizio del danno subito dallo studente disabile (Sentenza n. 1972/2010, p. 91).

(20) Sentenza della Corte Giustizia dell'Unione Europea, 23 marzo del 2010, Casi da C-236/08 a C-238/08, Paragrafo 109, infra in questa Rivista, infra p. 707, con nota di G. Spedicato; nonché. Disponibile presso: http://eur-lex.europa.eu/LexUriServ/LexUri Serv.do?uri= CELEX:62008J0236:EN:HTML.

(21) Disponibile presso: http://curia.europa.eu/jurisp/cgi-bin/gettext.pl? lang=en&num=79909077C19080236& doc=T&ouvert=T&seance=CONCL.

(22) Sulla libertà di espressione vedi per tutti, Zeno-Zenchovich, Freedom of Expression: A Critical and Comparative Analysis (Routledge, London, 2008).

(23) Vedi Lessig, Remix: Making Art and Commerce Thrive in the Hybrid Economy (Penguin Press, 2008).

(24) Sui vari modi in cui l'informazione è fornita ed aggregata, vedi Sunstein, Infotopia: How Many Minds Produce Knowledge (Oxford University Press, Oxford 2006).

(25) O'Reilly, `What Is Web 2.0 Design Patterns and Business Models for the Next Generation of Software'; O'Reilly, 2005, Disponibile presso: http://oreilly.com/web2/ archive/what-is-web-20.html; O'Reilly and Battelle, `Web Squared: Web 2.0 Five Years On'; O'Reilly, 2009, Disponibile presso: http://assets.en.oreilly.com/1/event/28/ web2009_websquared-whitepaper.pdf.

(26) Vedi, in particolare, Benkler, The Wealth of Networks: How Social Production Transforms Markets and Freedoms (Yale University Press: New Haven, Conn. 2006).

(27) Vedi Zittrain, `The Generative Internet' (1994). Harvard Law Review Vol. 119:1974-2006. p. 1993; Zittrain, The Future of the Internet (Yale University Press, New Haven, Conn. 2009).

(28) Per una discussione sulla libertà di espressione/manifestazione del pensiero e la responsabilità dei provider, vedi, BalkinThe Future of Free Expression in a Digital Age (2008). Pepperdine Law Review Vol. 36: 101-18.

(29) Solove, The Future of Reputation (Yale University Press: New Haven, Conn. 2008).

(30) Sulla responsabilità dei ISP secondo la legge italiana, vedi Pagallo, Sul principio di responsabilità giuridica in rete, (2009), in Il Diritto dell'informazione e dell'informatica, Vol 25: 705-34.

(31) Sentenza della Corte Europea di Giustizia 23 marzo del 2010, Casi C-236/08 a C-238/08.

Programmi-filtro e criteri di imputazione/esonero della responsabilità on-line. A proposito della sentenza google/vivi down

di Francesco Di Ciommo (*)

1. Internet, fatti illeciti e programmi-filtro.

Internet, come ormai noto, oltre a rappresentare lo straordinario "nuovo mondo" della comunicazione e dell'informazione ubiqua ed accessibile a tutti, può rappresentare anche l'ambiente − o, se si preferisce, lo strumento − ideale per il compimento di illeciti, contrattuali e non. Ciò dipende da svariate ragioni, che vanno dalla possibilità che la grande rete telematica offre ad ogni utente di diffondere in tempo reale una notizia, o più generalmente un contenuto, potenzialmente in tutto il mondo, senza grandi spese (ed in molti casi, praticamente senza spesa se non quella della connessione), all'anonimato di cui l'utente può fruire in Internet se, mentre naviga, pone in essere precauzioni tecniche minime finalizzate a non rendere percepibile la sua reale identità né agli alti user, né ai fornitori di servizi i cui siti eventualmente visiti o che comunque utilizzi, né tanto meno al suo provider fornitore di accesso.

Gli illeciti più diffusi della rete sono quelli che tipicamente possono essere compiuti, anche nella realtà off-line, attraverso l'uso di dati altrui o comunque attraverso informazioni: e dunque diffamazione, ingiuria, aggressioni al diritto alla privacy, alla riservatezza, al diritto all'identità personale, nonché violazione del diritto d'autore, del segreto industriale e più in generale di altrui privative. A compiere tali illeciti, come si diceva, sono spesso utenti che, celandosi dietro l'anonimato in qualche modo assicurato dalla rete, sfuggono alle responsabilità giuridiche conseguenti al loro operato e spesso sfuggono anche alle inibizioni personali che, altrimenti, potrebbero frenare la condotta socialmente disapprovata. Per entrambe le ragioni Internet rappresenta, o quanto meno può rappresentare, un ambiente adatto a favorire la tenuta di condotte illecite anche da parte di soggetti normalmente poco propensi a comportarsi in modo socialmente o giuridicamente sconveniente.

Quando, attraverso l'utilizzazione di un servizio prestato da un operatore della rete, un utente coperto da anonimato pone in essere un fatto illecito, al fine di non sacrificare le ragioni del danneggiato ci si chiede se esiste un soggetto ulteriore, rispetto al misterioso (e dunque non perseguibile) autore dell'illecito, che possa essere chiamato in giudizio come responsabile. Come vedremo nei prossimi paragrafi, considerata l'assenza di sistemi di assicurazione obbligatoria o di fondi più o meno pubblici destinati a risarcire i malcapitati, questo soggetto è stato sin qui individuato, quanto meno teoricamente, dalla giurisprudenza, sia negli Stati Uniti che in Europa, nella figura del provider, e cioè dell'operatore che fornendo servizi in Internet destinati agli utenti consente loro di pubblicare in rete, o inviare tramite la rete, i materiali o le dichiarazioni che producono il danno (1). Il tentativo pretorio di individuare responsabilità del provider per il-

(*) in *Diritto dell'Informazione e dell'Informatica*, 2010, 829.

leciti commessi dagli utenti di Internet, in vero, non ha riguardato solo casi in cui l'autore materiale del fatto sia rimasto anonimo, giacché si ritiene che, indipendentemente da questa circostanza, senza dubbio rilevante, il provider, in quanto soggetto organizzato che presta servizi nella c.d. società dell'informazione, abbia comunque una posizione tecnica ed economica tale da non potersi ritenere totalmente estraneo alla vicenda dannosa. Non a caso, si parla dei provider anche in termini di "intermediari" della comunicazione online (cfr. la direttiva 2000/31/CEE, su cui torneremo infra).

In particolare, negli scorsi lustri alcuni giudici hanno ritenuto i provider responsabili per non aver posto in essere quanto era nelle loro possibilità al fine di evitare la commissione dell'illecito, ovvero la diffusione degli effetti dannosi dello stesso, in particolare adottando i c.d. programmi filtro. Con tale locuzione si fa riferimento a software in grado di controllare i contenuti dei materiali che gli utenti immettono in rete tramite il servizio reso dal provider, così da consentire la presenza sul Web dei soli contenuti leciti. Le tipologie di programmi filtro che i provider possono utilizzare sono variegate, la loro conformazione ed operatività dipende dal servizio reso e dalla policy di gestione della propria attività decisa dal provider. Quest'ultimo, infatti, può scegliere di controllare in maniera più incisiva i comportamenti dei propri utenti, e di tentare in modo pervicace, per quanto tecnicamente possibile, di prevenire il compimento di illeciti, oppure può − in nome della libertà di espressione che, secondo i più, dovrebbe sempre presidiare la comunicazione telematica, ovvero più prosaicamente al fine di assicurarsi il favore degli utenti − decidere di svolgere un controllo superficiale, a campione, o solo a posteriori (e cioè sui materiali già immessi in rete, al fine, ad esempio, di rimuovere quelli ritenuti sconvenienti), o addirittura può preferire non interferire affatto con il modo in cui gli utenti utilizzano i suoi servizi (2).

La tematica è senz'altro di grande attualità in quanto non vi è dubbio che i provider rappresentano attualmente gli unici soggetti che potrebbero, nei limiti delle loro capacità tecniche, evitare − o quanto meno limitare − l'utilizzazione illecita di Internet, sicché l'esistenza, o meno, in capo ad essi di un obbligo giuridico di prevenzione può concretamente e significativamente modificare la stessa morfologia del mondo virtuale (3).

Sul punto il dibattito, non solo in Italia, è stato recentemente animato dalla sentenza n. 1972/2010 del 22 febbraio 2010-12 aprile 2010, con la quale il Tribunale Penale di Milano ha mandato assolti da responsabilità i vertici di Google Italy s.r.l. dall'accusa di aver offeso la reputazione dell'Associazione "Vivi Down" (per la ricerca scientifica e la tutela delle persone down) e di un ragazzo down protagonista, suo malgrado, della turpe vicenda, "consentendo che venisse immesso per la successiva diffusione a mezzo Internet, attraverso le pagine del sito http://video.google.it e senza alcun controllo preventivo sul suo contenuto, un filmato in cui persone minorenni, in concorso tra loro, pronunciando la seguente frase "Salve, siamo dell'associazioni Vivi down, un nostro mongolo si è cagato addosso [...]" e ponendo in essere numerosi altri atti vessatori nei con-

fronti di un loro coetaneo disabile, ledevano i diritti e le libertà fondamentali nonché la dignità degli interessati".

Pare utile approfondire la riflessione nei termini che seguono.

2. La recente sentenza del Tribunale Penale di Milano: troppo rumore per nulla.

"Troppo rumore per nulla". Con questa, fin troppo nota, citazione letteraria si chiude la citata recente sentenza del Tribunale penale di Milano, laddove con essa il Giudice ha inteso evidenziare che il clamore mediatico suscitato dal processo in questione sarebbe stato, a suo avviso, eccessivo ed ingiustificato posto che la sentenza avrebbe finito per applicare principi già affermati nella giurisprudenza italiana. Ed in effetti, con tutta probabilità, di troppo rumore per nulla si è trattato.

La elaborata sentenza del Tribunale di Milano, infatti, dopo aver a lungo disquisito di qualificazione di Google come "host" (più o meno attivo) o "content" provider, e di esistenza o meno in capo a Google, ed in generale ai provider rientranti nell'una o nell'altra categoria, di un obbligo di controllo preventivo sui contenuti di Internet, e dopo aver evidenziato che Google nel caso di specie non ha svolto i controlli preventivi all'epoca possibili − i quali avrebbero peraltro, nel caso di specie, evitato il compimento dell'illecito (giacché, come subito appresso si chiarirà, bastava un mero controllo lessicale sul titolo del video ad evidenziarne la natura illecita) − finisce per affermare il principio per cui non si può chiedere al provider di controllare tutto ciò che transita in Internet in quanto un controllo realmente efficace su tutti i materiali veicolati in rete non è tecnicamente possibile. Di conseguenza, non si può condannare un provider per concorso omissivo nel reato compiuto dall'utente, il quale ha dato impulso all'immissione in rete del materiale da cui è derivata la lesione del bene giuridico protetto, per il sol fatto di aver omesso di svolgere controlli preventivi sul materiale che veicola in Internet su richiesta dell'utente.

Dunque, realmente: molto rumore per nulla. Google e gli altri provider italiani e mondiali, sotto il profilo che più sta loro a cuore, che per l'appunto è quello dell'esistenza (o meno) di un obbligo di controllo preventivo dei contenuti, possono dormire sonni tranquilli.

Eppure, nella motivazione della sentenza, a proposito della possibilità/opportunità per Google di utilizzare i c.d. programmi-filtro, o comunque di svolgere un controllo preventivo sui contenuti trattati per conto degli utenti, si leggono valutazioni di tenore diverso.

Vero è, infatti, che i programmi-filtro in grado di trasformare il sonoro del video in testo, e di analizzare automaticamente tale testo attraverso un controllo per classi semantiche, non consentivano nel 2006, così come non consentono oggi, l'individuazione di tutte le casistiche di video illeciti, in quanto è evidente che anche attraverso parole apparentemente innocue possono pronunciarsi dichiarazioni ingiuriose, diffamatorie e quant'altro, così come è ben possibile che il sonoro del video non sia nitido e quindi non sia idoneo ad essere trasferito dal

software in testo, ed ancora può accadere che l'illiceità del video non dipende dalle parole che in esso vengono pronunciate ma dalle scene riprese. Tuttavia, nella stessa sentenza si legge che il perito del Giudice aveva sottolineato come, ciò nonostante, l'utilizzazione di programmi-filtro possa rappresentare un valido "compromesso tra un controllo diretto su tutti i video e il debole controllo sociale lasciato agli utenti della community".

Inoltre, come detto, è la stessa sentenza ad evidenziare come Google nel caso di specie non abbia posto in essere nemmeno il controllo lessicale sul titolo del video, controllo che sarebbe stato tecnicamente possibile e funzionalmente sufficiente ad evidenziare l'illiceità dello stesso considerato il titolo evidentemente volgare ed offensivo dal video in questione. Al riguardo, il Tribunale ha addirittura accertato in sentenza che tale controllo lessicale non è stato realizzato dal provider perché la quasi totalità dei dipendenti erano impiegati per altre mansioni che potevano far conseguire introiti e vantaggi alla sua attività di impresa (ad esempio, per la scansione dei testi di "Google books").

Sennonché, malgrado la corposa motivazione e le valutazioni espresse all'esito della complessa istruttoria, il Tribunale di Milano − come detto − perviene alla conclusione che il provider non ha concorso nel reato commesso dagli autori del filmato. Ma se questo è lo stato dell'arte sul versante penalistico, laddove il principio di tipicità dei fatti costituenti reato e quello di favor rei impongono al giudice la massima prudenza nel valutare la sussumibilità della condotta nella fattispecie di retato codificata, siamo così sicuri che lo stesso è a dirsi sul versante civilistico, nel quale, in mancanza di indici normativi più precisi, è il parametro della correttezza a distinguere i comportamenti e (le omissioni) leciti da quelli illeciti? In altre parole, siamo così sicuri che i provider non abbiano un obbligo di controllo preventivo la cui violazione, pur non configurando allo stato un reato, configura un illecito civile produttivo di responsabilità civile?

La sensazione è che, fuori da ogni suggestione, anche sul versante civilistico allo stato sia alquanto difficile configurare l'esistenza di un siffatto obbligo giuridico in capo ai provider, in quanto addirittura il D.Lgs. 70/2003 − che, come vedremo più avanti, reca le norme speciali applicabili in materia − e prima ancora la direttiva comunitaria che dal decreto è stata recepita (2000/31/CE), stabiliscono a chiare lettere che il provider che svolga una selezione dei contenuti risponde dei danni cagionati da tali contenuti, laddove, al contrario, se lo stesso si astiene da qualunque selezione non risponde di alcunché. In altre parole, i criteri di imputazione della responsabilità per fatti illeciti commessi on-line adottati dal D.Lgs. 70/2003 creano un sistema basato su una sorta di "immunità condizionata" dei provider. E cioè: i provider non sono responsabili a patto che rispettino le condizioni espressamente individuate dal citato decreto agli artt. 14 (Responsabilità per attività di mero trasporto), 15 (Responsabilità per l'attività di memorizzazione temporanea) e 16 (Responsabilità per l'attività di memorizzazione), sui quali ci soffermeremo tra breve.

Dunque, addirittura, le poche norme di derivazione legislativa che operano nella materia in esame sembrano voler scoraggiare i provider dall'adottare si-

stemi di filtraggio dei contenuti o comunque di controllo preventivo. Ed in proposito, giova inoltre ricordare che l'art. 17 del D.Lgs. 70/2003 è persino rubricato "Assenza dell'obbligo generale di sorveglianza".

Il sistema voluto dal legislatore europeo, che sostanzialmente − come a breve si vedrà − riproduce l'approccio nordamericano al tema dato con il Digital Millennium Copyright Act del 1998, è volto ad evitare che un aggravamento delle responsabilità, e dunque dei costi, dei provider possa rendere meno plurale e libera la comunicazione in Internet, ma anche a non penalizzare i provider europei rispetto ai concorrenti extracomunitari. Tale sistema, razionale sotto il profilo appena indicato, appare tuttavia inefficiente sotto un diverso profilo. Ed infatti, dato l'assetto normativo appena richiamato, quale provider europeo si doterà di un sistema di filtraggio o controllo preventivo, ben sapendo che al momento tali sistemi hanno un elevato grado di fallibilità, e soprattutto ben consapevole che il tentativo di limitare il rischio comporterà per lui imputazione di responsabilità nel caso in cui i sinistri si verifichino? È evidente come un sistema di tal fatta induce i provider a non dotarsi di alcun controllo preventivo, ed inoltre induce gli stessi a non investire nulla in sviluppo di filtri sicuri. Di talché, la domanda che bisogna porsi è se sia davvero questo il migliore dei mondi possibili. O, in altri termini, se siamo realmente sicuri di volere che gli intermediari della comunicazione su Internet consentano a chiunque di dire, fare e pubblicare qualsiasi cosa, anche restando anonimi, senza avere alcuna responsabilità circa i contenuti che essi veicolano on-line, e dunque senza avere nemmeno l'obbligo di evitare ciò che tecnicamente è evitabile.

Ed ancora, una volta che si sia eventualmente risposto in termini positivi a tali quesiti, occorrerebbe per coerenza domandarsi altresì perché ciò che vale riguardo ad Internet non dovrebbe valere anche, ad esempio, per i giornali e l'editoria tradizionale. Perché, in altre parole, un editore dovrebbe rispondere per l'illecito commesso da un giornalista che firma un pezzo pubblicato sul giornale ed un provider di Internet no, si badi bene a parità di scopo di profitto. A tali dubbi potrebbe rispondersi osservando che l'editore costituisce la tasca profonda in grado di risarcire il malcapitato effettivamente, al contrario o comunque a prescindere da quanto potrebbe fare il giornalista. Ma un analogo profilo non sussiste anche per gli illeciti commessi on-line? Anzi qui con un aggravante, e cioè che spesso, molto spesso, on-line l'autore dell'illecito, e cioè colui che immette in rete il contenuto dannoso, resta anonimo.

Per provare a formulare qualche risposta rispetto ai quesiti cennati e ad avanzare qualche proposta de iure condendo, giova svolgere alcune considerazioni circa le ragioni storiche e giuseconomiche che, alla fine degli anni Novante del secolo scorso, hanno determinato il legislatore nordamericano, seguito a ruota da quello europeo, a disciplinare l'attività dei provider nei termini appena sintetizzati.

3. Responsabilità dei provider per illecito degli utenti tra rischio di impresa e attività pericolosa.

I provider svolgono, per lo più, la propria attività in maniera organizzata e con fine di lucro. Per tale ragione, quando i primi illeciti compiuti via Internet da utenti rimasti anonimi vennero portati nelle aule dei tribunali, i provider furono visti come la "tasca" (se non proprio profonda, quantomeno) sicura a cui fare riferimento per garantire una tutela risarcitoria certa ai soggetti danneggiati da illeciti compiuti on-line in forma anonima (4). Inoltre, almeno nei primi anni Novanta, i giudici credevano di poter, in tal modo, incidere sulle misure preventive adottate dai provider. In altre parole, essi, affermando la responsabilità dei prestatori di servizi senza svolgere alcuna indagine circa la sussistenza di una colpa effettiva a questi rimproverabile, reputavano di poter indurre tali soggetti a minimizzare i rischi a proprio carico verificando preventivamente la liceità dei contenuti che gli utenti desideravano pubblicare in Internet, attraverso l'utilizzazione di programmi-filtro automatici o altre tecniche di controllo.

In breve può dirsi che, in una prima fase, la responsabilità civile dei prestatori di servizi di rete per illeciti compiuti dagli utenti sia stata notevolmente influenzata dalla teoria del rischio di impresa, a tenore della quale il soggetto che ottiene un vantaggio patrimoniale dall'esercizio di una certa attività deve farsi carico in senso oggettivo, e dunque indipendentemente dalla sua eventuale colpa rispetto al compimento dei singoli illeciti, dei costi sociali che essa inevitabilmente crea (5).

Tuttavia, pur condividendo l'esigenza di applicare ai provider un regime di responsabilità oggettiva − o, quanto meno, un regime basato sull'inversione dell'onere della prova circa l'elemento soggettivo e cioè circa la colpa del convenuto (c.d. responsabilità semi-oggettiva) −, alcuni autori, soprattutto nordamericani, evidenziarono le difficoltà concettuali insite nel tentativo di giustificare tale scelta di politica del diritto sulla base della mera teoria del rischio di impresa, in particolare mettendo in rilievo l'impossibilità, da parte del prestatore, di svolgere un effettivo controllo sulla liceità dei contenuti scaricati in rete dagli utenti attraverso l'utilizzazione di programmi-filtro o, più ancora, attraverso l'applicazione di persone fisiche incaricate di sorvegliare tutto ciò che avviene on-line.

Si provò, allora, a battere una strada parzialmente diversa sostenendo la dottrina della c.d. vicarious liability, in base alla quale risponde dell'illecito chi, avendo il diritto e la possibilità concreta di controllare le azioni dell'autore del fatto, omette di impedire il verificarsi dell'evento lesivo e ne trae profitto. Ovviamente, per questa via si cercò di valorizzare comportamenti attivi da parte dei provider finalizzati a tentare di prevenire l'illecito, fino al punto di esonerare il provider quando fosse in grado di provare di aver fatto quanto nelle sue possibilità per evitare che l'illecito si compisse (6). A ben vedere, però, anche il riferimento a tal ultima tesi non si sottrae a severe critiche ed appare, in definitiva, ingiustificato. L'istituto, infatti, tradizionalmente trova per lo più applicazione in caso di responsabilità del datore di lavoro per fatto illecito perpetrato da un dipendente nell'esercizio della attività a cui è preposto, ovvero in caso di responsabilità di genitori, maestri, docenti e tutori per illeciti commessi da mi-

nori o da persone incapaci d'agire. Tra prestatore e navigatori non si crea alcun rapporto di preposizione, né può dirsi che il primo ha un potere di scelta o di controllo sul comportamento dei secondi, ovvero che egli trae direttamente un'utilità economica dall'attività illecita compiuta in rete dall'utente; circostanze queste ultime che escludono si possa parlare, a suo carico, di una vera e propria vicarious liability(7).

Un'altra strada che si pensò di poter seguire, al fine di giustificare l'applicazione di un regime di responsabilità semi-oggettiva a carico dei provider, giunge a configurare il sito o il servizio, messi on-line a disposizione degli utenti, come una "cosa in custodia" del prestatore (cfr. art. 2051 c.c.). Anche tale tentativo, tuttavia, si rivelò privo delle necessarie fondamenta concettuali. Ciò in quanto il presupposto per l'applicazione dei principi operanti in materia di responsabilità per danno provocato da cose in custodia è costituito dalla disponibilità materiale e dal potere di controllo che il soggetto, a cui si vuole imputare il danno in qualità di custode, ha sulla cosa stessa; sennonché, come meglio si vedrà infra, i prestatori di servizi di Internet non hanno la possibilità di controllare in modo pienamente efficace l'utilizzazione che gli utenti fanno della rete e dei servizi on line, sicché, per qualificare il loro rapporto con le "cose" in parola, pare alquanto problematico il riferimento al concetto di "custodia". Del resto, a rigore, anche il riferimento al concetto di cose dovrebbe essere precluso nel caso di specie in quanto qui si tratta, per l'appunto, di "servizi", e non di "cose". Inoltre, a ben vedere, nella situazione in esame non è la risorsa messa a disposizione dei navigatori che produce il danno, bensì l'uso che della stessa vien fatto dagli utenti; considerazione quest'ultima, in ragione della quale può ben dirsi che il servizio predisposto dal prestatore non "cagiona il danno", bensì rappresenta soltanto il mezzo attraverso il quale esso viene arrecato.

Una configurazione ulteriore della responsabilità del prestatore di servi di rete per danno cagionato da un utente rimasto anonimo potrebbe, in astratto, far capo al concetto di attività pericolosa. In altre parole, e con particolare riferimento ad Internet, si è sostenuto che sia da considerarsi intrinsecamente pericolosa l'attività svolta dai provider che prestano servizi in favore di utenti la cui identità resta coperta dall'anonimato e ospitano materiali altrui sui propri siti o, addirittura, siti altrui sui propri server(8). Tuttavia, in senso contrario non può tacersi che i servizi offerti on-line, pure ad utenti anonimi, nella maggior parte dei casi (e quando così non sia, il discorso è ovviamente diverso), non hanno normalmente nulla di pericoloso perché non sono strutturalmente rivolti a realizzare danni, né producono statisticamente un certo rischio da considerarsi inevitabile per la natura del servizio stesso. È vero che il concetto di attività pericolosa, soprattutto nel nostro ordinamento, è spesso usato in maniera piuttosto arbitraria dalla giurisprudenza. È, però, anche vero che la stessa giurisprudenza cerca sempre di giustificare l'applicazione dell'art. 2050 c.c. rilevando come, quantomeno rispetto alle circostanze di fatto nelle quali una certa attività è stata compiuta, essa risulta intrinsecamente pericolosa. In altre parole, la pericolosità di una certa attività o di un certo servizio non può desumersi né da circostanze

straordinarie ed imprevedibili, né dall'uso che di questo vien fatto da parte di soggetti terzi rispetto a colui che dovrebbe essere chiamato a rispondere degli eventuali danni. Per questa ragione − ma non anche perché le questioni giudiziarie aventi ad oggetto illeciti commessi via Internet siano, a conti fatti, poche − non sembra possibile, allo stato dell'arte, nel nostro ordinamento, ricondurre nell'alveo di operatività dell'art. 2050 c.c. la responsabilità dei prestatori di servizi di rete per illecito commesso dagli utenti.

4. I programmi filtro nella prima giurisprudenza nordamericana.

Un gran numero di illeciti commessi on-line, sinora portati nelle aule giudiziarie, riguardano casi di diffamazione o, più in generale, di lesione dei diritti della personalità (9). Ciò ha indotto la giurisprudenza e la dottrina che si è occupata di tali vicende a riflettere circa l'applicazione, in capo ai prestatori dei servizi di rete attraverso i quali vengono compiuti tali illeciti, dei principi ulteriori rispetto a quelli cennati nel paragrafo precedente, e cioè dei principi operanti in materia di responsabilità editoriale (10).

Nell'ormai celebre caso nordamericano Cubby, Inc. v. CompuServe, Inc.(11), in un forum telematico gestito dalla società CompuServe erano stati diffusi alcuni messaggi dal contenuto diffamatorio, tendenti a gettare discredito sulla società Cubby. La corte, nella circostanza, escluse qualsiasi responsabilità editoriale da parte del gestore del forum, osservando che la velocità con cui i dati sono immessi in rete non consente un controllo sui loro contenuti ed equiparando l'attività del service provider a quella del bibliotecario o del giornalaio, i quali non sono tenuti a controllare il contenuto dei libri messi a disposizione del pubblico (12), sebbene, qualora coscienti della illiceità di un prodotto o di una informazione, debbano attivarsi per impedire la realizzazione dei danni.

Questa impostazione del problema non fu esente da critiche, sicché, dopo pochi anni, nell'ormai noto caso Stratton Oakmont, Inc. v. Prodigy Services, Co.(13), una società che gestiva un bullettinboardsystem (una sorta di bacheca elettronica), in cui erano diffusi alcuni messaggi diffamatori per l'attore, venne condannata in quanto, nella fattispecie, secondo i giudici, essa aveva assunto veri e propri poteri editoriali, visto che si era dotata di un sistema di filtraggio delle informazioni finalizzato ad evitare che fossero lanciati messaggi dannosi. Si andava così delineando una situazione paradossale, giacché l'aver adottato delle contentguidelines, in forza delle quali sarebbe stato possibile eliminare materiali offensivi dal sito, nonché l'aver applicato un automatico software screening per la ricerca e l'eliminazione delle parole oscene e offensive, invece che provare la diligenza del service provider, ne determinavano la condanna. Il che finì per disincentivare l'adozione di filtri automatici, in quanto questi erano (e sono) tecnicamente in grado di ridurre, ma non di eliminare, i materiali illeciti o comunque lesivi di diritti altrui presenti nei siti Internet.

Tale vicenda, insieme alle preoccupazioni sollevate dalla presenza in rete di una gran quantità di materiale pornografico accessibile a chiunque, e dunque anche ai minori, suscitò la reazione del legislatore americano che nel 1996 ema-

nò, all'interno del nuovo Telecommunications Act (47 United State Code 230 (14)), il Communication Decency Act (CDA), il quale, tra l'altro, e per quanto qui interessa, prevede che "nessun fornitore o utilizzatore di un servizio interattivo telematico sarà trattato come un editore nei confronti delle informazioni prodotte da un altro fornitore di contenuto (content provider)" ed inoltre afferma la non responsabilità dei prestatori per gli eventuali danni causati quando, in buona fede, impediscano l'accesso ai materiali ritenuti potenzialmente lesivi di diritti altrui (c.d. Good Samaritan Blocking and Screening of Offensive Material(15)), anche a prescindere dal fatto che i materiali in questione ricevano una specifica tutela costituzionale (16).

Le prime applicazioni giurisprudenziali di tale normativa confermarono la generale impossibilità di equiparare, a fini risarcitori, il prestatore di un servizio di retead un editore e, dunque, mandarono salvo quest'ultimo da eventuali imputazioni di responsabilità a titolo più o meno oggettivo (17). Tuttavia, dubbi in dottrina suscitò la scelta legislativa di consentire agli intermediari di Internet di impedire, in buona fede, agli utenti l'accesso alle informazioni on-line potenzialmente lesive di diritti altrui (18). Principio che si giustificava in ragione del fatto che l'Act in questione era stato voluto per combattere, in particolare, l'accesso dei minori ai siti pornografici. La Corte Suprema degli Stati Uniti intervenne sul punto facendo proprie le perplessità sollevate da alcuni autori ed affermando, di conseguenza, la parziale incostituzionalità dell'CDA per violazione del primo emendamento della costituzione americana (19).

Una volta esclusa, in ragione delle considerazioni qui brevemente riassunte, la configurazione della responsabilità civile dei provider di Internet in termini oggettivi o semioggettivi, negli Stati Uniti si è fatta larga, tanto in giurisprudenza, quanto in dottrina, l'idea di applicare alla situazione in esame la teoria del contributory infringment, a tenore della quale un soggetto (secondarily liable) può essere ritenuto responsabile quando contribuisca materialmente − ecco perché siamo fuori dal campo della responsabilità oggettiva − alla commissione di un illecito altrui (directly liable) (20). Al fine di rendere pienamente operativa la figura del contributory infringment, occorre, tuttavia, valutare la possibilità di rimproverare al responsabile secondario una effettiva partecipazione psicologica alla realizzazione dell'illecito (21). Questo rappresenta il punto critico dell'applicazione della teoria in parola, e non soltanto in relazione ai danni cagionati via (o per mezzo di) Internet. Sul contenuto e sulla natura di tale partecipazione si scontrano quanti ritengono che il presupposto psicologico, atto a giustificare l'imputazione della contributory liability, debba essere costituito dalla effettiva consapevolezza (actual knowledge) della strumentalità della propria attività alla causazione del danno cagionato direttamente da altri; e quanti, al contrario, pensano che basti la volontaria messa a disposizione di mezzi obiettivamente in grado di facilitare la commissione dell'illecito (si parla di constructive knowledge) per configurare una sufficiente partecipazione all'illecito.

Particolarmente significative, a questo riguardo, si rivelano, anche per il peculiare quadro normativo in cui si inseriscono, alcune vicende giurisprudenziali nordamericane in cui viene esaminata la responsabilità dei provider per violazione del diritto d'autore. In uno dei primi casi di copyright infringment riguardante Internet, la controversia Playboy v. Frena(22), un gestore di BBS a pagamento, venne convenuto in giudizio perché, tramite tale servizio, venivano scambiate on-line fotografie il cui diritto d'autore era in capo alla società attrice. Il prestatore si difese dichiarando di aver ritirato prontamente le fotografie in questione non appena venuto a conoscenza dello scambio di foto che avveniva tra gli utenti del servizio in spregio del diritto d'autore suddetto. La Corte, tuttavia, condannò il convenuto.

E, pur potendo fondare la decisione sulla teoria del contributory liability, in quanto era evidente che il service provider metteva volontariamente a disposizione degli utenti mezzi obiettivamente in grado di facilitare la commissione dell'illecito in questione, i giudici preferirono soffermarsi sul fatto che il convenuto prestava il suo servizio al fine di lucro e che da esso, dunque, traeva vantaggi patrimoniali, da ciò ricavando la sua responsabilità colposa come direct infringer(23). Questo orientamento rimase pressoché isolato, in quanto subito dopo venne sconfessato da numerose pronunce che sancirono l'impossibilità di rimproverare il prestatore di servizi di rete per attività, lesive del diritto d'autore, compiute dagli utenti. Nel caso Marobie v. NAFED, ad esempio, i giudici mandarono esente da responsabilità il provider equiparandolo al proprietario di una fotocopiatrice che non risponde dell'utilizzazione illecita della stessa fatta da altri (24).

Nello stesso senso si espresse la District Court della California nel caso Religious Technology v. Netcom, che respinse la richiesta di condanna del provider richiamando la giurisprudenza in materia di gestori di telefonia e dunque sottolineando l'impossibilità per ogni fornitore di servizi di comunicazione di controllare i contenuti veicolati (25).

Recuperata, in particolare attraverso l'applicazione della teoria del contributory infringment, una visione colpevocentrica della responsabilità degli Internet provider, per creare certezza nella complessa materia occorreva sottrarre alla discrezionalità dei giudici la valutazione circa l'elemento psicologico e la correttezza del fornitore di servizi via Internet.

E, dunque, occorreva precisare, una volta per tutte, i presupposti rispetto ai quali valutare la partecipazione del prestatore all'illecito dello user(26). Da qui al Digital Millennium Copyright Act il passo fu davvero breve.

5. Il Digital Millennium Copyright Act.

Il 28 ottobre 1998, negli Stati Uniti, fu emanato il Digital Millennium Copyright Act (DCMA) (17 United State Code 1201) (27), il quale, tra l'altro (28), disciplina la responsabilità dei prestatori di servizi di reteper la diffusione di materiali che violano le norme a tutela del copyright(29). Al fine suddetto, e cioè per limitare la discrezionalità del giudice nel valutare la contributoryliabili-

ty del provider, la § 512 del capitolo V del title 17 dello U.S.C. − introdotta dal title II del DCMA e rubricata "Limitations on liability relating to material online" − stabilisce regole di esonero della responsabilità per il prestatore che si limiti a fare da intermediario tecnico tra gli utenti coinvolti nell'illecito, senza partecipare volontariamente alla commissione di questo.

In particolare, per quanto concerne il fornitore di un servizio telematico che trasmette o fornisce accesso alla rete, la § 512 a) prevede che questi non possa essere considerato responsabile qualora: 1) l'informazione sia propagata da un soggetto terzo; 2) la trasmissione, la connessione o lo stoccaggio delle informazioni rientri in un processo tecnico, e l'operatore non abbia selezionato i contenuti da diffondere; 3) l'intermediario non selezioni i destinatari; 4) il contenuto non sia registrato e non sia mantenuto per un periodo di tempo che ecceda quello strettamente necessario allo svolgimento delle finalità tecniche; 5) l'informazione non sia modificata dall'intermediario. La § 512 b) prende in considerazione il caso del provider che, nel fornire un determinato servizio, non si limita a veicolare segnali, ma opera attraverso un procedimento di memorizzazione temporanea delle informazioni sul suo disco rigido (c.d. caching). Tale attività si differenzia dalla mera trasmissione in quanto consente l'intercettazione dei materiali memorizzati e, dunque, permette al prestatore di intervenire per bloccarne la ulteriore permanenza in rete, quando sia venuto a conoscenza di fatti o circostanze in base ai quali l'attività illecita è manifesta ovvero abbia ricevuto una apposita notificazione di un terzo. La section da ultimo citata prevede che la condotta dell'intermediario possa essere considerata neutra, e dunque corretta, quando l'informazione: 1) è fornita da un soggetto terzo, 2) è trasmessa da questo stesso soggetto senza l'intervento del prestatore; e 3) è memorizzata automaticamente al solo fine di essere a disposizione degli utilizzatori del servizio. Per quanto concerne la trasmissione, inoltre, il prestatore intermediario: 1) non deve modificare le informazioni; 2) deve aggiornarle su richiesta del destinatario del servizio; 3) non deve interferire con la tecnologia utilizzata da quest'ultimo. Infine, per quanto concerne l'attività di hosting, la § 512 c) prevede che essa possa generare responsabilità in capo al prestatore quando: 1) questi è a conoscenza dell'attività illecita compiuta dal suo cliente, ovvero di fatti e circostanze che rendono manifesta tale illiceità; 2) ha un beneficio economico che deriva direttamente dalla prestazione del servizio alla attività illecita (30); 3) rimane inerte rispetto all'obbligo di rimuovere i materiali illeciti (31).

La soluzione adottata con il DMCA − alla fine di un dibattito acceso che aveva portato, tra il 1997 e il 1998, alla presentazione di due distinti progetti di legge − sostanzialmente esonera i provider da ogni ipotesi di contributory liability, in caso di violazione di copyright da parte di utenti di Internet, quando la partecipazione dei prestatori di servizi di rete alla vicenda che produce un danno a terzi abbia caratteri esclusivamente tecnici. In altre parole, il legislatore nordamericano − sollevando non poche critiche nella dottrina specializzata (32) − ha così accolto la teoria per cui vi sarebbe contributory infringment solo quando

il prestatore eccede il suo ruolo tecnico di intermediario e partecipa volontariamente, anche se non dolosamente, alla commissione dell'atto lesivo. È evidente come, in tale contesto, l'utilizzazione di programmi filtro in grado di selezionare i materiali diffusi in rete ovvero mittenti e destinatari degli stessi, espone i provider al rischio di vedersi rimproverata una partecipazione attiva all'illecito e dunque di vedersi contestata una piena responsabilità giuridica per i danni causati.

6. Il regime di responsabilità dei *provider* nella direttiva 2000/31/Ce e nel D.Lgs. 9 aprile 2003 n. 70.

Con la direttiva 2000/31/CE (33), emanata l'8 giugno del 2000, l'Unione Europa, come noto, si è dotata di principi comuni in materia di "taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno" (34). La direttiva − recepita in Italia con il D.Lgs. n. 70 del 9 aprile 2003 − rappresenta l'unico riferimento normativo europeo in materia di responsabilità civile dei soggetti che, in quanto *provider*, offrono servizi on-line e che proprio tale articolato definisce "prestatori di servizi della società dell'informazione".

La normativa europea in parola dedica la sezione IV, rubricata "Responsabilità dei prestatori intermediari", al perseguimento di un difficile contemperamento tra gli interessi, spesso confliggenti, dei diversi soggetti che operano in Internet (cfr. il considerando n. 41): da un parte, quelli dei prestatori che forniscono servizi di varia natura a non essere ritenuti responsabili per attività illecite compiute dai propri utenti; dall'altra, quelli dell'intera comunità internazionale e delle imprese che temono le potenzialità lesive della rete, preoccupate che Internet rimanga uno spazio privo di regole, di controllori e, dunque, di responsabilità. Prima di passare in rassegna le singole disposizioni del testo comunitario che risultano, ai nostri fini, più significative − e che sono state riprodotte fedelmente nella normativa di attuazione italiana − occorre chiarire che la direttiva "non crea una forma di responsabilità *ad hoc* per gli intermediari della rete" (35), in quanto ha preferito consentire l'applicazione a questi soggetti delle regole di diritto comune, salvo affermare che, quando in capo a tali operatori non è possibile individuare alcuna responsabilità specifica espressamente prevista dalla direttiva stessa, essi non rispondono del fatto illecito compiuto on-line da chi utilizza i loro servizi (36).

Tale scelta − come anticipato − viene attuata attraverso il combinato disposto degli articoli da 12 a 15 del testo comunitario, a cui corrispondono gli artt. 14-17 della normativa italiana di recepimento. In particolare, all'art. 12, rubricato "Semplice trasporto", all'art. 13, "Memorizzazione temporanea detta *caching*", e all'art. 14, "*Hosting*", l'articolato in parola prevede che i prestatori di servizi di rete, in presenza di condizioni che garantiscano la loro totale estraneità rispetto ai contenuti veicolati o memorizzati (temporaneamente o meno), non sono responsabili dell'illiceità di quei contenuti. In ogni caso, non appena

l'operatore abbia notizia di tale illiceità, deve provvedere a rimuovere i materiali coinvolti (37).

In particolare, per quanto concerne quella che possiamo definire "l'immunità condizionata" dell'intermediario, l'art. 12 della direttiva stabilisce espressamente che "nella prestazione di un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione, il prestatore non sia responsabile delle informazioni trasmesse a condizione che egli: *a*) non dia origine alla trasmissione; *b*) non selezioni il destinatario della trasmissione; e *c*) non selezioni né modifichi le informazioni trasmesse". L'ultimo comma dell'art. 12, con una formula poi ripetuta anche agli artt. 13 e 14, lascia impregiudicata la possibilità, secondo gli ordinamenti degli stati membri, che un organo giurisdizionale o un'autorità amministrativa esiga che il prestatore impedisca o ponga fine ad una violazione. A sua volta, l'art. 13, a proposito dell'attività di memorizzazione temporanea, prevede che il prestatore non sia responsabile quando: "*a*) non modifichi le informazioni; *b*) si conformi alle condizioni di accesso alle informazioni; *c*) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore"; *d*) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni; ed *e*) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione dell'accesso". L'art. 14, infine, individua due condizioni sufficienti ad esonerare da responsabilità il fornitore di *hosting*: 1) quest'ultimo non deve essere effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non deve essere al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione; 2) non appena al corrente dei fatti, il fornitore deve agire immediatamente per rimuovere le informazioni o per disabilitare l'accesso. Ed inoltre, al fine di evitare sin troppo facili raggiri, al punto 2, prevede che il paragrafo 1 − contenente il principio che abbiamo definito di immunità condizionata dell'intermediario − non si applica quando il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore; statuizione questa che si giustifica in ragione del fatto che un prestatore, il quale voglia compiere attività illecite, potrebbe avere buon gioco, ad esempio, a creare una propria società figlia che gestisca un sito ospitato sul proprio *server*, limitandosi formalmente a svolgere il ruolo di mero intermediario, e così scaricando sul gestore del sito eventuali responsabilità derivanti dalla commissione di illeciti.

Dalla lettura degli artt. 12-14 della direttiva, appare subito evidente come la responsabilità del prestatore sia definita in negativo. La disciplina, di cui alle norme ora citate, stabilisce infatti che, in presenza di determinate condizioni,

questi non risponde degli illeciti on-line commessi dagli utenti; la qual cosa, posto che la verificazione di tali condizioni dipende esclusivamente dal comportamento dell'intermediario, equivale a dire che quest'ultimo può essere condannato a risarcire il danno soltanto se ha volutamente consentito che si integrasse una delle condizioni che fanno scattare la sua responsabilità, mentre gode di una sorta di immunità quando si limita a svolgere in rete esclusivamente un ruolo tecnico di intermediazione. Il legislatore comunitario ha sottratto i prestatori intermediari alla scure rappresentata dall'applicazione di criteri di imputazione della responsabilità di natura più o meno oggettiva, per ricondurre il regime della responsabilità, a loro applicabile, nel porto sicuro dell'imputazione per colpa (38). In definitiva, può dirsi che vi sarà colpa del prestatore quando questi non si limita a svolgere il ruolo tecnico di intermediario e partecipa, perciò, più o meno attivamente − anche paradossalmente al solo fine di svolgere un vaglio di legittimità − alla vicenda che trova il suo attore principale nell'utente.

7. L'espressa previsione normativa dell'assenza di un obbligo di sorveglianza in capo ai *provider*.

La direttiva 2000/31/Ce sembra appositamente studiata per non lasciare l'accertamento della colpa del *provider* alla discrezionalità del giudice. Quest'ultimo, infatti, non è genericamente chiamato, come sarebbe in forza dell'art. 2043 c.c., a valutare la correttezza della condotta e dell'atteggiamento psichico dell'intermediario, bensì è tenuto ad applicare i principi della direttiva − che il D.Lgs. 70/2003 ha riprodotto fedelmente −, e dunque esclusivamente ad accertare, quando il danneggiato agisca contro l'intermediario cercando di provare la sua colpa specifica, che quest'ultimo non abbia posto in essere nessuna delle condizioni che fanno scattare la sua responsabilità. Siamo, dunque, alle prese con un sistema di imputazione della responsabilità basato esclusivamente sulla colpa specifica dell'intermediario, e cioè sulla colpa per violazione di legge (39); mentre al giudice è precluso, in quanto inutile al fine dell'imputazione della responsabilità (40), ogni accertamento ulteriore relativo all'atteggiamento psichico del convenuto. La circostanza, al di là di ogni pur legittima giustificazione di carattere tecnico-giuridico, mette in chiaro l'obiettivo perseguito dalla normativa in esame, che è quello di modulare regole giuridiche (volte ad esonerare il più possibile gli intermediari della società dell'informazione da ipotesi risarcitorie) di applicazione non arbitraria al fine di creare certezza in una materia nella quale sinora ha dominato l'incertezza.

Nel sistema di responsabilità di cui si sono qui tracciate le linee essenziali un ruolo pivotale è quello svolto dall'art. 15 della direttiva, riversato nell'art. 17 del D.Lgs. 70/2003. Il paragrafo 1 di tale disposizione ribadisce il divieto per gli Stati membri di imporre ai prestatori dei servizi di cui agli articoli 12, 13 e 14 "un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano [e] di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite". Ancora più importante, nell'economia della riflessione che si sta compiendo in questa sede, appare il paragrafo 2 dell'art. 15. nel quale

si consente espressamente agli Stati di stabilire, in sede di recepimento (come ha fatto il legislatore italiano del D.Lgs. 70/2003 nel secondo comma del citato art. 17), "che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati". L'unica interpretazione possibile delle due norme in grado di ricondurle ad una certa coerenza è quella per cui non possono imporsi obblighi di sorveglianza in capo al *provider*, ma se questi per caso viene a conoscenza di attività illecite dei proprio utenti ha l'obbligo di informare l'autorità preposta e collaborare con essa.

Meno facile è interpretare in modo coerente con quanto sin qui esposto il considerando 48 della direttiva, nel quale il legislatore europeo ha chiarito di non voler pregiudicare "la possibilità per gli Stati membri di chiedere ai prestatori di servizi [...] di adempiere al dovere di diligenza che è ragionevole attendersi da loro ed è previsto dal diritto nazionale, al fine di individuare e prevenire alcuni tipi di attività illecite". L'utilità di un tale "richiesta" resta alquanto indecifrabile, posto che, se gli obblighi generali di diligenza esistono, così come è nel nostro ordinamento, essi devono essere rispettati indipendentemente da una sollecitazione del legislatore, e dovrebbero condizionare integralmente l'attività del *provider*, sicché il loro rispetto dovrebbe indurre quest'ultimo, oltre che a rimuovere senza ritardo il materiale illecito quando ne abbia notizia (41), a tentare di prevenire, per quanto possibile, la stessa commissione dell'illecito. Tuttavia, una tale interpretazione rischia di far rientrare dalla finestra delle clausole generali l'obbligo di sorveglianza in capo ai *provider* che il legislatore ha, invece, cacciato dalla porta principale dell'articolato normativo. Meglio, allora, intendere il considerando in parola come un'esortazione rivolta agli Stati affinché questi chiariscano nel dettaglio il contenuto degli obblighi gravanti sugli intermediari di Internet ai sensi della direttiva europea (42).

8. Le ragioni gius-economiche della soluzione adottata con la direttiva 2000/31/Ce.

Una volta chiarito che la direttiva 2000/31/Ce, in relazione agli illeciti commessi in rete dagli utenti, ha adottato una soluzione in linea con la vicenda giurisprudenziale e legislativa maturata negli Stati Uniti, finalizzata a deresponsabilizzare gli intermediari della società dell'informazione, a patto che non abbiano contribuito con la propria condotta alla realizzazione dell'attività illecita nei modi indicati nei precedenti due paragrafi, occorre verificare le ricadute sociali ed economiche di tale soluzione, onde verificarne l'efficienza in termini di politica del diritto o, se si preferisce, in termini gius-economici.

Per prima cosa, va sottolineato che − come anticipato − la scelta legislativa in questione è stata dettata principalmente dall'esigenza di evitare che sui fornitori di servizi on-line gravino costi eccessivi in termini di spese risarcitorie e di

predisposizione di sistemi di protezione volti ad evitare, per quanto possibile, la commissione di illeciti rimasti anonimi da parte degli *user*. In una situazione in cui gli intermediari dovessero rispondere dei danni realizzati dagli utenti, e, dunque, in buona sostanza, dovessero far fronte ai costi sociali creati dall'utilizzazione della rete telematica, da un lato diminuirebbero gli operatori che forniscono servizi on-line, in quanto si verificherebbe un processo di selezione naturale per cui solo i soggetti meglio organizzati potrebbero sopravvivere, dall'altro vi sarebbe un inevitabile aumento del prezzo dei servizi offerti, in quanto gli operatori cercherebbero di allocare i costi in parola sugli utenti(43). Entrambe le derive ora prospettate non sono certamente auspicabili. In una società che da poco, e proprio grazie ad Internet, ha scoperto quanto ricca possa essere l'informazione e la comunicazione umana in presenza di un vero pluralismo delle fonti di informazione e di intermediazione, proporre un ritorno al passato − affidando Internet ai soggetti economicamente in grado di svolgere gli opportuni controlli sui contenuti immessi dagli utenti in rete e di far fronte ai danni che inevitabilmente verrebbero a prodursi − vorrebbe dire negare l'essenza stessa del *medium* in parola e, di conseguenza, depotenziare quest'ultimo anche dal punto di vista commerciale. Come è ovvio, né le imprese che su Internet continuano ad investire ingenti capitali, né gli stati nazionali hanno interesse a ridurre il pluralismo attualmente presente su Internet, in tal modo depotenziando il valore relazionale e commerciale della rete(44). Nell'ordinamento italiano, così come nella maggior parte dei sistemi occidentali, peraltro, il pluralismo delle fonti di informazione appare addirittura dotato di rango costituzionale(45)**.**

Una eventuale scelta di politica del diritto volta ad applicare la teoria del rischio di impresa o, in ogni caso, un criterio (più o meno) oggettivo di imputazione della responsabilità, ai c.d. intermediari della società dell'informazione, non avrebbe determinato effetti sociali positivi e, dunque, sarebbe stata inefficiente. Tale sensazione, già ampiamente giustificata in forza delle considerazioni sin qui svolte, diventa certezza se solo si prende in esame un altro aspetto della questione.

Come ormai noto, la scelta di un criterio di imputazione, piuttosto che di un altro, dipende dalle condizioni in cui la singola attività viene svolta. Tra le circostanze che occorre prendere in considerazione per valutare l'opportunità di adottare un modello di responsabilità oggettiva ovvero un modello di responsabilità per colpa, vi è la capacità, *rectius* la possibilità, tecnica e/o tecnologica dell'imprenditore di prevenire o ridurre il rischio di incidenti. Nel caso del prestatore di servizi che svolga in Internet il ruolo di *service provider*, è di tutta evidenza che questi non potrà mai effettuare una reale azione totalmente preventiva volta ad evitare che l'utente commetta illeciti in Internet in forma anonima. Egli, infatti, quando non sia anche *access provider* dell'utente, non può controllarne le generalità, in quanto quest'ultimo gli si presenta esclusivamente mostrando il suo Ip (Internet Protocol), né può verificare a priori la liceità dei contenuti veicolati in rete, ovvero ospitati sul proprio sito, o sul proprio *server***.**

Una tale verifica (non solo, richiederebbe tempi che rallenterebbero la rete snaturandola e, nel contempo, costituirebbe una grave violazione della *privacy* degli utenti e della possibilità di esprimere liberamente il proprio pensiero, ma) si rivelerebbe senza dubbio inefficace considerato che, molto spesso, la liceità della diffusione di un certo materiale non può essere valutata senza considerare circostanze ulteriori rispetto al materiale stesso. Ciò è a dire, ma gli esempi potrebbero essere tantissimi, che la pubblicazione in un sito Internet di una immagine che ritrae un corpo di donna nudo non è di per sé lecita o illecita, e può diventarlo soltanto nella misura in cui il soggetto ritratto non ha mai autorizzato la pubblicazione dell'immagine. Men che meno è possibile, per il prestatore, controllare preventivamente i contenuti scaricati in rete dagli utenti attraverso servizi che consento la comunicazione in tempo reale tra due o più persone: *chat***,** *newsgroup***,** *bullettinboard systems*; la qual cosa, del resto, finirebbe anche per violare il diritto alla libertà e alla segretezza della comunicazione e corrispondenza privata.

L'applicazione di un criterio di responsabilità oggettivo o semioggettivo, dunque, indurrebbe, considerate le circostanze suddette, il prestatore a concedere i propri servizi soltanto a clienti o attività fidate e sicure. Il che si tradurrebbe in una censura diretta anche di siti e materiali con contenuti non immediatamente illeciti(46)**.** Ad esempio, un *host provider* potrebbe decidere di concedere ospitalità solo a siti contenenti materiali con una bassissima potenzialità lesiva di diritti altrui, con ciò negando il proprio servizio anche agli operatori o agli utenti che non abbiano alcuna intenzione di compiere illeciti. Il rischio è che i prestatori di servizi diventino i censori istituzionali della rete "decidendo cosa è conveniente fare e cosa non lo è"(47)**.**

A questo rischio − che il legislatore comunitario ha voluto evitare adottando all'uopo una soluzione di politica del diritto che sottrae il prestatore ad un criterio oggettivo di imputazione della responsabilità − se ne contrappone, tuttavia, uno esattamente speculare. La scelta di sottrarre i prestatori di servizi di Internet ad ipotesi di responsabilità per omesso controllo ha un effetto di *underdeterrence* da non sottovalutare. In una situazione legislativa in cui ai *provider* non si chiede un controllo sui contenuti veicolati in Internet, ovvero ospitati sui propri siti o sul proprio *server*, nessuno è incentivato ad investire in *software* o strategie aziendali in grado, se non proprio di eliminare, di limitare il rischio costituito da illeciti commessi da utenti rimasti anonimi. Sicché, anche le imprese produttrici dei *software* in grado di controllare alcune informazioni e filtrarle, non avendo mercato, smetteranno di sviluppare tali tecnologie. Tutto ciò aumenta certamente le possibilità che in rete vengano commessi illeciti senza che nessuno risponda del relativo danno e, dunque, contribuisce ad alimentare la sensazione di deresponsabilizzazione che l'utente prova mentre naviga, nonché quella di impotenza che il danneggiato avverte di fronte agli illeciti altrui(48).

Rischio quest'ultimo che si determinerebbe tal quale anche qualora le politiche legislative adottate nei Paesi più importanti, in quanto maggiormente tecnologizzati e ricchi, incentivassero, se pure indirettamente ed involontariamente, la

collocazione dei prestatori di servizi della società dell'informazione nei Paesi dove la normativa applicabile in materia fosse molto più tollerante e, dunque, meno esigente con loro. Si potrebbe, in altre parole, determinare un fenomeno di *rule* **e** *forum shopping* nell'ambito del quale i provider intenzionati a fornire in rete servizi ad alto rischio, perché esposti alla possibilità che l'utente li utilizzi per commettere illeciti, andrebbero ad ubicare i proprio server ed organizzare li svolgimento delle proprie attività in Paesi nei quali non sarebbero in ogni caso chiamati a rispondere dei relativi danni. La mancanza di confini geografici che caratterizza il mondo virtuale delle reti telematiche, ed in particolare Internet, consente senz'altro il ricorso a simili sotterfugi. Ed anche con questa circostanza devono fare i conti i legislatori chiamati a regolamentare Internet ed in particolare intenzionati a disciplinare il problema degli illeciti commessi on-line.

Alla luce delle considerazioni appena svolte, al fine di comprendere ancora meglio le ragioni che hanno condotto all'emanazione della DMCA negli Stati Uniti e della direttiva 2000/31/Ce in Europa, occorre domandarsi perché, rispetto al trattamento dei dati personali, il legislatore comunitario, con la direttiva 95/46/Ce abbia adottato un regime di responsabilità semi-oggettiva (sostanzialmente prevedendo che il titolare del trattamento risponde dell'illecito se non prova di aver fatto tutto il possibile per evitare il danno; riguardo all'ordinamento italiano cfr. artt. 18 del legge 675/96, oggi come noto abrogata, e 15 del D.Lgs. 196/2003), mentre relativamente alla responsabilità dei *provider* abbia mostrato un atteggiamento affatto diverso. La risposta che appare più plausibile si basa sulla considerazione per cui il trattamento dei dati personali altrui, pur non rappresentando un'attività in sé pericolosa, può diventare dannosa, e dunque fonte di responsabilità civile, soltanto quando sia proprio il titolare di tale trattamento a contravvenire alle regole di comportamento dettate dalla normativa in vigore o, più in generale, quando viola l'obbligo di correttezza a cui la disciplina in materia fa espresso riferimento. Dunque, l'applicazione di un criterio di imputazione di natura semi-oggettiva può ben svolgere, in questo caso, una funzione preventiva, in quanto i titolari del trattamento, pur di evitare giudizi di responsabilità, presteranno maggiore attenzione alle modalità con cui svolgono la loro attività ed in tal modo si eviteranno, o si ridurranno sensibilmente, i danni da questa cagionati.

Per giustificare pienamente la scelta di politica del diritto che spinse il legislatore comunitario a prevedere un regime di tal fatta per regolare la responsabilità per trattamento dei dati personali, e per sottolineare ulteriormente come tale scelta, in ogni caso, non poteva essere estesa a carico dei prestatori di servizi della società dell'informazione rispetto al problema degli illeciti commessi in rete da utenti anonimi, va altresì sottolineato che: mentre, rispetto ad Internet, è da tutti condivisa l'esigenza di non inaridire le fonti, gli spazi e le occasioni di comunicazione e di informazione on-line − e l'assunzione del regime in parola, come visto, avrebbe prodotto questo effetto −; rispetto al trattamento dei dati personali, non c'è motivo di credere che l'applicazione di un criterio di imputazione della responsabilità, piuttosto che di un altro, possa determinare effetti

negativi per i mercati o i rapporti sociali, considerato che la normativa di derivazione comunitaria garantisce espressamente il diritto a trattare lecitamente dati personali altrui (con il solo limite dei dati sensibili).

9. I tempi cambiano: una nuova stagione per la responsabilità in Internet?

Quello tracciato nei paragrafi precedenti è, in estrema sintesi, lo stato dell'arte della disciplina di matrice legislativa operante in materia di responsabilità civile dei *provider* tanto in Italia, quanto all'interno dell'Unione europea e negli Stati Uniti. Stato dell'arte che abbiamo a più ripreso definito razionale e, sotto molteplici profili, tutto sommato, efficiente.

Resta da domandarsi soltanto se sia davvero questo − oggi che ormai abbiamo superato la fase sperimentale e siamo ormai definitivamente entrati nell'era di Internet − il migliore dei mondi possibili. In altre parole, rimane da chiederci se siamo realmente sicuri che sia efficiente, cioè utile ed opportuno, che gli intermediari della comunicazione su Internet consentano a chiunque di dire, fare e pubblicare in rete qualsiasi cosa, anche restando anonimi, senza avere alcuna responsabilità giuridica circa i contenuti che essi veicolano on-line. O, per dirla ancora diversamente, se siamo davvero sicuri di volere che in Internet continui ad essere possibile − cioè realizzabile senza conseguenze sul piano giuridico − tutto, anche ciò che normalmente è vietato e fonte di responsabilità nella realtà atomistica, cioè la realtà che si svolge fuori dalla grande rete.

La mia sensazione è che sino a quando Internet ha dovuto diffondersi, ampliarsi e consolidarsi, travalicare confini geografici, culturali e politici, entrare nelle case, negli uffici, nella vita delle persone, mostrare tutte le sue infinite possibilità, schiudere all'uomo possibilità infinite e finanche sogni, insomma sino a quando Internet era nella sua fase espansiva, sarebbe stato davvero controproducente tentare di limitare le immense e progressive potenzialità del nuovo mezzo, laddove per altro era ed è evidente che la tecnologia cerca, per ragioni molteplici ed eterogenee, di sfuggire alla regolamentazione giuridica. Tuttavia, oggi che Internet rappresenta un riferimento allo stato indispensabile ed irrinunciabile per ogni uomo, in quanto il mondo virtuale ubiquo è divenuto oramai una realtà alla quale più o meno tutti, per varie ragioni (ludiche, professionali, di ricerca, relazionali, commerciali e quant'altro), attingiamo, ed all'interno della quale, soprattutto nei paesi progrediti, gran parte della popolazione trascorre molte ore ogni giorno, la situazione è cambiata perché Internet non ha più bisogno di espandere la propria presenza ma di consolidarla, sicché *mutatis mutandis* andrebbero rivalutate ragioni e circostanze, fino a riconsiderare il ruolo del diritto − anzi, meglio, del momento giuridico − nel panorama virtuale. Internet, infatti, attualmente non ha più ragione di temere il diritto, la regolamentazione giuridica, mentre l'ordinamento giuridico oggi ha senz'altro buone ragioni per guardare Internet con sospetto. Peraltro, se è vero che rispetto a vent'anni anni fa la struttura della rete sostanzialmente non è cambiata perché i *provider* costituiscono ancora gli unici soggetti potenzialmente in grado di ef-

fettuare un filtro sui contenuti veicolati on-line, sono tuttavia enormemente aumentate le possibilità tecniche che essi hanno di sviluppare, volendo, sistemi di controllo su tali contenuti. Ciò, come detto, senza pretesa di esaustività, ma con la consapevolezza che investendo le giuste risorse molto si può fare per prevenire, sventare o comunque punire il compimento di illeciti in rete.

Continuare a sottovalutare l'importanza di un sistema di responsabilità giuridica che sia in grado di funzionare anche rispetto agli illeciti compiuti on-line, dunque, vuol dire oggi sottostimare i costi sociali che Internet determina, ed in definitiva trascurare la potenza del mezzo telematico, o dell'ambiente digitale ubiquo, o ancora, secondo alcuni, di Internet inteso come nuova coscienza collettiva. Pensare che Internet possa ancora a lungo restare − per dirla con Jean Carbonnier (*Regards sur le droit et le non-droit*, Paris, Dalloz, 2005) − il regno del "non diritto" sembra alquanto anacronistico o, quanto meno, non pare il modo migliore per facilitarne la definitiva consacrazione come agorà in cui le persone si incontrano, si conoscono, si scambiano idee, espongo informazioni di cui sono in possesso e ne cercano di ulteriori, mettono in rete saperi, conoscenze, dubbi, risposte, si chiedono e si offrono assistenza, servizi, beni, volgono transazioni di mercato ed altro ancora.

Né a tal proposito può sottovalutarsi che tutti i c.d. *mass-media* costituiscono tecnologie altamente invasive e condizionanti addirittura il pensiero e la coscienza dell'uomo. In proposito, in tema di immagini che è possibile vedere on-line anche in forma di video (come nel caso di cui si è occupato il Tribunale di Milano nella citata recente sentenza), è opportuno ricordare che, già in epoca pre-Internet, relativamente al mezzo televisivo, Cristopher Lasch, nel saggio "La cultura del narcisismo" (1979), osservava come "Le immagini arrestano le esperienze e tolgono la responsabilità". E che Ghunter Anders, nel suo celebre "L'uomo è antiquato" (1956), esplicava ancora meglio il concetto evidenziando come "chi vede un'esplosione nucleare fornita a domicilio dalla TV è privato della capacità di cogliere quello che è accaduto davvero e quindi prendere posizione responsabilmente", in quanto inevitabilmente ed inconsciamente finisce per credere che i possibili effetti di un disastro nucleare nella sua vita siano quelli che ha già vissuto quando attraverso la televisione ha visto nello schermo l'esplosione. Senza, ovviamente, dimenticare che, di contro, proprio Internet, consentendo a chiunque di diffondere in tutto il mondo qualsiasi materiale riproducibile in formato digitale, permette all'opinione pubblica di conoscere fatti e circostanze che un tempo restavano nascoste per volontà politica di questo o quel dittatore, di questa o quella nazione, così contribuendo ad evitare, o quanto meno, condannare, atrocità, barbarie, violenze, censure e quant'altro.

Dunque, l'impatto che può avere sulla coscienza individuale e collettiva, nonché sulla formazione dell'opinione e della sensibilità singola e di massa, la pubblicazione o la non pubblicazione di un video immesso on-line da un utente tramite uno dei tanti *provider* esistenti, sia nel bene che nel male, è altissimo. Da qui l'esigenza di parametrare in modo attento l'eventuale − ed a mio avviso,

auspicabile − imposizione in capo ai *provider*, o meglio determinati *provider*, di un obbligo di controllo sui contenuti immessi in rete per conto dei clienti.

Sono − quelli qui appena accennati − aspetti giustamente evidenziati dai sociologi, dagli antropologi e dagli psicologi, che il giurista non può trascurare nel momento in cui si occupa di nuove tecnologie della comunicazione e dell'informazione.

Il mio auspicio, dunque, è che l'attuale assetto di Internet, inteso per quello che ho appena detto, come nuovo "regno del non diritto", in realtà sia solo il prodotto di contingenze temporali, e che dunque − come accaduto, ad esempio, in materia dei costi sociali prodotti dalla circolazione dei veicoli − dopo un'iniziale stagione di sostanziale deresponsabilizzazione generale, possano nascere sistemi di responsabilità idonei sotto il profilo tecnico, efficienti in termini economici e giusti in termini di equità sociale. Io in proposito qualche idea ce l'avrei − è, ad esempio, dal 2001 che sostengo la tesi per cui l'identità degli utenti di Internet dovrebbe essere sempre conosciuta dall'*access provider* di riferimento così da tutelare la *privacy* di ogni singolo *user* senza al contempo garantire sacche di impunità − ma ovviamente anche una scelta di tal fatta non ha senso se compiuta dal singolo legislatore nazionale, in quanto Internet impone, per le ragioni sopra cennate, decisioni di politica del diritto adottate su scala internazionale da quanti più paesi possibili.

Molto lavoro, insomma, c'è da fare soprattutto sotto il profilo culturale, perché, per arrivare ad un'ampia condivisione internazionale di scelte di politica del diritto epocali in materia, occorre mettere d'accordo tecnologi, antropologi e giuristi, oltre che ovviamente politici, utenti di Internet e grandi imprese coinvolte. Non resta che rimboccarsi le maniche.

NOTE

* Relazione presentata all'incontro di studi dal titolo "Il futuro della responsabilità sulla Rete. Quali regole dopo la sentenza Google/Vivi-Down" 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 in questa Rivista, 2010, 474.

(1) Ormai è ben nota la differenza tra i diversi tipi di provider. Per una rapida ricognizione della tematica sia consentito rinviare a F. DiCiommo, Internet (responsabilità civile), voce dell'Enc. giur. Treccani, Aggiornamento 2002 Roma, 2002.

(2) Circa l'utilizzazione dei filtri da parte dei provider, cfr. J.P. Semitsu, Burning Cyberbooks in Public Libraries: Internet Filtering Software vs. The First Amendment, 52 Stan. L. Rev. 509 (2000); e M.S. Nadel, The First Amendment's Limitations on the Use of Internet Filtering in Public and School Libraries: What Content Can Librarians Exclude?, 78 Texas L. Rev. 1117 (2000). Per considerazioni meno datate, v. M. Grady e F. Parisi (a cura di), The Law and Economics of Cybersecurity, New York, 2006.

(3) Come efficacemente sottolinea G. Pascuzzi, Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche, Bologna, 2003, 126-127: "Considerare i provider immuni da qualsivoglia responsabilità per le attività commesse da chi per loro tramite accede alla rete significa rinunciare ad avvalersi dell'unico strumento oggi a disposizione per controllare la rete (il provider è il solo collo di bottiglia attraverso il quale è possibile intercettare e scoprire eventuali abusi)". Sia consentito sul punto, anche per consi-

derazioni più generali, rinviare a F. DiCiommo, Internet e crisi del diritto privato: tra globalizzazione, dematerializzazione e anonimato virtuale, in Riv. crit. dir. priv., 2002, 57.

(4) Cfr. E. Montero, La responsabilité des prestataires intermédiairies sur les réseaux, in AA.VV., Le commerce électronique européen sur les rails? Analyse et propositions de mis en oeuvre de la directive sur le commerce électronique, Bruxelles, 2001, 273.

(5) Emblematica, a questo riguardo, risulta una delle prime vicende giurisprudenziali europee aventi ad oggetto la responsabilità di un provider, al termine della quale la signora Leff-Bure, coniugata Hallyday, riuscì ad ottenere la condanna al risarcimento dei danni da un provider di Internetper illecito commesso da un utente che, sfruttando un sito Internet da quest'ultimo messo a disposizione di chiunque volesse pubblicare online, aveva diffuso in rete, senza autorizzazione, fotografie "strettamente private" della signora. Il Tribunale sancì la responsabilità del provider per omesso controllo sui contenuti da lui ospitati, senza svolgere alcuna indagine volta ad accertarne la colpa (Trib. gr. inst. Parigi, 9 giugno 1998, in Expertises, 1998, n. 216, 319; tra i principali commenti alla pronuncia, v. M.H. Tonnelier, Responsabilité de l'hébergeur, ibid., n. 219, 308; ed È.A. Caprioli, Respondabilitédufournisseur d'hébergment d'un site Web, in Droit&Patrimoine, 1999, n. 67, 90). La Court d'Appel di Parigi, con sentenza 10 febbraio 1999 (in Dalloz, 1999, jur., 389; pubblicata anche Italia in Danno e resp., 1999, 754, con traduzione e nota di DiCiommo, e in questa Rivista, 1999, 929, con nota di Riccio) confermò la condanna del provider. Per una riflessione su un caso giurisprudenziale francese più recente, che ha riguardato la enciclopedia virtuale "Wikipedia", V. F. Casarosa, Wikipedia: Exemption from Liability in Case of Immediate Removal of Unlawful Materials, (2009) 6:3 SCRIPTed 669.

(6) Nella prima giurisprudenza italiana, cfr. Trib. Roma, 4 luglio 1998, in questa Rivista, 1998, 807; Trib. Roma, 22 marzo 1999, in id., 2000, 66; Trib. Teramo, ordinanza 11 dicembre 1997, id., 1998, 372; Trib. Napoli, decreto 18 marzo 1997, in Foro it., 1997, I, 2307; Trib. Napoli, ordinanza 8 agosto 1997, in Giust. civ., 1998, 1, 258.

(7) Diverso si presenta il caso in cui siano commessi illeciti attraverso un computer messo dal datore di lavoro a disposizione di un dipendente per svolgere le sue funzioni.

(8) Cfr. G. Facci, La responsabilità extracontrattuale dell'internet provider, in Resp. civ. e prev., 2002, 265.

(9) In argomento, sia ancora consentito rinviare a F. DiCiommo, Diritti della personalità tra media tradizionali e avvento di Internet, in G. Comandé (a cura di), Persona e tutele giuridiche, Torino, 2003, 3.

(10) Cfr., tra i molti, O. Braun, Internet Publications and Defamation: Why the Single Publication Rule Should Not Apply, 32 Golden Gate U.L. Rev. 325 (2002), e T. Komasara, Planting the Seeds of Hatred: Why Imminence Should No Longer Required to Impose Liability on Internet Communications, 29 Cap. U.L. Rev. 835 (2002).

(11) 776 Fed. Supp. 135 (S.D.N.Y. 1992).

(12) In questi termini si espressa la giurisprudenza americana già nel primo caso di illecito telematico di cui si abbia notizia: Daniel v. Dow Jones, 520 N.Y.S.2d 334 (N.Y. Civ. Ct. 1987). Per affermazioni dello stesso principio, che viene giustificato in ragione della libertà di diffusione delle informazioni, v. anche Auvil v. CBS '60 Minutes, 800 Fed. Supp. 928, 1992; e Stern v. Delphi Service Corp., 626 N.Y.S.2d 694 (N.Y. Sup. 1995).

(13) Per l'epilogo della vicenda processuale, v. la sentenza della New York Supreme Court, 11 dicembre 1995, in West Law, 1995, 323710. Per un commento critico a tale

pronuncia, v. M.C. Sideritis, Defamation in Cyberspace: Reconciling Cubby, Inc. v. Compuserve, Inc. and Stratton Oakmont v. Prodigy Services Co., 79 Marq. L. Rev. 1996, 1079.

(14) Il Telecommunication Act ha modificato il Communication Act del 1934 (47 United State Code 201 et seq.).

(15) Per gli opportuni approfondimenti N.W. Guenther, Good Samaritan to the Rescue: America Ondine Free from Publisher and Distributor Liability for Anonymously Posted Defamation, 20 Comm. and the Law 35 (1998).

(16) Il § 230 c) (2) (A) del Communication Decency Act stabilisce espressamente che il provider non risponde per "any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be oscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected". Per gli opportuni approfondimenti, v. S. Beckett, A Brave New World of Free Speech: Should Interactive Computer Srvice Providers Be Held Liable for the Material They Disseminate, 5 Richmond J. of Law & Tech.nn. 13-40 (1998).

(17) Così, ad esempio, la prima pronuncia in materia successiva all'emanazione dell'Act: Zeran v. American Online (AOL) 958 Fed. Supp. 1124 (E.D. Va. 1997), aff'd129 F.3d 327 (4th Cir. 1997); nonché, Lunney v. Prodigy Services 683 N.Y.S. 2d 557 (App. Div. 1998), aff'd164, 1999 N.Y. Lexis 3746 (1999).

(18) La soluzione forte, adottata dal legislatore nordamericano, non piaceva alla dottrina che, in larga maggioranza, suggeriva approcci diversi al problema. Cfr., ad esempio, A.M. Major, Internet Red Light District: A Domain NameProposal for Regulatory Zoning of Obscene Content, in J. Marshall J. Computer & Info. 21 (1997), il quale proponeva di attribuire ai siti un nome di dominio di secondo livello in grado di qualificare immediatamente il contenuto e la natura del sito.

(19) La sentenza, che chiuse la vicenda Reno v. ACLU, fu emanata il 26 giugno 1997 ed è pubblicata in Italia in Riv. dir. ind., 1998, II, 140, trad. e nota di Cucinotta, e in questa Rivista, 1998, 64, trad. e nota di ZenoZencovich. Le motivazioni che supportano la decisione dei giudici federali appaiono particolarmente significative in quanto sottolineano come il Communication Decency Act costituiva una limitazione in contrasto con il Primo Emendamento giacché rischiava di restringere eccessivamente la libertà di espressione che spetta agli adulti e, nel contempo, di non essere realmente efficace come mezzo di prevenzione dell'accesso dei minori al materiale pornografico on-line.

(20) Così, tra gli altri, D.N. Weiskopf, The Risks of Copyright Infringment on the Internet: A Practitioner's Guide, 33 U.S.F.L. Rev. 1 (1998); J. Carmichael, In Support of the White Paper: Why Online Service Providers Should Not Receive Immunity from Traditional Notions of Vicarious and contributory Liability for Copyright Infringment, 16 Loy. L.A. Ent. L.J. 771 (1996); e J.C. Ginsburg, Putting Cars on the "Information Superhighway": Authors, Exploiters, and Copyrights in Cyberspace, 95 Colum. L. Rev. 1493 (1995). Contra, S.C. Pomeroy, Promoting the Progress of Science and the Useful Arts in the Digital Domain: Copyright, Computer Bullettin Boards, and Liability for Infringments by Others, 45 Emory L. Rev. 1061 (1996).

(21) Negli Stati Uniti, tradizionalmente, gli intermediari operanti nel settore dell'informazione, quando si limitano a svolgere un ruolo di mero trasporto di informazioni altrui, sono considerati non responsabili per l'eventuale illiceità di tali contenuti, in quanto materialmente impossibilitati, e per motivi di celerità e per motivi di privacy, a controllare i messaggi prima di spedirli; e ciò a meno che essi non siano a conoscenza della illiceità dei materiali trasportati. È il caso, ad esempio, degli operatori telefonici o

telegrafici, i quali sono definiti common carriers. Secondo i più, i common carriers rientrerebbero nella categoria dei secondary publishers e, dunque, dei secondarily liables. In proposito, v. 47 United State Code § 153 (1991). Tra le sentenze più significative a riguardo, v. Western Union Tel. v. Lesesne, 182 F.2d 135 (5th Cir. 1950). Cfr. J.C. Proya, Liability of Telegraph or Telephone Company for Transmitting or Permitting Transmission of Libelous or Slanderous Messages, 91 A.L.R.3d 1015 (1979).

(22) 839 F. Supp. 1552 (M.D. Fla. 1993).

(23) La giurisprudenza americana ha più volte rilevato come, perché vi sia violazione del copyright da parte del direct infringment, non occorra che l'autore dell'illecito sia consapevole della pericolosità o della dannosità della sua condotta. Tra le altre, v. Da Costa v. Brown, 146 F.2d 408 (2d Cir. 1944).

(24) Marobie-FL, Inc. v. National Association of Fire Equip. Distributors, 853 F. Supp. 1167 (N.D. Ill. 1997).

(25) Religious Technology Center, and Bridge Publication, Inc. v. Netcom, Inc. D. Erlich, and T. Klenesrud, 907 F. Sip. 1361 (N.D. Cal. 1995).

(26) Su tale esigenza si sofferma in particolare C. Butler, Plotting the Return of An Ancient Tort to Cyberspace: Towards a New Federal Standard of Responsability for Defamation for Internet Service Providers, 6 Mich. Telecomm. Tech. L. Rev. 247 (1999-2000). Cfr. D.J. Loundy, Computer Information System Operator Liability, 21 Seatlle Univ. L. Rev., 1167 (1998).

(27) 17 U.S.C. 1201, Pub. L. 105-304, 112 Stat. 2860 (Oct 28, 1998).

(28) Cfr. R. Caso, Introduzione. 2. L'evoluzione del copyright statunitense e del diritto d'autore italiano, in G. Pascuzzi-R. Caso (a cura di), I diritti sulle opere digitali. Copyright statunitense e diritto d'autore italiano, Padova, 2002, 38; nonché D. Nimmer, Puzzles of the Digital Millennium Copyright Act, 46 J. Copyright Soc'y USA 401 (1999); A.R. Fox, The Millennium Copyright Act: Disabusing the Notion of a Constitutional Moment, 27 Rutgers Computer &Tech. L.J. 267 (2001), e J.C. Ginsburg, Il "Digital Millennium Copyright Act'ed il "Sonny Bono Copyright Act": due novità dagli Stati Uniti (trad. it. a cura di P. Marzano), in Riv. dir. comm., 1999, 625.

(29) Cfr. M.P. Goldstein, Service Provider Liability for Acts Committed by Users: What You don't Know can Hurt You, 18 The John Marshall Journal of Computer & Information Law 591 (2000); e Yen, op. cit.

(30) Sulconcetto di "beneficio economico diretto", cfr. O.G. Hatch, Towards a Principled Approach to Copyright Legislation at the Turn of the Millennium, 59 Univ. Of Pitts. L. Rev. 828 (1999).

(31) Tale obbligo è dettato dalla §512 b)(2)(E). In proposito, giova segnalare che il DMCA prevede un procedimento di denuncia della presenza di materiali illeciti, nel corso del quale l'interessato produce una notification all'intermediario, che, una volta a conoscenza dell'attività illecita, dovrà attivarsi per bloccarla rimuovendo i materiali o sospendendo l'invio delle informazioni. Sul punto, v. J.A. Friedman-F.M. Buono, Using the Digital Millennium Copyright Act to Limit Potential Copyright Liability Online, 6 Richmond Jour. of. Law & Tech. 13 (1999).

(32) Tra gli studiosi maggiormente critici nei confronti del DMCA, in quanto ritenuto eccessivamente benevolo con gli Internet provider, v. D.R. Cahoy, New Legislation Regarding On-Line Service Provider Liability for Copyright Infringment: A Solution in Search of a Problem?, 38 IDEA: The J. Of Law and Tech. 335 (1998); M.A. Ravn, Navigating Terra Incognita: Why the Digital Millennium Copyright Act Was Needed to Chart the Course of Online Service Provider Liability for Copyright Infringment, 60 Ohio St. L.J. 778 (1999); e L.H. Holmes, Making Waves In Statutory Safe Harbors:

Reevaluating Internet Service Providers' Liability for Third-Party Content and Copyright Infringement, 7 Roger Williams U.L. Rev. 215 (2001). Cfr. anche D.L. Burk,MuddyRules for Cyberspace, 21 Cardozo L. Rev. 121 (1999), secondo cui il DMCA crea una situazione di incertezza che potrebbe anche rivelarsi economicamente efficiente.

(33) La direttiva 2000/31/Ce riproduce il testo della Posizione Comune n. 23/2000, adottata il 28 febbraio 2000, in G.U.C.E., 8 maggio 2000, C 128. La dottrina italiana che ha commentato la direttiva in parola è molto ampia, sicché in questa sede, se consentito, si rinvia, anche per gli autori ivi citati, a F. DiCiommo, Evoluzione tecnologica e regole di responsabilità civile, Napoli, 2003.

(34) Ai sensi del considerando n. 17 della direttiva 2000/31/Ce, la definizione di servizi della società dell'informazione "ricopre qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica, mediante apparecchiature elettroniche di elaborazione (compresa la compressione digitale) e di memorizzazione di dati, e a richiesta individuale di un destinatario di servizi". Tale definizione è mutuata da quella utilizzata nella direttiva 98/34/Ce del 22 giugno 1998.

(35) Così G.M. Riccio, Profili di responsabilità civile dell'Internet Provider, Salerno, 2000, 78 e nello stesso senso Id. La responsabilità civile degli Internet providers, Torino, 2002. Cfr. A. Pierucci, La responsabilità extracontrattuale del fornitore di servizi telematici, in Maschio (a cura di), op. cit., 459.

(36) Sui rapporti tra i principi stabiliti dalla direttiva 2000/31/Ce e gli ordinamenti nazionali, si sofferma ampiamente R. Bocchini, La responsabilità civile degli intermediari del commercio elettronico. Contributo allo studio dell'illecito plurisoggettivo permanente, Napoli, 2003.

(37) Cfr. Trib. Grand di Parigi, 20 novembre 2000, in questa Rivista, 2001, 209, con nota di Costanzo. Sull'obbligo di rimuovere i materiali illeciti, cfr. G. Cassano-F. Buffa, Responsabilità del content provider e dell'host provider, in Corriere giur., 2003, 77. Più in generale, sulla portata degli artt. 12-15 della Direttiva, tra gli altri, si veda DiCiommo, Internet (responsabilità civile), cit.; nonché L. Edwards, Articles 12-15 ECD: ISP Liability, The Problem of Intermediary Service Provider Liability, in Id. (a cura di), The New Legal Framework for E-Commerce in Europe, Oxford, 2005, 93.

(38) Su tale scelta di politica del diritto, cfr., ex multis, A. Pierucci, La responsabilità del provider per i contenuti illeciti della Rete, in Riv. crit. dir. priv., 2003, 143, in part. 161; nonché L. Bugiolacchi, La responsabilità dell'Host Provider alla luce del d.lgs. 70/2003: esegesi di una disciplina dimezzata, in Resp. civ. e previd., 2005, 70.

(39) Il ricorso normativo alla colpa specifica in qualche modo si giustifica in ragione del fatto che il legislatore comunitario ha deciso di imputare in capo al provider una responsabilità omissiva. Poiché − posta la "libertà di non agire" che in via generale l'ordinamento riconosce ad ogni consociato − l'obbligo di attivarsi per evitare danni ad altri viene considerato dai più un'ipotesi eccezionale rispetto al semplice canone di diligenza di cui all'art. 2043, è necessario che esso sia tassativamente previsto da una norma di legge. In altre parole, occorre vi sia una norma primaria, che rende obbligatoria la tenuta di un certo comportamento, perché la violazione della stessa integri un fatto illecito di natura extracontrattuale. Da qui la coerenza, in termini di teoria generale, di un sistema basato sulla colpa specifica, cioè sulla violazione di un obbligo previsto espressamente dalla legge.

(40) A ben vedere, il grado della colpa dell'intermediario − che, in presenza di un sistema di imputazione basato sulla colpa specifica, il giudice, come chiarito, non ha motivo di accertare al fine di decidere se un illecito compiuto on-line da un utente sia im-

putabile al provider − torna a giocare un ruolo importante in sede di applicazione del secondo comma dell'art. 2055.

(41) Cfr. l'ordinanza del Trib. Napoli, 28 dicembre 2001 (in Dir. ind., 2003, 159, con commento di Montuschi), secondo la quale non è dato escludere la responsabilità solidale, nella commissione dell'illecito, in capo al provider che non abbia adoperato tutta la diligenza esigibile da un operatore professionale e necessaria per evitare che, una volta reso edotto degli abusi commessi, tali abusi potessero continuare senza che egli provvedesse all'oscuramento dei siti contenenti i materiali considerati illeciti. Lo stesso tribunale partenopeo, con ordinanza del 15 maggio 2002, ibid., 163, pronunciandosi sul reclamo formulato contro il provvedimento del 28 dicembre 2001, ha inoltre precisato: "Ancorché la direttiva 2000/31/Ce [...] escluda il potere degli Stati membri di imporre al prestatore di servizi della società dell'informazione un obbligo generale di sorveglianza sulla informazioni da lui trasmesse o memorizzate per conto degli utenti nella rete o di ricercare attivamente fatti o circostanza che indichino la presenza di attività illecite. [...] non può escludersi la legittimità di una interpretazione valevole per l'ordinamento italiano che, mettendo in risalto la natura professionale dell'attività svolta dal provider nella prestazione dei servizi [...] e gli indubbi profitti che egli ne trae, esiga da lui una piena cooperazione nel momento in cui si tratta di impedire il protrarsi dell'illecito posto in essere attraverso la rete informatica [...]". Per una rapida rassegna della giurisprudenza italiana in argomento, v. da ultimo G. Cassano-A. Contaldo, La natura giuridica e la responsabilità civile degli Internet Service Providers (ISP): il punto sulla giurisprudenza, in Corriere giur., 2009, 1206.

(42) Cfr. M. Vermeer, Unfair Competition Online and the European Electronic Commerce Directive, 7 Ann. Surv. Int'l & Comp. L. 87 (2001).

(43) Cfr. G.M. Riccio, Anonimato e responsabilità in Internet, in questa Rivista, 2000, 335; nonché Id., La responsabilità civile degli internet providers, in part. 39-40.

(44) Cfr. il considerando n. 2 della direttiva 2000/21/Cee.

(45) La Corte Costituzionale italiana, nella sentenza n. 420 del 7 dicembre 1994, in Foro amm., 1994, 2667, ha affermato che nel nostro ordinamento il diritto all'informazione, garantito dall'art. 21 Cost., implica indefettibilmente il pluralismo delle fonti e comporta per il legislatore il vincolo di emanare norme che impediscano la formazione di posizioni dominanti. Anche negli Stati Uniti la giurisprudenza afferma costantemente l'esigenza di mantenere libero e pluralista il marketplace of ideas come strumento di difesa della democrazia effettiva. Il diritto di partecipare alla produzione e alla distribuzione di informazioni è stato elaborato nell'ambito della c.d. "Gertz doctrine", che trae la sua denominazione dal caso Gertz v. Robert Welch, Inc., 418 U.S. 232 (1974). Per l'applicazione di tale principio ad Internet, cfr. M. Hadley, The Gertz Doctrine and Internet Defamation, 84 Va. L. Rev. 477 (1998). A questo proposito, cfr. il considerando n. 10 della direttiva 2000/31/Ce.

(46) Cfr. G. Pino, Tra anarchia e caccia alle streghe. Alterne vicende della libertà di manifestazione del pensiero in Internet, in Ragion pratica, 2001, 133.

(47) Crf. S. Rodotà, Libertà, opportunità, democrazia e informazione, in Internet e privacy: quali regole?, Atti del Convegno di Roma dell'8 e 9 maggio 1998, intitolato Cittadini e Società dell'informazione, Supplemento n. 1 al Bollettino n. 5 del Garante, 1998, 15; Id., Qualche limite è necessario, in Teléma, 8, Primavera, 1997, 6. Cfr. C. Fried, Perfect Freedom or Perfect Control, 114 Harv. L. Rev., 606 (2000). Circa il rapporto tra esigenza di controllo dei contenuti della rete e privacy degli utenti, v. Corte Federale d'Appello degli Stati Uniti d'America, I circ., sentenza 29 giugno 2004, in Foro it., 2004, IV, 449, con nota di DiCiommo.

(48) Così S. Freiwald, Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation, 14 Harv. J. of L. & Tech. 643 (2001); nonché A.K. Patel, Immunizing Internet Service Providers from Third-Party Internet Defamation Claims: How Far Should Courts Go?, 55 Vand. L. Rev. 647 (2002). Cfr. J.M. Zitter, Liability of Internet Service Provider for Internet or E-mail Defamation, 84 A.L.R.5th 169 (2000); e A. Hamdani, WhòsLiable for Cyberwrongs?, 87 Cornell L. Rev. 901 (2002), il quale si pone il problema di cercare gli "optimal liabilitystandards" per gli Internet provider, e cioè il livello di controllo e prevenzione − ottimale perché potenzialmente in grado di non realizzare effetti né di over deterrence né di under deterrence − a cui gli intermediari devono attenersi per sollevarsi da responsabilità in caso di illecito compiuto dai naviganti; ma conclude osservando che non è possibile individuare un'unica soluzione, in quanto bisogna indagare, di volta in volta, la natura dell'illecito compiuto e le circostanze in cui si è sviluppato il rapporto tra provider ed autore dell'illecito. Cfr. anche M. Schruers, The History and Ecnomics of ISP Liability for Third Party Content, 88 Va. L. Rev. 205 (2002), il quale giunge ad affermare che "the economic analysis above illustrates that negligence and strict liability regimes fail to produce an efficient level of monitoring", per cui la soluzione attualmente preferibile, al fine di "minimizing social costs and maintaining the benefits of the Internet", appare quella che punta a sviluppare un sistema di controllo e valutazione degli sforzi fatti dai provider per evitare che gli utenti commettano fatti illeciti attraverso i servizi offerti dagli intermediari.

Corte d'Appello di Milano, sez. I Penale,
sentenza 21 dicembre 2012 – 27 febbraio 2013, n. 8611
Presidente Malacarne – Relatore Milanesi

La responsabilità per il trattamento dei dati è legata al mancato adempimento di specifiche condizioni che rendono lecito l'uso di tali dati, ma tali condizioni non possono che essere messe in capo al titolare, al controller *dei dati medesimi. Acquisire un video, memorizzarlo, cancellarlo, non può significare di per sé trattamento di dati sensibili .*

Va escluso il dolo specifico quando manca qualsiasi riscontro di un vantaggio direttamente conseguito dagli imputati, da non confondersi con la vocazione economica eventualmente caratterizzante l'attività dell'imputato

Per sostenere la responsabilità a titolo di omissione in capo ad un host *o* content provider, *occorre affermare a suo carico un obbligo giuridico di impedire l'evento e quindi da un lato, l'esistenza di una posizione di garanzia, dall'altro la concreta possibilità di effettuare un controllo preventivo* [che non sussiste nel caso in esame].

L'attribuzione ad un internet provider di un dovere/potere di verifica preventiva va valutata in relazione alla collisione con forme di libera manifestazione del pensiero

Svolgimento del processo

1 - LA SENTENZA IMPUGNATA

Con la sentenza n° 1972/2010 emessa dal Tribunale di Milano in composizione monocratica, all'esito di giudizio abbreviato, in data 24/02/2010, D.D.C., F.P.A., D.L.R.G., A.D. venivano assolti perché il fatto non sussiste dall'imputazione loro contestata al capo A) ai sensi degli artt. 110, 40 comma II, 595 comma I e III cp. nei termini di seguito indicati: perché in concorso tra loro D.D.C.- Presidente del Consiglio di Amministrazione di G. Italy s.r.l. dal 19/03/2004 e successivamente nominato amministratore delegato in data 2/04/2004 (fino al 21/05/2007), F.P.A.- Responsabile delle policy sulla privacy per l'Europa (Global Privacy Counse) di G. Inc., D.L.R.G. -membro del Consiglio di Amministrazione di G. Italy s.r.l e successivamente nominato amministratore delegato in data 2/4/2004 (fino al 21/5/2007), D.A.- Responsabile del progetto G. Video per l'Europa, offendevano la reputazione dell'associazione Vivi Down-associazione italiana per la ricerca scientifica e per la tutela della persona Down - nonché di D.L.F.G., consentendo che venisse immesso per la successiva diffusione a mezzo Internet, attraverso le pagine del sito http://video,G..it e senza alcun controllo preventivo sul suo contenuto, un filmato in cui persone minorenni, in concorso tra loro, pronunciano la seguente frase "Salve, siamo dell'associazione Vivi Down, un nostro mongolo si è cagato ad-

dosso e mò non sappiamo che minchia fare perché l'odore di merda c'è entrato nelle narici" e pongono in essere numerosi altri atti vessatori nei confronti di un loro coetaneo disabile, ledendo i diritti e le libertà fondamentali nonché la dignità degli interessati. In Milano in epoca immediatamente successiva all'8 Settembre 2006 (data dell' upload video) fino al 07 novembre 2006 (data della rimozione del video).

Obbligo giuridico ex art. 40 comma 2 così individuato: omettevano- ciascuno nella rispettiva qualità - il corretto trattamento di dati personali così come prescritto dal D.L.vo 30 Giugno 2003 n. 196 (e altresì più volte sollecitato dall'Autorità Garante per la protezione dei dati personali, dopo il procedimento di cui al successivo capo C) in data 22/03/2006, 09/05/2006 e 03/07/2006), ed in particolare: dall'art. 13, difettando del tutto l'informativa sulla privacy, visualizzabile in italiano dalla pagina iniziale del servizio G. l'ideo, in sede di attivazione del relativo account, al fine di porre in essere l'upload dei files, in ordine a quanto prescritto dal comma 1 della richiamata norma, e per essa, del valido consenso di cui all'art. 23 comma 3; dall'art. 26, riguardando altresì dati idonei a rivelare lo stato di salute della persona inquadrata; dall'art. 17, per i rischi specifici insiti nel tipo di trattamento omesso nell'ipotesi di cui al presente procedimento, non attivandosi G. Italy srl neppure in tal senso, tramite il prescritto interpello, presso l'Autorità Garante. Trattamento omesso- anche in relazione alla concrete misure organizzative da apprestare, idonee alla sua successiva attuazione- fin dalla fase antecedente alla effettiva localizzazione del servizio G. Video sulla pagina http://video.G..it (di fatto avvenuta in data 12 Luglio 2006), non avendo né i due rappresentanti legali di G. Italy s.r.l., né il responsabile del progetto G. Video, (durante le numerose conference-call per la definizione delle modalità operative con il personale di G. Italy s.r.l. assegnato al progetto), né tantomeno il Global Privacy Counsel di G. Inc. affrontato la problematica relativa alla protezione dei dati personali che sarebbero stati trattati in relazione a G. Video, che invece veniva volutamente lanciato come servizio di "libero accesso" dopo un'attenta analisi del mercato italiano (confluita nel documento G. Video: "Preliminary analysis of italian market peculiarities"- redatto su indicazione di DES1KAN Arvind, dal personale di G. Italy s.r.l. assegnato al progetto G. Video - nel quale la consolidata presenza dei siti internet italiani che offrivano esclusivamente video di qualità veniva indicata come punto di criticità per diventare leader nel mercati dei video on line).

Con la medesima sentenza D.D.C., F.P.A., D.L.R.G. venivano riconosciuti responsabili del reato loro contestato al capo B) d'imputazione, per violazione degli artt. 110,167, comma 1 e 2 D.L.vo 30 Giugno 2003 n. 196, perché, in concorso tra loro e nelle circostanze di fatto di cui al precedente capo, al fine di trarne profitto per il tramite del servizio G. Video (in relazione al quale G. Italy s.r.l. beneficia degli indotti pubblicitari degli inserzionisti), procedevano al trattamento di dati personali in violazione agli artt. 23, 17 e 26stesso D.L.vo. con relativo nocumento per la persona interessata (D.L.F.G.). E pertanto gli stessi venivano condannati, con le attenuanti generiche e la diminuente del rito, alla

pena di mesi 6 di reclusione ciascuno, oltre il pagamento delle spese processuali; veniva inoltre riconosciuto il beneficio della sospensione condizionale della pena in favore di tutti gli imputati e disposta, ai sensi dell'art. 172 D.L.vo 30/06/2003 n.196, a cura e a spese dei medesimi imputati, la pubblicazione della sentenza una volta e per estratto sui quotidiani "Il Corriere della Sera", "La Repubblica" e "La Stampa".

2-Il FATTO

La sentenza appellata nell'esposizione del fatto e dell'esito delle indagini esperite richiama integralmente la ricostruzione operata da PM, in quanto pienamente condivisibile nella sua precisione e completezza.

In data 09/11/2006 l'associazione "Vivi Down" depositava presso la Procura della Repubblica di Milano una denuncia querela in relazione al contenuto di un video apparso in internet sul sito http://video.G..it nella sezione "video divertenti". Nel video, della durata di circa 3 minuti, compariva un ragazzo presumibilmente "down", in un ambiente scolastico, che veniva schernito e deriso da un gruppo di ragazzi, e si sentiva un voce fuori campo pronunciare la seguente frase: "salve, siamo dell'associazione VIVI DOWN, un nostro mongolo si è cagato addosso e mò non sappiamo che mischia fare, perché l'odore di merda ci è entrato nelle narici. "

A sua volta, il padre del ragazzo disabile D.L.F.G. proponeva denuncia-querela per il fatto, descrivendo i comportamenti vessatori posti in essere nei confronti del figlio.

Entrambe le querele portavano all'attenzione della Procura di Milano profili di responsabilità penale anche a carico dei responsabili del sito, sul rilievo che trattavasi di filmato che, non solo era circolato sul web tramite G. Video, ma non poteva essere passato inosservato perché aveva conquistato la prima posizione nella categoria "video più divertenti" ed era addirittura finito all'interno della classifica ufficiale dei video più scaricati.

Il padre del minore si doleva in particolare, della totale assenza di controllo da parte del Provider, nella specie G. Italia, non solo sui video immessi nel sito, ma anche su quelli rimasti tanto a lungo da entrare nelle classifiche predisposte.

Venivano dunque iniziate le indagini da cui emergeva che:

- Il video era stato girato nella classe di un istituto tecnico di Torino, in data 24/05/2006.

- Il medesimo video veniva caricato su G. Video tra T08/09/2006 ed il 10/09/2006 da tale G.L., non imputata nel presente procedimento.

- Il video nel corso dei due mesi successivi, veniva visualizzato 5.500 volte tanto da finire al 1° posto tra i "video più divertenti" ed al 29° tra i video più scaricati.

- In data 05/11/2006 il blogger D.A. segnalava sul suo blog "Giornalettismo militante - Il Cannocchiale.it" la presenza del video sul sito.

- In data 06/11/2006 tale BARAD1NO Silvia chiedeva la rimozione del video tramite il centro di assistenza G..

- In data 07/11/2006 la Polizia Postale di Roma richiedeva la rimozione del video.

- In data 07/11/2006 il video veniva rimosso.

Dopo l'identificazione degli autori del video, la Guardia di Finanza veniva delegata a compiere l'analisi tecnica dei servizi offerti da G. Video. Tale attività consentiva di accertare l'inesistenza di qualsiasi controllo preventivo nella fase di caricamento dei video.

La Polizia postale di Milano veniva di seguito delegata a svolgere indagini presso la sede di G. Italy s.r.l. ed in particolare a sentire H.S., Responsabile delle comunicazioni e M.M., Country Sales Manager, nonché ad effettuare una ispezione ai sistemi informatici della medesima società presso la sede operativa di Corso E., Milano. Nel corso del medesimo atto veniva rivenuto un file contenente nel testo riscontri sulla strategia di mercato di G. Italy s.r.l. a proposito del servizio G. Video da lanciare sul territorio dello Stato.

In sintesi risultava che G. Video doveva rappresentare sul mercato italiano un servizio di alta qualità, facile da usare, da intendersi come una piattaforma video di libero accesso anche in grado di massimizzare la sua potenzialità virale tramite la trasmissione di video ripresi con i cellulari.

All'esito delle complesse indagini svolte, comportanti l'acquisizione oltre che di una cospicua massa di documenti anche delle dichiarazioni delle dipendenti di G. Italy s.r.l., L.G. e V.P., l'Accusa perveniva alla conclusione che il servizio era stato lanciato volutamente senza controlli per sfondare sul mercato. Solo in seguito poi, dato l'enorme successo, veniva messa a punto la possibilità da parte degli utenti di segnalare contenuti inappropriati nei video immessi in rete al fine di consentire una loro eventuale rimozione. Comunque tutte le attività di controllo successivo e di rimozione nella realtà risultavano particolarmente inefficaci in considerazione della scarsità degli investimenti tecnici e di personale predisposti.

Per quanto riguarda il ruolo nelle vicende degli imputati, D.D.C. e D.L.R.G., agli stessi a fare data dal 2/04/2004 risultavano essere state affidate le cariche specificate in contestazione con i relativi poteri anche rappresentativi. La Guardia di Finanza evidenziava poi che i medesimi imputati risultavano ricoprire cariche di responsabilità anche in G. France, in G. UK. in G. Ireland, società tutte riferibili a G. Inc.

Per quanto riguarda il ruolo di A.D. lo stesso dalla documentazione reperita presso la sede di G. Italy e dalle dichiarazioni dei dipendenti italiani coinvolti nel progetto, emergeva essere il responsabile del progetto G. Video per l'Europa: proprio quest'ultimo imputato in una mail inviata a V.P. in data 13/11/06, a proposito dei fatti oggetto del presente procedimento, chiariva che le procedure di screening manuale non potevano considerarsi una soluzione praticabile, viceversa occorreva promuovere procedure automatizzate per ottenere una rimozione dei video più veloce.

Veniva quindi preso in considerazione il profilo commerciale di G. attraverso l'attività di ADwords.

Tale sistema di pubblicità basato su parole chiave, di enorme efficacia in quanto estremamente personalizzato, risultava essere proprio il programma pubblicitario di G.. Secondo la tesi accusatoria questo meccanismo era previsto anche in relazione al servizio G. Video.

A fronte delle prove raccolte dall'accusa il teste D.J. - la cui testimonianza era stata ammessa dal Tribunale con l'accoglimento dell'istanza proposta da tutti i difensori di rito abbreviato condizionato - sentito all'udienza del 29/09/09, escludeva però nel modo più assoluto che al tempo dei fatti fosse possibile inserire pubblicità su G. Video. Il medesimo teste inoltre dichiarava che inizialmente i controlli venivano svolti negli Stati Uniti, in seguito quando G. Video si espandeva in Europa, i controlli venivano effettuati anche da un team in Irlanda.

Sulla base delle considerazioni sopra riportate, l'Organo dell'accusa riteneva ampiamente provato il fine di lucro richiesto dall'art. 167 Codice Privacy contestato al capo B) della rubrica. Questo anche perché, sempre a parere dell'Accusa, in nessun caso il sistema G., di cui G. Video può essere considerata una parte, può ritenersi espressione di una mera intermediazione, un mero User Guaranted Content, come sostenuto dalla difesa degli imputati.

La tesi della mera intermediazione dalla quale far discendere una generale irresponsabilità, sempre seguendo la tesi accusatoria, cade una volta di più poi, laddove si ponga attenzione alla operatività del motore di ricerca ed anche proprio in relazione al tipo di servizio che ha generato l'odierna vicenda.

Per quanto riguarda il tema della possibilità di controllo sull'immissione di video in G. Video, veniva chiarito per prima cosa che oggi indubbiamente il servizio si presenta in termini completamente diversi da quello esistente in epoca immediatamente successiva ai fatti essendo lo stesso regolato dalla funzione Safe Search.

Per il passato, la Pubblica Accusa si rifaceva alle risultanze della perizia disposta e redatta a cura del prof. S.B., secondo cui in effetti erano esistenti strumenti tecnici utili per l'eliminazione di video illeciti da parte del gestore del servizio. Strumenti quantomeno utili a ridurre il più possibile la ricerca di video a rischio, necessitanti però anche di ulteriori apposite strutture necessarie per la verifica della liceità o meno del contenuto, e comunque inidonei in senso assoluto a consentire l'individuazione di tutte le casistiche di video illeciti.

La sentenza impugnata, prima di procedere alla trattazione delle singole posizioni, dà atto che nell'udienza 18/2/2009 veniva depositata dichiarazione di remissione di querela da arte di F.G. e di E.D.L. nei confronti di tutti gli imputati per il reato di cui al capo A), nonché accettazione della stessa da parte di questi ultimi; il processo quindi proseguiva, a seguito di declaratoria di improcedibilità nei confronti degli imputati ex artt. 469 e 129 cpp, per il capo A) in relazione alla querela dell'associazione Vivi Down per diffamazione ai danni dell'associazione medesima.

Al riguardo precisava il Giudice di prime cure, che la remissione di querela da parte dei D.L. escludeva solo la configurabilità del fatto nei confronti degli imputati in relazione a questa parte lesa, ma non incideva sugli elementi costitu-

tivi del reato di diffamazione ed in particolare sulla ricostruzione dello stesso così come prospettato e cioè come obbligo giuridico di impedire l'evento dannoso ai danni del minore disabile in primis e in conseguenza di ciò anche nei confronti dell'associazione Vivi Down.

Si dà inoltre atto che con ordinanza 18/2/2009 il Tribunale accoglieva la richiesta difensiva di estromissione della costituzione di Parte civile del Difensore Civico del Comune di Milano in ordine al capo B, mantenendo valide le altre costituzioni; e che con ordinanza 21/4/2009 veniva disposto lo stralcio degli atti relativi al capo C) d'imputazione, contenuto originariamente nel decreto di citazione diretta del PM di Milano, contestato ad A.N. per la violazione dell'art. 168 D.L.vo 30/06/2003 n. 196 con trasmissione degli stessi atti al Tribunale di Roma per competenza territoriale.

Con la medesima ordinanza veniva rigettata l'eccezione di incompetenza territoriale del Tribunale di Milano, formulata dalle difese degli imputati.

Il capo B) di imputazione: 11 trattamento dei dati personali del D.L..

Secondo la Pubblica Accusa gli imputati D.D.C., D.L.R.G., F.P.A., nella loro rispettive qualità, dovevano essere ritenuti responsabili del reato sub B), per avere trattato i dati personali e sensibili di D.L.F.G., consentendone il caricamento, l'utilizzo ed il mantenimento sul sito G. Video.it senza rispettare le regole relative alla protezione dei dati, ed al fine di trarne profitto; profitto derivante a mezzo della gestione del sistema AdWords.

Sempre secondo l'accusa le complesse modalità di applicazione del servizio ADwords, incidendo sui dati immessi nel sistema G. Video comportavano necessariamente un trattamento degli stessi e quindi escludevano la possibilità di considerare G. Italy o comunque G. Video un mero intermediario passivo (host provider) che agisce a richiesta del destinatario del servizio, quanto piuttosto un content provider e cioè un gestore di contenuti con tutte le relative conseguenze di responsabilità penale per i contenuti immessi.

Le difese degli imputati contestavano tali affermazioni e le valutazioni espresse dalla Procura osservando che:

- Il Codice Privacy non poteva essere applicato a G. Italy in quanto il trattamento dei dati contenuti nel video incriminato non avveniva in Italia ma negli Stati Uniti, a Denver, luogo ove sono ubicati i server di G. Inc.;

- G. Italy esercitando unicamente una attività di marketing a favore di G. Inc. non aveva alcun potere né alcuna possibilità di trattare i dati riferibili a quest'ultima.

- Andava escluso che ci fosse un collegamento G. Video- ADwords.

- G. Video non poteva che essere qualificato come host provider e dunque irresponsabile rispetto al contenuto dei dati immessi da terzi.

- Non esisteva alcun obbligo di controllo da parte della società sulle informazioni trasmesse e memorizzate, né obbligo di ricerca di video contenenti attività illecite.

- L'unico controllo sui dati spettava al soggetto che aveva proceduto del video incriminato e che era nelle condizioni di chiedere e di ricevere il consenso,

non incombendo sull'host provider alcun obbligo di controllo successivo in merito all'effettività del consenso prestato.

- L'obbligo dell'host provider rimane esclusivamente quello di indicare l'esistenza di obblighi a carico dell'utente quali quelli derivanti dalla normativa sulla privacy, il cui adempimento però resta di esclusiva responsabilità degli utilizzatori privati.

- I dati del D.L., rinvenibili sul video, non riguardavano il suo stato di salute, non essendo il minore affetto da Trisomia 21 e quindi non potevano essere considerati dati sensibili.

- Non si poteva ravvisare alcuna violazione né dell'art. 17 né dell'art. 13 Codice Privacy, avendo G. Video fornito una completa informativa agli utenti in merito al trattamento dati.

- Non esisteva alcun fine di profitto da parte di G. Italy essendo G. Video un servizio totalmente gratuito.

Il Giudice di primo grado dopo la disamina delle opposte prospettazioni, rilevava per prima cosa che non vi era possibilità di dubbio sul fatto che il video in questione contenesse allusioni e indicazioni sullo stato di minorità del soggetto. Pertanto occorreva partire dal fatto che il video di per sé fosse un dato personale e sensibile e come tale inquadrabile nella previsione dell'artt. 167 D.L.vo citato.

Nemmeno risulta poi dubitabile il fatto che il D.L. non avesse prestato alcun tipo di consenso in ordine alla divulgazione del video incriminato.

Ed ancora che non poteva dubitarsi dell'evidente nocumento alla persona offesa.

Da quanto sopra non poteva che concludersi dunque con l'affermazione della sussistenza di una palese violazione dell'artt. 167 D.L.vo cit. per lo meno dal punto di vista oggettivo.

Sempre secondo il giudicante poi non può esistere in materia una zona franca che consenta a un qualsiasi soggetto di ritenersi esente dagli obblighi di legge nel momento in cui venga in possesso di dati sensibili.

Ed in effetti il concetto di trattamento dei dati comprende qualsiasi comportamento che consenta ad un soggetto di apprendere un dato e di mantenerne il possesso fino al momento della sua distruzione.

In questo senso a poco vale la distinzione tra host provider e content provider.

Il proprietario o il gestore di un sito web che compia anche solo una di tale attività (raccolta, elaborazione, selezione, utilizzo, diffusione, organizzazione) si può dire che tratti i dati che gli vengono consegnati.

Detto ciò, non pare plausibile secondo il giudicante pretendere come nell'assunto accusatorio che un ISP possa verificare che tutte le migliaia di video, che vengono caricati in ogni momento sul suo sito web, abbiano ottemperato agli obblighi concernenti la privacy di tutti i soggetti negli stessi riprodotti.

L'ISP però deve fornire agli utenti tutte le necessarie avvertenze in ordine al rispetto delle norme con particolare attenzione nel caso a quelle che concernono

la necessità di ottenere l'obbligatorio consenso in ordine alla diffusione dei dati personali sensibili.

Esiste quindi non un obbligo di controllo preventivo dei dati immessi del sistema a carico dell'ISP quanto quello di una corretta e puntuale informazione da parte di chi accetti ed apprenda dati provenienti da terzi.

E quanto sopra è imposto non solo dall'art. 13 del D.L.vo cit. ma anche dal buon senso.

A parere del giudice di primo grado poi il fatto che l'ISP faccia un attività ulteriore rispetto a quella di mero intermediatore diventando hoster attivo o content provider è un elemento importante ma non trasforma l'ISP in un immediato realizzatore dei possibili reati emergenti dai dati caricati, in quanto non esiste fino ad oggi un obbligo di legge codificato che imponga all'ISP un controllo preventivo e non appare possibili ricavar tale obbligo aliunde con un'analogia in malam pattern.

In definitiva quello che può imporsi a G. Video, quale hoster attivo, è un obbligo di corretta informazione agli utenti degli obblighi agli stessi imposti dalla legge, del necessario rispetto degli stessi, dei rischi che si corrono a non ottemperarli oltreché naturalmente dell'obbligo di immediata cancellazione di quei dati e di quelle comunicazioni che risultassero correttamente segnalate come illegali.

Detto ciò andava escluso, secondo il Giudice di prime cure, che la condotta tenuta da G. potesse essere considerata sufficiente ai fini imposti dalla legge.

Questo in quanto le informazioni sugli obblighi derivanti dalla legge sulla privacy non venivano fornite in modo chiaro e con modalità di facile reperimento, ma anzi potevano essere trovate solo nascoste all'interno delle "condizioni generali di servizio" e per di più espresse con modalità incomprensibili.

Concludeva dunque il giudicante, osservando che nel caso erano stati accertati, al di la di ogni ragionevole dubbio, i seguenti elementi probatori.

- G. Italy costituiva la mano operativa e commerciale di G. Inc. in Italia.

- Attraverso ADwords, G. ltaly era in grado di collegare i clienti con i video immessi in rete da G. Video, e quindi in definitiva di trattare i dati contenuti in quest'ultimo sito.

- G. Italy di conseguenza era responsabile rispetto alla normativa sulla privacy dei dati contenuti nei video caricati sulla piattaforma di G. Video.

- In G. Video l'informativa sulla privacy era del tutto carente, l'avviso in questione, in effetti era presente, ma fornito in modo generico ed astratto e comunque tale da non risultare minimamente utile se non quasi a costituire una sorta di alibi la stessa società.

- Il fine di profitto richiesto dalla norma, per la sussistenza del dolo, in effetti poteva rinvenirsi nell'interazione derivante dalla operatività del sistema ADwords.

In definitiva, quindi il giudizio di responsabilità in ordine al reato di illecito trattamento dei dati personali, veniva espresso non sulla base di un obbligo preventivo di controllo sui dati immessi ma, sulla base di un profilo valutativo dif-

ferente, costituito dalla insufficiente e quindi colpevole comunicazione degli obblighi di legge agli uploaders.

Sempre sulla base di tutti gli indici rivelatori di tipo fattuale e documentale, sopra riportati, la sentenza perveniva al riconoscimento della sussistenza nel caso anche dell'elemento soggettivo richiesto dalla legge, in quanto rilevava una chiara accettazione consapevole del rischio concreto di trattamento di dati sensibili, per fini di profitto, concludendo con la dichiarazione di sussistenza della penale responsabilità degli imputati in relazione al reato loro contestato al capo B) della rubrica.

Capo A) d'imputazione: Il concorso nel reato di diffamazione.

Il Giudice di primo grado non poneva alcun dubbio sulla portata e valenza diffamatoria del fatto nel suo complesso ai danni della parte lesa Vivi Down, giudicando tra l'altro non accoglibile l'eccezione relativa all'improcedibilità per difetto di querela prospettata dalle difese; proseguiva quindi nella esposizione delle ragioni per cui non riteneva condivisibile la prospettazione accusatoria.

Secondo l'analisi svolta dal PM, i responsabili di G. oggi imputati, avevano l'obbligo preventivo di controllo sul contenuto dei video caricati e non avevano posto in essere tutti i filtri possibili, limitandosi ad un sistema di controllo successivo, conseguente alle segnalazione degli utenti.

Da una parte dunque, si riteneva una posizione di garanzia a carico del sito web, posizione derivante da un obbligo giuridico contenuto nella legge sulla privacy; quindi da tale posizione si giungeva a costruire un obbligo di controllo preventivo sui video caricati.

Tali affermazioni però, a parere del giudicante, non potevano essere condivise in quanto non ravvisabile, per lo meno fino ad oggi, "un obbligo di legge codificato che imponga agli ISP un controllo preventivo delle innumerevoli serie di dati che passano ogni secondo, nelle maglie dei gestori dei siti web, né appare possibile ricavarlo aliunde, superando il divieto di analogia in malarn partem, cardine interpretativo della nostra cultura procedimentale penale".

D'altra parte una posizione di garanzia, da cui derivi un obbligo di attivazione, in mancanza del quale ricorre la previsione dell'art. 40 C.P. non può essere frutto di una costruzione giurisprudenziale.

Dunque, pur non essendovi dubbio, prosegue il giudicante, che il gestore o il proprietario di un sito web qualificabile come content provider, possa essere ritenuto responsabile della violazione del D.Lvo sulla privacy, non appare rispondente alla vigente normativa, poterlo considerare corresponsabile del reato di diffamazione derivabile dal contenuto di materiale caricato da terzi.

Nella realtà poi, l'obbligo di controllo preventivo indicato dall'accusa, pare esser un comportamento inesigibile in ragione delle estreme difficoltà tecniche e delle conseguenze di sostanziale "illegittima" censura che ne potrebbe derivare.

Mancando una precisa legislazione in materia, la responsabilità penale degli ISP, non può essere costruita al di là dei canoni dell'attuale quadro normativo.

Anche se, a parere del Giudice di primo grado si sente l'esigenza di una buona legge sull'argomento, "in quanto internet è un formidabile strumento di

libera comunicazione, ma ogni esercizio collegato alla libertà non può essere assoluto": non resta che assolvere gli imputati dal reato di cui al capo A) perché il fatto non sussiste.

3) L APPELLO PROPOSTO DAL P.M

Con atto del 29/06/2010 il Pm chiedeva in riforma della sentenza di primo grado condannare gli imputati anche per il reato loro contestato al capo A) della rubrica, oltre che la conferma della condanna emessa per il capo B).

Sulla Sussistenza della posizione di garanzia di cui al capo A) degli elementi costitutivi del reato di cui al combinato disposto ex artt. 110, 40 cpv., 595 comma 3 C.P. e dell'elemento soggettivo richiesto dalla legge.

Premesso che il giudicante dopo aver riconosciuto all'interno del percorso motivazionale in relazione al capo B)- "che il video in questione contenga delle pesanti allusioni allo stato di salute del soggetto D.L. " e che " sia di per sé un "dato personale sensibile riferibile al D.L. , e come tale possa essere inquadrato nell'art. 167 D.L.vo citato, e che ribadisca anche in relazione al capo A) come non esista "dubbio...sulla portata e valenza diffamatoria del fatto a danno della parte lesa Vivi Down", ciononostante con argomentazioni non condivisibili, a parere dell'accusa, il Giudice di prime cure riteneva non sussistente la posizione di garanzia prospettata dall'accusa.

In sintesi, in quanto non esisterebbe: "un obbligo di legge codificato che imponga agli ISP un controllo preventivo della innumerevole serie di dati che passano ogni secondo nelle maglie dei gestori o proprietari dei siti web, e non appare possibile ricavarlo aliunde superando d'un balzo il divieto di analogia in malam partem cardine interpretativo della nostra cultura procedimentale penale.

L'analisi della prospettiva accusatoria però avrebbe dovuto limitarsi all'oggetto del procedimento ovvero al servizio G. Video e alle condotte poste in essere dagli imputati ciascuno per il loro ruolo di responsabilità nell'ambito della vicenda relativa alla progettazione/lancio del servizio nel Luglio 2006 sul territorio italiano.

In realtà, gli imputati omettevano ciascuno nella rispettiva qualità il corretto trattamento dei dati personali come prescritto dal dl.vo 30 Giugno 2003 numero 196 ed in particolare:

- dall'art. 13 difettando del tutto l'informativa sulla privacy, (visualizzabile dalla pagina iniziale di G. Video, in sede di attivazione del relativo account al fine di porre in essere l'upload dei files), rispetto a quanto prescritto dal comma 1 della richiamata normativa e al valido consenso di cui all'art. 23 comma 3.

- dall'art. 26 trattandosi di dati idonei a rivelare lo stato di salute della persona in oggetto.

- dall'art. 17 essendoci rischi specifici insiti per il tipo di trattamento omesso nell'ipotesi di cui al presente procedimento.

La ratio dell'introduzione nei sistemi penali moderni di norme come quelle di cui all'articolo 40 C.P., atte ad incriminare ipotesi di reato commissivo mediante omissione deve ricercarsi nella necessità di soddisfare esigenze dì politica criminale. Si tratta cioè di incriminare quei casi di mancato impedimento di

eventi lesivi che, pur non contemplati direttamente dalle varie legislazioni, si è ritenuto sostanzialmente eguagliassero quanto a disvalore penale le corrispondenti ipotesi di commissione di reato mediante azione positiva.

Un simile giudizio di equivalenza tra l'agire e l'omettere presuppone che il soggetto obbligato rivesta una posizione di garanzia nei confronti del bene protetto, che nel caso sottoposto all'esame del Giudice di primo grado si caratterizzava in una posizione di protezione secondo la dizione normativa del codice della privacy che parla di protezione dei dati personali.

Bisogna dare rilevanza agli interessi in gioco, ovvero quelli della tutela dei diritti fondamentali della persona nei confronti del diritto di iniziativa economica.

Il giudicante nella motivazione complessiva cade sul tema generale della possibilità degli ISP di effettuare un controllo preventivo delle innumerevoli serie di dati che passano nelle maglie dei gestori o proprietari dei siti web.

Nella realtà gli JSP avevano la possibilità di attuare dei controlli, si veda per esempio il Safe Search, che è un filtro automatizzato al quale possono essere uniti anche controlli effettati da persone.

Va ricordato che veniva accertato che il servizio G. Video veniva volutamente lanciato in Italia come servizio di libero accesso proprio dopo un'attenta analisi del mercato italiano ed in vista di una strategia commerciale volta all'acquisizione del competitor You tube.

Nella sostanza, l'azione doverosa quindi può essere ricostruita nella compiuta osservanza degli obblighi e dalle cautele previste dalla normativa relativa la trattamento dei dati personali.

Occorreva verificare se l'adempimento di quanto richiesto, ove complessivamente osservato, avrebbero impedito l'evento con una probabilità prossima alla certezza.

Così come la questione relativa alla violazione della normativa in materia di trattamento dei dati personali rilevante per il capo B) non si limitava all'adempimento dei soli obblighi informativi, anche l'obbligo giuridico di attivarsi rilevante ai sensi del capo A) va inteso nella sua accezione più ampia e laddove attuato avrebbe sicuramente impedito l'evento.

Il giudicante, nel percorso motivazionale relativo ad entrambi i capi di imputazione, si fermava ad un'analisi della normativa in materia di trattamento dati personali limitata agli obblighi di informativa. Si ritiene tuttavia che la stessa adesione del tribunale ai fatti così come così complessivamente ricostruiti dalle indagini dell'accusa avrebbe dovuto portare anche sotto il profilo del capo A) ad una sentenza di condanna sussistendo in capo a ciascuno degli imputati la prova dell'elemento psicologico richiesto, dolo diretto o eventuale.

Sulla inapplicabilità dei principi di responsabilità di cui alla direttiva sul commercio elettronico (dl.vo 70/2003).

Non vi è dubbio poi sulla prevalenza della normativa sulla protezione di dati personali oltre che nel dato costituzionale dell'art. 41 comma 2, trovi un ricono-

scimento testuale nell'art. 1 comma 2 lettera d) D.L.vo 70/2003, disposizione in linea con l'art. 1 comma 4 lettera b) della Direttiva 200/31/CE.

In effetti il servizio G. così come concepito deve essere qualificato come di hosting attivo, diverso dal servizio di mero hosting di cui all'art. 16 comma 1 Decreto citato.

Di fronte ad un servizio che per le sue caratteristiche operative si poneva nel mezzo tra la posizione di hosting provider e quella di content provider, ovvero di produttore in proprio di contenuti, si tratta di verificare quale possa essere il regime di responsabilità in concreto applicabile ed è la ratio dello stesso art. 16 già citato ad indicare univocamente che non si possono applicare all'hoster attivo le regole di minore responsabilità fissate dalla direttiva sul commercio elettronico; infatti tale disposizione prevede che in conformità con la previsione dell'art. 14 comma 2 Direttiva 200/3I/CE, il regime indicato dall'art. 16 non si applica se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore.

In questo caso il provider non agisce da mero intermediario ma è il soggetto che volontariamente decide quali informazioni trasmette e attraverso quali modalità, con la consequenziale applicazione della ordinarie norme sulla responsabilità.

4- L APPELLO PROPOSTO DAGLI IMPUTATI

Il difensore dell'imputato D.D.C. presentava appello avverso la sentenza, chiedendo:

- Riformarsi la sentenza appellata con assoluzione dell'imputato perché il fatto non sussiste o perché l'imputato non lo ha commesso o perché il fatto non costituisce reato.

- Rilevarsi il difetto di giurisdizione italiana, nonché l'assenza delle condizioni di procedibilità.

- Dichiararsi la nullità della sentenza di primo grado per difetto di correlazione con l'imputazione contestata ex art. 604 primo comma cpp. In subordine, ridursi la pena inflitta e sostituirsi la pena detentiva con quella pecuniaria. Concedersi il beneficio della non menzione della condanna ex art. 175 cp ed estendersi gli effetti della sospensione condizionale anche alla pena accessoria della pubblicazione della sentenza.

- In particolare il difensore rilevava che:

- La sentenza affermava erroneamente che il trattamento dei dati relativi al servizio G. Video veniva effettuato anche da G. Italy.

- La sentenza riteneva erroneamente che G. Italy attraverso il sistema AdWords avesse la possibilità i gestire i dati contenuti in G. Video in modo da trarvi un profitto.

- La sentenza in modo non condivisibile riteneva carente e nascosta l'informativa sulla privacy.

La sentenza erroneamente condannava l'imputato per il reato di cui all'art., 167 D.L.vo 196/2003.

La sentenza affermava la penale responsabilità dell'imputato sulla base di presupposti erronei.

La sentenza erroneamente riteneva applicabile il codice privacy a G. Video ravvisando la giurisdizione italiana D.D.C. doveva essere ritenuto non punibile per mancanza dei presupposti ex art. 10 CP.

La sentenza deve essere dichiarata nulla ex artt. 521 comma 2, 522 e 604 comma 1 CPP. Per difetto di correlazione con l'imputazione contestata.

Il difensore dell'imputato D.L.R.G. presentava appello avverso la sentenza, chiedendo:

a) In via preliminare, dichiararsi l'assenza delle condizioni di procedibilità ex art. 10 CP. o, in ogni caso, accogliere l'eccezione di incompetenza territoriale.

b) In via principale riformarsi la sentenza appellata con assoluzione dell'imputato perché il fatto non sussiste o per non aver commesso il fatto o perché il fatto non costituisce reato;

c) In via subordinata accogliersi gli altri motivi d'appello e in via ulteriormente subordinata concedersi il benefico della non menzione della condanna nel certificato del casellario giudiziale. In ogni caso ridursi la pena nei minimi con sostituzione della pena detentiva con quella pecuniaria prevista dall'art. 53 L. n. 689/81.

In particolare il difensore dell'appellante rilevava:

1) In sussistenza del reato di cui all'art. 167 Codice Privacy.

- La presunta violazione dell'obbligo di corretta informazione: in sussistenza in fatto e irrilevanza penale in diritto.
- I due trattamenti (G. Inc.- utente; utente- interessato)
- G. Inc. ha correttamente informato l'utente.
- Era l'utente che doveva acquisire il consenso dall'interessato.

2) G. Italy non trattava e non poteva trattare i dati del servizio G. Video e non ha effettuato alcun trattamento dei dati del D.L..

- Distinzione tra G. Italy srl e G. Inc.
- G. Italy non ha contribuito alla predisposizione della piattaforma informatica di G. Video.
- G. Italy e l'impossibilità tecnica di qualsiasi operazione di trattamento dati relativa al servizio G. Video.

3) G. Video era un servizio gratuito e non comportava profitto per G. Italy.

- Non era possibile inserire annunci del servizio AdWords sul servizio G. Video.
- Non vi era interazione commerciale operativa tra G. Video e G. Italy tramite il servizio AdWords.
- G. Italy non traeva alcun profitto dal servizio G. Video.

Il difensore dell'imputato F. P, A. presentava appello avverso la sentenza, chiedendo:

1) Assolvere l'imputato dal reato contestatogli sub B) perché il fatto non sussiste per erronea applicazione della legge penale e delle altre norme giuridiche di cui si deve tener conto nell'applicazione dell'art. 167 D.L.vo 196/2003.

- Il D.L.vo 70/2003
- Il D.L.vo 196/2003
- L'art. 167 Trattamento illecito dei dati
- L'art. 13 La motivazione della condanna

Il trattamento dei dati: le motivazioni dell'assoluzione

2) Assolvere l'appellante per non aver commesso il fatto per inconfigurabilità del reato di illecito trattamento di dati personali in capo agli imputati.

Erronea valutazione delle risultanze processuale in relazione all'inconfiguarabilità del reato di illecito trattamento in capo a G. Italy.

- AdWords.
- Il gruppo G..
- I link tra G. Italy e G. Inc.
- I precedenti delle Autorità.

3) Assolvere l'appellante per non aver commesso il fatto quale concorrente del reato contestato.

- In fatto: il ruolo di F.P.A. in G..
- In diritto: concorso omissivo nell'omesso trattamento.

4) In subordine riconoscere le già concesse attenuati generiche nella loro massima estensione ed in tal modo determinare la pena nei minimi edittali con conversione della stessa nella corrispondente pena pecuniaria ai sensi del combinato disposto degli artt. 53 D.P.R. 698/81- 135 C.p. e con riconoscimento del beneficio della non menzione della condanna nel certificato del casellario giudiziale ex art. 175 C.p.

5 - IL PROCESSO D'APPELLO

A seguito di emissione di decreto di citazione per l'udienza del 4/12/2012 avanti la Corte venivano depositate memorie difensive.

In data 16/11/2012 i difensori di D.D.C. insistevano nell'accoglimento delle conclusioni già formulate nell'atto d'appello principale e chiedevano in riforma della sentenza appellata l'assoluzione dell'imputato dal capo B) della rubrica perché il fatto non è previsto dalla legge come reato ovvero perché il fatto non costituisce reato.

In particolare lamentavano che con il percorso argomentativo il giudice di primo grado superava la mancanza nella norma incriminatrice contestata di un espresso richiamo all'art. 13 D.L.vo 196/2003.

E per tale ragione finiva per riscrivere tanto il contenuto letterale di quest'ultima norma quanto di quelle ex art. 167 Medesimo Decreto con il risultato della creazione di un nuovo precetto penale.

Ancora si dolevano ì difensori che non veniva accertata l'insussistenza dell'elemento soggettivo del reato contestato sotto il duplice profilo della carenza di dolo specifico e dell'inapplicabilità del dolo eventuale alla fattispecie incriminatrice di cui all'art. 167 Codice Privacy.

Nel processo l'accertamento del dolo specifico nella sua declinazione di fine di profitto, non poteva aver ad oggetto né i generici scopi economici di un sistema commerciale, né le sue generiche potenzialità lucrative.

Nella realtà la mancanza di un dolo specifico nel caso appariva in modo evidente sia dalla comprovata impossibilità dell'appellante di conoscere personalmente il contenuto del filmato e l'eventuale dato personale ivi incluso, sia dall'assenza di link pubblicitari associati a quel video.

Da ultimo il difensore evidenziava il problema di compatibilità del dolo eventuale con il dolo specifico in un reato di mera condotta quale quelle previsto nella fattispecie di cui all'art. 167 Legge Privacy.

In data 29/11/2012 congiuntamente tutti i difensori degli appellanti introducevano un parere pro veritate del Professor P., già presidente dell'Autorità Garante per la Protezione dei Dati Personali, le cui argomentazioni e conclusioni facevano proprie con particolare riferimento all'obbligo di informativa ex art. 13 Codice Privacy.

Tale obbligo infatti a parere degli scriventi riguarda sempre e soltanto il rapporto tra il titolare e coloro che sono direttamente interessati ai trattamenti che questo pone in essere.

In nessun caso per proprietà transitiva può invece riguardare terzi estranei al rapporto tra titolare e interessati, anche quando questi terzi siano oggetto di trattamenti posti in essere grazie ai servizi messi a disposizione dagli utenti.

Ed ancora il consenso rispetto ai dati di terzi presenti nei contenuti audiovideo ospitati e memorizzati dall'ISP in seguito all'attività degli utenti spetta a coloro che tali dati hanno raccolto e intendono farne oggetto di trattamento attraverso il loro caricamento sulla piattaforma di G. Video.

All'udienza del 4/12/2012, formalizzata la costituzione delle Parti dopo la relazione introduttiva venivano fissate per la discussione le udienze dell'11 e del 21/12/2012.

In data 13/12/2012 il PG depositava in Cancelleria memoria ex art. 121 C.C.P.

Nella stessa preliminarmente veniva chiarito il punto della insussistenza della mancanza di correlazione tra il capo di imputazione e il dispositivo della sentenza lamentata dai difensori degli appellanti, poiché l'illecito trattamento dei dati personali e sensibili è lo stesso fatto di reato descritto nel capo di imputazione e sviluppato in sentenza.

In particolare il capo di imputazione stabilisce la responsabilità degli imputati appellati per aver violato l'art. 167 della Legge Privacy, mediante il trattamento di dati sensibili al fine di trarne profitto senza aver fatto il preventivo controllo e senza le prescritte autorizzazioni.

Nel capo di imputazione sono citati gli artt. 23, 17, 26, mentre non è richiamato l'art. 13 del citato D.L.vo., indubbiamente interessante ma non rilevante per il processo.

La sentenza di primo grado ha esaurientemente dimostrato che il trattamento è avvenuto, che i dati trattati erano sensibili e che il consenso non è stato dato

né orale, né per iscritto, che non è stato chiesto alcun interpello al garante , che gli imputati in quanto titolari erano coloro che avrebbero dovuto prendere le opportune decisioni prima del trattamento con il dovuto controllo preventivo, che il controllo preventivo era possibile ma non è stato fatto, e che il trattamento è stato fatto al fine di trarne profitto.

Il D.L.vo. 70/03 invocato dalle difese nel caso non è applicabile in quanto l'art. 1 esclude che nel campo di applicazione del presente decreto le questioni relative al diritto alla riservatezza con riguardo al trattamento dei dati personali nel settore della comunicazione di cui alla legge 675 e al D.L.vo. 171/98

Gli appelli degli imputati sostengono che G. non era tenuta a nessun controllo in quanto Internet Provider e quindi obbligata solo a fornire le necessarie avvertenze delle norme esistenti a tutti gli utenti del servizio.

In effetti questa definizione di G. come semplice internet provider sembrerebbe fatta propria dalla sentenza di primo grado ma, questa definizione è sbagliata perché G. non è un semplice host provider in ragione dei numerosi servizi aggiuntivi offerti, per esempio le miniature e i sistemi di raffinazione della ricerca. G. quindi non è responsabile per mancata o insufficiente informazione ma per mancanza di controllo, controllo che doveva fare in quanto responsabile di trattamento e che veniva omesso perché costoso.

La visione di questo video e dei filmati che apparivano su G. Video era fonte di guadagno per G. quindi la finalità di lucro di cui all'art. 167 D.L.vo cit. è sussistente ed è provata dai documenti sequestrati nella sede di G. Italy e dalla dichiarazione dei suoi responsabili.

Si sostiene ancora nei motivi d'appello che il controllo non era possibile ma questa affermazione non corrisponde al vero sulla base delle risultanze della perizia B..

Gli appellanti sostengono la carenza di legittimazione passiva dei tre imputati ma, anche sotto questo profilo la sentenza merita piena conferma, in quanto dall'istruttoria svolta e dai documenti rinvenuti nella sede originaria, G. Italy è stata costituita il 22/08/2002 e qualunque questione organizzativa veniva decisa su preciso mandato dei legali rappresentanti, che non hanno mai delegato operativamente nessun altro soggetto rispetto al territorio italiano.

In sostanza G. Italy era un mera esecutrice delle decisioni prese dalla casa madre G. Inc., ed è assolutamente contrario al materiale probatorio acquisito sostenere un'autonomia di G. Italy o di G. Video.

Al termine il P.G. si riportava alle conclusioni già prese in sede di requisitoria finale in data 11/12/2012 e, vista la intervenuta remissione di querela da parte dell'associazione Vivi Down, concludeva con la richiesta di declaratoria di non doversi procedere in ordine al capo A) remissione di querela, e la conferma nel resto della sentenza impugnata.

In data 19/12/2012 i difensori degli appellanti sottoponevano all'attenzione della Corte memoria ex art. 121 C.P.P.

Nella stessa veniva evidenziato come la legge sulla privacy e la legge sul commercio elettronico costituiscano un sistema normativo armonico in grado di

fornire una piena regolamentazione alla vicenda in esame e pertanto non è possibile creare inesistenti e ulteriori obblighi di controllo preventivo a carico dell'ISP così come sostenuto dall'accusa.

A parere degli scriventi poi, nel caso di G. e nel caso di G. Video andava applicata la legge sul commercio elettronico.

In base alla legge sul commercio elettronico, il fornitore di un servizio di hosting non è responsabile delle informazioni memorizzate, a condizione che non sia effettivamente a conoscenza del fatto che l'attività o l'informazione sia manifestamente illecita e che non appena a conoscenza di tali fatti, a seguito di comunicazione delle autorità competenti, non agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

Ammesso e non concesso che G. Video nel 2006 fosse un hosting provider attivo doveva comunque applicarsi la normativa sul commercio elettronico sulla base della quale non esiste e non è esigibile un obbligo di controllo preventivo dei contenuti.

Tale interpretazione a parere degli scriventi veniva confermata a livello europeo da due recenti pronunce della Corte di Giustizia del 2012 ove si specifica che l'art. 15 par. 1 della direttiva 2000/31 vieta alle autorità nazionali di adottare misure che impongano ad un prestatore di servizi di hosting di procedere ad una sorveglianza generalizzata sulle informazioni che esso memorizza.

Nel caso di specie, poi non vi era alcun conflitto tra la legge del commercio elettronico e la disciplina della privacy poiché G. non poteva essere considerato titolare dei dati inerenti le persone riprese nei video caricati da terzi, che si limitava ad ospitare.

Sempre secondo gli appellanti l'accusa poi imputava a G. la mancata effettuazione di asseriti controlli, non tenendo conto che gli stessi non erano nemmeno tecnicamente possibili.

Per trarre le giuste conclusioni infine il caso di specie andava ripensato nel suo complesso. Dallo stesso episodio infatti nascevano tre procedimenti penali.

Nel primo i ragazzi che trattavano i dati illecitamente sono stati condannati per violazione dell'art. 167

Legge Privacy.

Nel secondo procedimento chi aveva l'obbligo di impedire il fatto illecito altrui, ossia l'insegnante dei ragazzi, è stata condannata.

Nel terzo procedimento non essendo G. titolare del trattamento dei dati del D.L., in forza della legge sul commercio elettronico, non poteva essere condannata, in quanto prontamente rimuoveva il video dopo la segnalazione ricevuta da parte dell'autorità.

L'accusa poi non poteva essere che ritenuta tanto più infondata poiché coinvolgeva un soggetto, G. Italy Srl, e segnatamente i suoi amministratori che non svolgevano ruoli esecutivi e che non avevano relazioni con il servizio G. Video.

In nessun caso infatti G. Italy poteva dirsi coinvolta nell'attività dei trattamenti dei dati relativi al servizio G. Video.

Oltre a quanto sopra secondo gli appellanti doveva rilevarsi poi che, contrariamente a quanto sostenuto dall'accusa, all'epoca dei fatti non era possibile posizionare AdWords su G. Video.

Ancora gli appellanti insistevano nell'evidenziare che la prova più importante della debolezza dell'accusa poteva facilmente cogliersi nella contraddittorietà della motivazioni che venivano di seguito poste alla base della sentenza di condanna.

In effetti il capo di imputazione nel caso poggiava su ragioni smentite dalla sentenza di primo grado, che a sua volta veniva ampiamente criticata non solo dalla dottrina italiana che l'ha analizzata ma anche dalla stessa Procura Generale che forniva nuove e diverse argomentazioni a sostegno delle richieste formulate in sede di appello.

La Difesa da ultimo insisteva nella richiesta di assoluzione di tutti gli imputati da tutte le imputazioni loro ascritte anche dal punto di vista della insussistenza dell'elemento psicologico del reato.

Non risultava infatti possibile comprendere quale fosse il comportamento doveroso che gli imputati avrebbero dovuto tenere nella sostanza; informare l'utente che non avrebbe dovuto violare la privacy altrui o invece effettuare controlli preventivi.

Non poggiando la sentenza di primo grado su solide basi di diritto e apparendo contraddittorie le argomentazioni motivazionali si concludeva per l'assoluzione.

In data 21/12/2012 il difensore dell'appellante D.D.C., depositava note di udienza, chiedendo la dichiarazione di inammissibilità dell'atto di appello presentato dalla Procura della Repubblica in relazione al delitto di diffamazione di cui al capo A) della rubrica.

Questo considerato che l'appellante veniva assolto dal giudice di primo grado dal reato di cui al capo A) perché il fatto non sussiste, che in data 29/06/2010 la Procura proponeva appello chiedendo in riforma della pronuncia di prime cure la condanna degli imputati anche in relazione al reato di cui al capo A) e che in data 7/07/2010, la residua parte civile costituita dall'Associazione Vivi Down, provvedeva a rimettere la querela sporta in data 9/11/2009.

L'intervenuta remissione della querela comportava ex lege l'estinzione del reato con doverosa dichiarazione di inammissibilità dell'impugnazione per sopravvenuta carenza di interesse.

Nell'udienza del 21/12/2.012, conclusi gli interventi delle Parti con le richieste di cui a verbale, la Corte, all'esito della camera di consiglio, ha dato lettura del dispositivo in atti.

Motivi della decisione

La sentenza va riformata limitatamente al capo B) della rubrica in relazione al quale tutti gli imputati devono essere assolti con la formula perché il fatto non sussiste.

Quanto all'imputazione di cui al capo A) ritiene la Corte che l'appello proposto dal PM non fornisce elementi di ordine logico o probatorio che consentano di discostarsi dalla decisione di primo grado, sul punto del tutto condivisibile, in quanto risulta rispondente alle acquisite risultanze processuali e sorretta da congrua motivazione in fatto oltre che in diritto; motivazione che deve considerarsi qui integralmente richiamata secondo il principio della reciproca integrazione delle sentenze di primo e di secondo grado, in caso di conferma.

Alle considerazioni già svolte dal Giudice di prime cure, sembra doversi aggiungere solo che per sostenere la responsabilità a titolo di omissione in capo ad un host o content provider, occorre affermare a suo carico un obbligo giuridico di impedire l'evento e quindi da un lato, l'esistenza di una posizione di garanzia, dall'altro la concreta possibilità di effettuare un controllo preventivo.

Detta posizione di garanzia però, concordemente a quanto già sostenuto dal Giudice di primo grado, non può essere ravvisata nel diritto vigente, stante l'assenza di una specifica previsione in tal senso, e ciò a prescindere dalla questione dell'auspicabilità o meno di una normativa che colmi questo vuoto legislativo.

Né la posizione di garanzia di cui trattasi può desumersi da fonte diversa, quale in via esemplificativa quella dettata ex art. 57, e 57bis C.P. in materia di stampa, in quanto si tratterebbe di analogia in malam partem.

Quanto al secondo aspetto preso in considerazione, si osserva che non può essere ravvisata la possibilità effettiva e concreta di esercitare un pieno ed efficace controllo sulla massa dei video caricati da terzi, visto l'enorme afflusso di dati.

Non può non vedersi come l'obbligo del soggetto-web di impedire l'evento diffamatorio, imporrebbe allo stesso un filtro preventivo su tutti i dati immessi in rete, che finirebbe per alterarne la sua funzionalità.

Considerata l'estrema difficoltà tecnica di tale soluzione, e le conseguenze che potrebbero derivarne, appare quindi condivisibile anche la conclusione a cui perveniva il Tribunale secondo cui si finirebbe per richiedere un comportamento inesigibile e di conseguenza non perseguibile penalmente ai sensi dell'art. 40 cpv C.P.

Per completezza a quanto già esposto, valga solo aggiungere che la presenza di una posizione di garanzia da cui far derivare un obbligo di attivazione, in mancanza della quale far ricorrere la previsione dell'art. 40 C.P., di certo non può essere fatto derivare dalla violazione di norme di legge quali quelle a protezione dei dati personali, che non hanno per oggetto tali condotte e che sono state emanate a copertura di comportamenti diversi da quelli oggetto di contestazione.

Insisteva ancora l'Accusa ricordando che secondo l'insegnamento della Suprema Corte, una posizione di garanzia può derivare da una fonte normativa di diritto pubblico o privato anche non scritta, ma anche da: "una situazione di fatto per precedente condotta illegittima, che costituisca il dovere di intervento" ed anche può derivare: "dall'esistenza di un potere giuridico o di fatto, attraverso il

corretto uso del quale, il soggetto garante sia in grado di attivandosi di impedire l'evento". (Cassazione Sezione IV n° 32298 del 06/07/2006).

Occorre sottolineare però, che neppure sotto questo profilo la tesi accusatoria, secondo cui in sostanza la responsabilità degli imputati deriverebbe dal mancato controllo preventivo sul contenuto dei video, attuabile attraverso l'attivazione di tutti i filtri disponibili, pare condivisibile in quanto anche l'attivazione di tali dispositivi non sarebbe comunque efficace, a causa dei limiti degli strumenti tecnici, tanto più di quelli utilizzabili al tempo dei fatti.

In effetti va escluso, così come sostenuto e documentato dalla difesa degli appellanti, che nel periodo settembre - dicembre 2006 fosse esistente ed operante una tecnologia di filtraggio preventivo compiutamente idoneo ad identificare automaticamente i contenuti illeciti di un video.

Oltre alle argomentazioni sopra esposte, questa Corte non ritiene poi, possa essere trascurata la linea dettata dalla Suprema Corte, secondo cui in materia di concorso di persone la condotta consistente nel non impedire l'evento, che si ha l'obbligo giuridico di impedire, deve essere accompagnata dal dolo che caratterizza il concorso stesso, da ravvisarsi nella coscienza e volontà di concorrere con altri nella realizzazione del reato.

Sulla base di tutto quanto sopra esposto non resta dunque quanto al capo A) che pervenire al medesimo giudizio di assoluzione già espresso.

Sempre a proposito del capo A), il fatto che dopo la sentenza di primo grado, in data 07/07/2010, la residua Parte Civile, Associazione Vivi Down, abbia rimesso la querela sporta in data 09/11/2009 in ordine al reato di diffamazione - remissione che veniva ritualmente accettata da tutti gli imputati – non comporta poi, a parere di questa Corte, l'inammissibilità dell'appello proposto dal P.M., così come eccepito dalla difesa di D.D.C..

Questo in quanto la richiesta finale del P.G. di non doversi procedere in relazione al capo A) per intervenuta remissione di querela, indubbiamente costituisce una richiesta di reformatio in peius della sentenza di primo grado.

Trattasi comunque di questione che rimane assorbita dalla decisione di conferma della statuizione di primo grado ampiamente assolutoria nel merito perché il fatto non sussiste.

Non ci si può esimere, prima di passare ad esporre le ragioni per cui questa Corte ritiene che in riforma di quanto deciso in primo grado, gli imputati debbano essere assolti dalla imputazione loro mossa al capo B), offrire preliminarmente alcune brevi considerazioni generali.

Innanzitutto non vi è dubbio che lungi dal "molto rumore per nulla", secondo la citazione utilizzata dalla sentenza di primo grado, ci si trovi di fronte a una vicenda molto complessa, non tanto per la massa delle risultanze della notevole attività istruttoria svolta, per le ingenti produzioni delle parti e per gli estesi e puntuali interventi proposti dalla stesse a sostegno delle rispettive tesi, quanto perché attiene alla questione del governo di internet.

Di seguito non pare potersi procedere oltre seguendo un ordine logico, senza affrontare il tema della giurisdizione.

Per quanto riguarda la competenza territoriale, la sentenza di primo grado rimandava all'ordinanza presa dal giudicante in data 21 Aprile 2009.

Quindi, esaurita la fase dibattimentale, sosteneva la permanenza dell'assenza di qual si voglia dubbio sulla competenza della A.G milanese, in relazione al reato sub B) ai sensi degli artt. 8 e 9 C.P.P., essendo stato il reato in questione commesso almeno in parte nel nostro Paese, a Milano, dove ha sede G. Italy responsabile del comportamento incriminato e cioè del trattamento dei dati inteso come elaborazione ed organizzazione dei video caricati in G. Video.

Quanto al profilo in oggetto, le doglianze mosse dalla difesa degli appellanti, sono infondate in quanto ai fini della sussistenza della giurisdizione italiana, concordemente a quanto puntualmente sostenuto dall'ufficio del PM, non appare rilevante il luogo in cui sia collocato il server sul quale vengono caricati i video, dovendosi avere riguardo la luogo in cui si sono verificati gli effetti pregiudizievoli dell'illecito.

Vedi art. 5.3 della Convenzione di Bruxelles del 27/09/68 come interpretato dalla consolidata giurisprudenza della Corte di Giustizia.

L'evento del caricamento del server, ammesso che si verifichi negli U.S.A., è di per sé solo potenzialmente generatore di danno, ma privo di efficacia dannosa, che si verifica solo nel momento in cui i contenuti vengono diffusi nell'area di mercato ove la parte danneggiata esercita i suoi diritti, nella specie appunto il territorio italiano.(Cfr. Trib. Di Roma - Sez. IX Civile Ord. 15-l6/dic./2009- Cass. Sez. III n. 49437/09 del 29/09/09).

D'altra parte non fa venire meno la giurisdizione del giudice nazionale, neppure la circostanza che la condotta di partecipazione sia stata posta in essere all'estero quando una parte della condotta comune abbia luogo in Italia.(Cfr. Cass. Sez. V 09/07/2008-20/10/2008 n. 39205)."Il giudice italiano rimane competente a conoscere della diffamazione, compiuta mediante l'inserimento nella rete telematica internet, di frasi offensive e/o immagini...anche nel caso in cui il sito web sia stato registrato all'estero purché l'offesa sia stata percepita da fruitori che si trovano in Italia.(Cfr. Cass. Sez. V 17/11/2000-27/12/2000 n. 4741).

Per quanto riguarda la problematica relativa alla legittimazione passiva degli imputati D., D.L.R., F., la Corte trova ineccepibili le conclusioni a cui perveniva l'Accusa sulla base dei complessivi atti di indagine richiamate nella memoria ex 121 C.P.P. del PM e riportate nella sentenza di primo grado.

Secondo le stesse, D. risultava essere Vicepresidente e Legale rappresentante di G. Inc, nonché Vicepresidente di G. International, ovvero il vertice proprio delle due società detentrici delle complessive quote sociali di G. Italy srl, società costituita a Milano il 27/08/2002.

Nel caso dunque, al di là del concetto delle scatole cinesi evocato dal P.G., non può non vedersi la sussistenza di un accentramento organizzativo nelle mani degli amministratori americani.

D'altra parte sempre al medesimo proposito, va evidenziata anche la significativa circostanza della mancata nomina da parte della casa madre, di qualsiasi

altro rappresentante delle società G. Italy e G. Video, stabilito nel territorio dello Stato.

A partire dal 2006 il servizio G. Video veniva localizzato in Europa e poi in Italia a partire dal 12/07/2006.

Essendo A. il responsabile del progetto G. Video per tutta l'Europa con gestione rispetto all'Italia a cura di G. Italy srl.

Occorre a questo punto solo sottolineare che essendo G. Italy srl soggetto giuridico stabilito nel territorio della Stato, nei suoi confronti trova applicazione la disciplina in materia di dati personali ex art. 5 comma 1 Codice Privacy.

Ove poi si ritenga che il luogo di stabilimento rilevante ai sensi del Codice Privacy possa non essere individuato, rispetto alla sede milanese, rimane comunque applicabile l'articolo 5 comma 2 D.L.vo che menziona gli " strumenti situati nel territorio dello Stato anche diversi da quelli elettronici" in quanto non vi è dubbio che dalla società in oggetto nel nostro paese, sia stata creata nel tempo una struttura organizzativa ben rientrante nella nozione di "strumento anche non elettronico".

Salvo quanto verrà meglio illustrato in seguito, pare poi pienamente rientrare nell'attività complessivamente posta in essere da G. Italy in relazione ai dati immessi nel sistema di G. Video, la nozione di trattamento prevista dall'art. 4 del medesimo D.L.vo.

E valga a conferma di quanto sopra, richiamare il parere del Gruppo per la tutela dei dati personali WP29, inviato con lettera proprio all'imputato F., in cui veniva precisato che "nonostante il centro direzionale di G. si trovi negli Stati Uniti, G. ha l'obbligo legale di attenersi alle leggi europee, ed in particolare alle normative sulla privacy, dato che i servizi di G. vengono forniti a cittadini europei e che svolge le attività di trattamento dati in Europa".

Molto si è detto in merito ad uno dei punti essenziali della vicenda processuale e cioè se G. Video possa essere considerato mero host provider o altro.

Decisione particolarmente rilevante, poiché, secondo la tesi della difesa degli appellanti, da questo discenderebbe la sostanziale irresponsabilità del provider, in ragione dell'applicazione degli artt. 16 e 17 D.L.vo 70/03.

L'evoluzione della rete informatica mondiale sembra però avere superato nei fatti la figura di mero prestatore di servizio, che veniva elaborata all'epoca della citata direttiva e che delineava tale soggetto come del tutto estraneo rispetto alle informazioni memorizzate, sia a livello di gestione che di regolamentazione contrattuale con i destinatari del servizio.

Oggi, i servizi offerti dall'Ip non si limitano al processo tecnico che consente di attivare e di fornire l'accesso alla rete ma, come nel caso del content provider, arrivano ad offrire la possibilità di immettere contenuti propri o di terzi nella rete e dunque non possono non essere chiamati a rispondere secondo le comuni regole di responsabilità in materia di trattamento dei dati.

Valga specificare poi che veniva delineata un'ulteriore categoria denominata di hosting attivo, cioè di prestatore di servizi non neutra rispetto all'organizzazione ed alla gestione dei contenuti degli utenti, caratterizzata an-

che dalla possibilità di un finanziamento economico attraverso l'inserimento di inserzioni pubblicitarie.

Questa categoria in realtà, non è presente in alcuna norma di legge ma risulta fondata su una costatazione fattuale del ruolo svolto dall'Ip, e' frutto dell'elaborazione di numerose pronunzie in materia di responsabilità.

L'organizzazione dei servizi pubblicitari non può, certo, come correttamente sostenuto dall'accusa ed in sentenza, essere considerato un dato irrilevante rispetto alla verifica da compiersi, sia nella prospettiva della giurisdizione, sia in quella del rapporto con l'eventuale illiceità del contenuto del materiale immesso dagli utenti.

Orbene tutti gli elementi valutati nel caso - la possibilità del filtraggio, della rimozione, dell'individuazione di contenuti tramite parole chiave, dell'indicizzazione dei contenuti e della eventuale utilizzazione a fini pubblicitari - portano a ritenere che G. Video non possa che essere qualificata quantomeno come un hosting attivo.

In effetti va escluso che G. Video, in quanto capace di organizzare e selezionare il materiale trasmesso dagli utenti possa continuare ad insistere nella sua pretesa neutralità.

Detto ciò, come già sostenuto in sentenza e come già anticipato in premessa rispetto all'imputazione di cui al capo A), va esclusa, anche per il prestatore di servizi che fornisca hosting attivo, la possibilità ipso facto di procedere ad una efficace verifica preventiva di tutto il materiale immesso dagli utenti.

Come si è già osservato, tale comportamento non può essere ritenuto doveroso, in quanto non esigibile per la complessità tecnica di un controllo automatico e comunque, demandare ad un internet provider un dovere/potere di verifica preventiva, appare una scelta da valutare con particolare attenzione in quanto non scevra da rischi, poiché potrebbe finire per collidere contro forme di libera manifestazione del pensiero.

Da ultimo, appare opportuno a conclusione dell'argomento, richiamare le considerazioni finali svolte dal Giudice di prime cure, per la loro linearità e chiarezza.

"È ovvio che l'hoster attivo o il content provider che dir si voglia avrà certamente un livello di obblighi più elevato di quello di un semplice host provider o service provider o access provider, lo rende inevitabile il suo divenire dominus dei dati che, per il solo fatto di essere organizzati e quindi selezionati e quindi appresi non sono più il flusso indistinto che non si conosce e che non si ha l'obbligo di conoscere; ma tale fatto non crea una specie di effetto catena che fa dell'hoster attivo automaticamente il corresponsabile di tutti i reati che gli uploaders hanno commesso comunicando e caricando dati sensibili."

Agli imputati veniva contestato al capo B) della rubrica il reato di illecito trattamento di dati personali, per avere in concorso tra loro e nelle circostanze di fatto di cui al precedente capo, al fine di trarne profitto, proceduto al trattamento dei dati personali di D.L.F.G., con violazione degli artt. 23, 17 e 26 stesso D.L.vo, con relativo nocumento della persona interessata.

Tale prospettazione accusatoria però, risultava da subito problematica in ragione della modifica dell'impostazione operata, sia dall'appellata sentenza, sia successivamente dal PG nella sua requisitoria e nella sua memoria ex artt. 121 C.P.P.

In effetti dalla motivazione della sentenza, la responsabilità degli imputati in relazione al capo d'imputazione in oggetto si esclude possa discendere da una posizione di garanzia con conseguente obbligo preventivo di sorveglianza sui contenuti di quanto immesso in rete, per assenza di un tale obbligo preventivo e per la sua inesigibilità, ma viene fatta, invece, derivare dalla carenza di una corretta puntuale e doverosa informazione agli utenti delle norme poste a tutela della privacy, ex art. 13 D.L.vo citato.

Orbene, data questa premessa non pare possibile non cogliere l'incongruenza della scelta operata dal Giudice di primo grado, costituita dal fatto che il citato art. 13 non è neppure richiamato nel testo dell'art. 167 in questione.

La norma di cui all'art. 167 appare caratterizzata dalla tipicizzazione della condotta penalmente rilevante in quanto richiede esplicitamente che l'autore del reato abbia agito non rispettando le disposizioni indicate.

E nessuna di queste disposizioni impone all'Internet Provider, di rendere edotto l'utente circa l'esistenza ed in contenuti della legge della privacy, pertanto quanto sostenuto in sentenza, anche se di "buon senso" non si ritiene, possa essere condiviso.

Va detto inoltre, che dalla lettura della normativa di cui trattasi, l'eventuale violazione dell'art. 13, ovvero l'omessa o inidonea informativa all'interessato, testualmente non viene sanzionata dall'art. 167, bensì dall'art. 161 Legge Privacy.

La sentenza prosegue esponendo gli elementi essenziali del reato:

a) l'avvenuto trattamento dei dati sensibili di una persona.

b) Il mancato consenso da parte del soggetto.

c) Il nocumento della persona offesa.

d) Il dolo specifico da parte del soggetto agente.

Quanto sopra però, senza procedere, come lamentato dalle difese, ad analizzare il concetto di titolarità del trattamento.

La responsabilità per il trattamento dei dati è legata al mancato adempimento di specifiche condizioni che rendono lecito l'uso di tali dati, ma tali condizioni non possono che essere messe in capo al titolare, al "controller" dei dati medesimi.

In effetti trattare un video, acquisirlo, memorizzarlo, cancellarlo, non può significare di per sé trattamento di dati sensibili.

Esistono due distinte modalità di trattare dei dati che non possono essere, a parere di questa Corte. considerati in modo unitario.

Trattare un video non può significare trattare il singolo dato contenuto, conferendo ad esso finalità autonome e concorrenti con quelle perseguite da chi quel video realizzava.

Sarà il titolare del trattamento ad avere l'obbligo di acquisire il consenso al trattamento dei dati personali.

Nel caso, toccava a G.L., l'uploader che caricando il video si assumeva la responsabilità del trattamento dei dati personali del D.L., chiedere ed ottenere il consenso prescritto e tale soggetto doveva ricevere l'informativa sugli obblighi di legge da parte di G..

Cfr. in senso conforme Cass. Pen. Sez. 3 17/11/2004-15/02/2005 n.5728.

Anche la Corte di Giustizia Europea, in un caso di pubblicazione di dati personali su internet, ha ritenuto titolare del trattamento il soggetto che aveva provveduto all'uploading, "...è la persona che crea, invia o carica i dati on line che deve essere ritenuto il titolare del trattamento dati e non la parte, il provider che fornisce gli strumenti".

Non è superabile neppure dalla presenza del video per un considerevole periodo nelle classifiche predisposte, il fatto che il prestatore di servizio G. Video, non aveva la contezza del contenuto del video, né poteva essere in grado di apprezzare la presenza di un dato sensibile non lecitamente trattato.

D'altra parte è pacifico che la valutazione dei fini di un'immagine all'interno di un video in grado di qualificare un dato come sensibile o meno, implica un giudizio semantico e variabile che certamente non può essere delegato ad un procedimento informatico.

E sul punto si veda anche quanto affermato nella sentenza di primo grado secondo cui non può essere considerato punibile chi raccolga, utilizzi o diffonda dati, che in buona fede debba o possa considerare come lecitamente raccolti da altri in quanto "...sarebbe impossibile pretendere che un'Isp possa verificare che in tutte le migliaia di video che vengono caricati in ogni momento siano stati rispettati gli obblighi concernenti la privacy di tutti i soggetti negli stessi riprodotti".

Ad abundantiam, va sottolineato che nella normativa sul commercio elettronico, che costituisce unitamente alla normativa sulla privacy un quadro giuridico coerente e completo, e che non può essere letta in modo alternativo ma integrato, si indica che: " il prestatore non è responsabile delle informazioni memorizzate...a condizione che detto prestatore non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita...e che non agisca immediatamente per rimuovere le informazioni medesime".

Questa Corte poi, ricorda di essersi già diffusa quanto all'assenza in capo al prestatore di servizi, che fornisca anche un hosting attivo, di un obbligo di controllo preventivo del materiale immesso sotto il profilo della inesigibilità della condotta.

Valga solo dunque, rispetto a quest'ultimo punto, aggiungere che la relazione al Parlamento Europeo in merito alla responsabilità giuridica degli intermediari Internet dell'08/06/2000, addirittura vieta, tenendo a mente l'art. 15 del D.L.vo 70/03, "...agli Stati membri di imporre agli intermediari Internet l'obbligo generale di controllare le informazioni che si trasmettono o si archi-

viano ovvero l'obbligo generale di cercare attivamente fatti o circostanze atte a indicare il proseguimento di attività illegali".

Quanto sopra non può che essere condiviso laddove non si trascuri di porre attenzioni alle difficoltà che ancora oggi permangono in materia di una efficace tecnologia in grado di filtrare informazioni illegali e nocive, senza bloccare informazioni perfettamente legali.

Ancora la Corte rileva, che mentre il riferimento all'art. 110 C.P. esplicitato quanto al capo B) di imputazione, prevede una partecipazione attiva nel reato da parte degli imputati, la sentenza ed in parte l'Accusa, finiscono per ravvisare un concorso costituito da una condotta omissiva.

Sotto questo profilo deve però evidenziarsi che trattandosi di reato di pura condotta, non possono ravvisarsi i presupposti per pervenire su queste basi ad un giudizio di responsabilità essendo la sfera dell'art. 40 comma 2 C.P. limitata ai reati di evento.

Ulteriore imprescindibile argomento, ostativo al giudizio di colpevolezza espresso in primo grado, è costituito dall'insussistenza dell'elemento soggettivo del reato contestato.

Prima di tutto infatti si osserva che non può essere condivisa l'ottica dell'estensore della sentenza di primo grado nel momento in cui confonde il dolo specifico con il fine di profitto costituito dalla palese vocazione economica dell'azienda G.. (Cfr. in senso conforme Cass. III Sez. n. 1464/12 del 24/05/2012).

L'attività dell'azienda nei suoi molteplici servizi non può che essere considerata lecita e non può essere assunta a prova della sussistenza del dolo.

In conclusione va escluso che nel caso possa essere rinvenuto il dolo specifico richiesti dalla norma, mancando qualsiasi riscontro di un vantaggio direttamente conseguito dagli imputati, in conseguenza della condotta tenuta, tanto più nell'ambito di un servizio gratuito quale era G. Video ed in assenza di link pubblicitari associati allo specifico video, oggetto del procedimento.

La mancanza di un dolo specifico emerge poi dalla ragionevole certezza che gli imputati non fossero preventivamente a conoscenza del contenuto del filmato e dell'immissione del dato personale non lecitamente trattato. Cfr. In senso conforme Cass. S.U. 27/03/2008 in Cass. Pen. 2008 n.12. e Cass. Sez. IV 18/09/2009 n.47997 Rv. 245742.

Si pone da ultimo un problema di compatibilità tra la forma del dolo eventuale - individuata in capo agli imputati nella sostanza per avere serbato una " voluta disattenzione" nelle politiche societarie relative al trattamento della privacy, al fine dell'ottenimento di buoni risultati di mercato - ed il dolo specifico richiesto dalla norma in oggetto.

La soluzione in senso positivo, non appare accettabile, in quanto la struttura della fattispecie di cui all'art. 167 Codice privacy postula la necessaria partecipazione psichica intenzionale e diretta del soggetto al raggiungimento di un profitto. (Cfr. In senso conforme Cass. Sez. I 14/10/94 C. in Cass. Pen. 1996, 2177).

Quanto sopra argomentato consente di ritenere assorbite tutte le altre numerose questioni sollevate dagli appellanti in ordine alle specifiche responsabilità con riferimento alle cariche rivestite all'interno del gruppo, rispetto alle quali comunque la Corte ha già offerto alcune considerazioni.

Pertanto l'impugnata sentenza deve essere riformata limitatamente al capo B d'imputazione, con conferma nel resto come da dispositivo che segue.

Ricorrono i presupposti di legge per la fissazione del termine di giorni 60 per il deposito della motivazione.

P.Q.M.

Visto l'art. 605 c.p.p. in parziale

RIFORMA

della sentenza emessa dal Tribunale di Milano del 24/02/2010

ASSOLVE

D.D.C. D.L.R.G. F.P.A. dall'imputazione a loro ascritta al capo B) perché il fatto non sussiste.

CONFERMA

nel resto l'impugnata sentenza.

Fissa in giorni 60 il termine per il deposito delle motivazioni.

La vicenda Google Vividown

di David Terracina (*)

1. Introduzione.

Con la sentenza n. 8611/2013, la Corte d'Appello di Milano ha probabilmente scritto la parola definitiva sulla vicenda giudiziaria che ha visto coinvolto uno dei più importanti operatori della Rete, e che aveva portato, nel giudizio di primo grado, alla condanna di alcuni suoi dirigenti per violazione della normativa sulla *privacy* ([1]). Si è trattato del primo caso in cui è stata riconosciuta la responsabilità penale di un *Internet provider* (IP), che non fosse anche *Content Provider*, per i dati diffusi da soggetti terzi e, proprio per tale ragione, la pronuncia di primo grado aveva avuto una notevole eco mediatica, non solo in Italia, innescando polemiche e riflessioni a vari livelli ([2]).

Da parte degli utenti della Rete la decisione del giudice di Milano veniva percepita come un'intollerabile minaccia alla libertà di manifestazione del pensiero, che trova in *Internet* la sua massima espressione. A ben vedere, però, il c.d. "popolo del *Web*" non aveva colto pienamente il senso e la portata della sentenza nei suoi profili strettamente tecnico-giuridici (comunque censurati in appello), in cui ci si era sostanzialmente limitati a stabilire una responsabilità dell'IP ai sensi del d.lgs. 196/2003 (c.d. codice della *privacy*), senza riconoscere alcun obbligo di controllo delle informazioni gestite e, dunque, senza riconoscere in capo allo stesso l'esercizio di alcun potere/dovere di censura.

Diversa la reazione da parte degli operatori del diritto i quali, prendendo spunto dal caso di specie, effettivamente circoscritto alla sola violazione della normativa sulla *privacy*, hanno esteso la riflessione al più generale problema della responsabilità penale dell'IP. Come se ad interessare non fosse tanto la condanna inflitta ai dirigenti di Google, quanto che si fosse minacciata l'indipendenza di uno dei principali operatori della Rete e, dunque, della Rete in generale ([3]).

(*) In *Indice penale*.

([1]) Si tratta, come commentato da una parte della dottrina, di un vero e proprio *leading case*, dal momento che è la prima volta che in Italia viene affermata la responsabilità penale di un *Internet Provider* a livello omissivo (Manna, *La prima affermazione, a livello giurisprudenziale, della responsabilità penale dell'*Internet provider: *spunti di riflessione tra diritto e tecnica*, in *Giur. cost*., 2010, 2, 1856).

([2]) Oltre all'eco mediatica, il caso Goole-Vividown aveva rischiato di creare un incidente diplomatico tra Italia e Stati Uniti (si veda, in proposito, Pezzella, *Google Italia, diffamazione e riservatezza: il difficile compito del provider (e del giudice)*, in Giur. mer., 2010, 9, 2232).

([3]) Scriveva, in proposito, una parte della dottrina che "*questa sentenza non è solo una sentenza sulla* privacy*… La sentenza che qui si pubblica è una sentenza che, in concreto, può gravemente pregiudicare la libertà della rete, rovesciando il sistema di responsabilità di chi, servendosi della rete, commette fatti illeciti… Questa sentenza va letta come una sentenza sulla responsabilità dei motori di ricerca, degli operatori non strutturati e, quindi, sulla responsabilità dei* provider" (Franceschelli, *Sul controllo pre-*

Il timore diffuso era, infatti, che la sentenza del giudice di Milano potesse costituire lo spunto ed il via per uno sviluppo giurisprudenziale e normativo che facesse da sponda alle tendenze liberticide provenienti da più parti ([4]).

A prescindere, però, delle riflessioni su alcuni aspetti tecnici – approfonditi dalla Corte d'Appello di Milano nella sentenza oggetto del presente commento e sui quali, comunque, ci si soffermerà in seguito – il caso giudiziario che ci occupa, per l'importanza dei temi trattati e per la novità che esso rappresenta, induce inevitabilmente a riflessioni più estese.

Tutte le volte in cui, infatti, si giudica la Rete, ne deriva un certo clamore. Ciò accade essenzialmente perché da parte della "comunità di *Internet*", e non solo, si ha la percezione – non importa se corretta o errata – che il "sistema" tenti di portare degli attacchi alla libertà dello strumento che oggi, per eccellenza, garantisce a tutti il pieno esercizio della libertà di manifestazione del pensiero, ed alla libertà dei soggetti che consentono l'accesso a tale strumento. Si ha la percezione, cioè, che dietro alle iniziative legali/giudiziarie, volte apparentemente alla tutela di questo o di quel diritto, vi sia in realtà un irrefrenabile desiderio di censura, di porre un limite ad una situazione vista da molti come di sostanziale anomia, come se *Internet* fosse una sorta di territorio franco dove la legalità resta sospesa.

Al di là, però, delle eccessive semplificazioni in cui, inevitabilmente, si rischia di cadere quando si ragiona più in termini ideologici che giuridici, non v'è dubbio che le problematiche coinvolte dalla vicenda giudiziaria che ci occupa sono molteplici, di notevole complessità ed investono diritti e libertà di fondamentale importanza per il nostro ordinamento giuridico ([5]). E se, abbandonando le anguste prospettive legate agli interessi di parte, si vuole davvero trovare una soluzione normativa adeguata alla complessità del fenomeno, occorre tenere in considerazione tutti gli aspetti di tale complessità ([6]).

Il caso di specie risulta, dunque, sintomatico delle diverse sensibilità che si scontrano sul terreno (virtuale) di *Internet*. Da una parte la posizione di chi ritiene che la Rete dovrebbe godere della più assoluta libertà, dall'altra la posizione di chi, al contrario, ravvisa la necessità di individuare delle regole applicabili al *Web* già nella normativa esistente.

---

ventivo del contenuto dei video immessi in rete dai provider. A proposito del caso Google/Vividown, in *Riv. dir. ind*., 2010, 4-5, 347).

([4]) Così anche l'ex Garante delle *privacy*, Stefano Rodotà, si esprimeva in termini di preoccupazione (Pezzella, *cit*.).

([5]) Come, infatti, sottolineato da una parte della dottrina, "*Google-Vividown rappresenta uno tra i casi di maggiore complessità giuridica e di più intenso clamore mediatico*" (Melzi D'Eril, Vigevani, *Nelle motivazioni di condanna della sentenza violazione della privacy per mancato consenso*, in *Guida al Diritto*, 25/2010, 20 ss.).

([6]) Si commenta, in proposito, che "*quando si parla di* Internet, *gli stessi giuristi sembrano perdere di vista il riferimento normativo e le regole del diritto per lasciarsi coinvolgere da quella che pare ormai diventata una sorta di guerra di religione*" (Pezzella, *cit*.).

Si tratta, a ben vedere, di due *weltanschauung* contrapposte che finiscono per influenzare le soluzioni prospettate, forzando, in entrambi i casi, il dato normativo.

2. La sentenza di primo grado.

Veniamo ora al caso concreto, partendo proprio da una breve analisi della sentenza di primo grado.

Come già detto in precedenza, il giudice di prime cure aveva ritenuto gli imputati responsabili esclusivamente per le violazioni della normativa sulla *privacy*, mentre li assolveva dall'accusa di concorso omissivo, ai sensi dell'art. 40 *cpv*. c.p., nel reato di diffamazione, per aver omesso di impedire la divulgazione in Rete di immagini dal contenuto palesemente diffamatorio.

Paradossalmente, ai fini delle nostre riflessioni, la sentenza interessa più nella parte in cui assolve, piuttosto che in quella in cui condanna. E ciò perché la decisione se assolvere o condannare gli imputati ai sensi del citato art. 40 *cpv*. c.p. ha comportato da parte del giudice di Milano una netta presa di posizione su uno degli aspetti più delicati legati al riconoscimento di un'eventuale responsabilità penale degli IP, vale a dire la possibilità di rinvenire, in capo agli stessi, una posizione di garanzia, con il conseguente obbligo di impedire la commissione di reati per il tramite del servizio offerto, mediante l'esercizio di un controllo preventivo sul contenuto di tutti i dati immessi nel relativo spazio *Web*.

Ebbene, secondo quanto stabilito dal Tribunale di Milano, un simile obbligo potrebbe sussistere solamente nell'ipotesi in cui il *provider*, sia esso *hosting provider* o *content provider*, abbia in qualsiasi modo acquisito la consapevolezza del contenuto dei dati immessi in Rete da terzi attraverso il servizio offerto.

Ma procediamo con ordine: due sono, infatti, i potenziali profili di responsabilità degli imputati sui quali si è espresso il giudice di primo grado nel caso Google.

In primo luogo, come oramai noto, gli imputati venivano assolti dall'accusa di concorso mediante omissione nel reato di diffamazione, ai sensi dell'art. 40, *cpv*. c.p., contenuta alla lettera A) del capo d'imputazione, per non aver impedito l'evento rappresentato dalla diffusione del filmato dal palese contenuto diffamatorio. Secondo il giudice di primo grado non sarebbe, infatti, possibile riconoscere una posizione di garanzia in capo all'IP, non essendo tecnicamente possibile, da parte di questi, il controllo preventivo di tutti i dati gestiti dal servizio offerto. Si sottolinea, inoltre, come la presenza di una posizione di garanzia ai sensi dell'art. 40 cpv. c.p. non si possa far derivare da una legge, come quella sulla *privacy*, che sia stata emanata a copertura di comportamenti diversi da quello contestato.

Al contrario, secondo il giudice di prime cure, sarà possibile ritenere gli IP responsabili dei contenuti dei *file* caricati da terzi nel momento in cui si provi la loro consapevolezza circa il fatto delittuoso, e ciò al di là dell'esistenza di posizioni di garanzia non mutuabili da altri settori dell'ordinamento.

In secondo luogo, viene sottolineato come la diffusione del video in questione rappresenti un illecito trattamento di dati personali rilevante ai sensi dell'art. 167, II comma, d.lgs. 196/2003.

Rileva, infatti, il giudice di prime cure come nel caso di specie non vi sia dubbio sul fatto che il video in questione contenga dei dati personali sensibili raccolti senza il necessario consenso. Così come non vi sarebbe alcun dubbio sul fatto che, vista l'ampia definizione di trattamento contenuta dall'art. 4 d.lgs. 196/2003, anche la condotta posta in essere da Google possa considerarsi un trattamento a tutti gli effetti ([7]).

Secondo il Tribunale di Milano, ci si deve allora domandare se gli obblighi previsti dalla normativa sulla *privacy*, oltre ad incombere sul soggetto che ha girato e caricato il video, incombano anche sull'IP che il video ha avuto in carico. Si sottolinea in proposito in sentenza, come "*non può escludersi (come si è detto da un punto di vista meramente oggettivo) che "tratti" un dato chi "raccolga, elabori, selezioni, utilizzi, diffonda, organizzi" dati che, per la loro natura, siano qualificabili come "sensibili"*". In tal senso non vi sarebbe alcuna distinzione tra *host provider* e *content provider*. E', però, altrettanto evidente come un simile comportamento possa essere considerato colpevole solamente se vi sia coscienza e volontà, mentre non può ritenersi punibile chi tratti dati personali ritenendo in buona fede che siano stati lecitamente raccolti da terzi. E questo ancor prima di valutare la sussistenza del dolo specifico previsto dalla fattispecie di reato contestata.

Lo stesso giudice di primo grado sgombera poi il campo da dubbi stabilendo come non sussista alcun obbligo in capo all'IP di controllo preventivo circa l'ottemperanza da parte dell'utente del servizio degli obblighi di legge in materia di *privacy*. Sarebbe, infatti, del tutto impossibile pretendere che l'IP possa verificare le migliaia di video che in ogni momento vengono caricate sul sito *web*.

Secondo una parte della dottrina ([8]), la sentenza in esame si porrebbe, dunque, in contrasto con la giurisprudenza espressa dalla Corte di cassazione nel noto caso "*Pirate bay*" dove, invece, sebbene nella fase monitoria, veniva astrattamente riconosciuta una possibile responsabilità a titolo di concorso dell'IP qualora questi non si fosse limitato alla mera attività di *hosting provider*, ma avesse anche svolto la funzione di *content provider*, provvedendo, ad esem-

---

([7]) Come sottolineato anche dalla dottrina, "*non vi è dubbio che vi sia stato un trattamento di dati sensibili senza il prescritto consenso e che ciò abbia determinato un danno alla persona offesa; più problematico è comprendere se Google – oltre naturalmente a chi aveva immesso il video in rete – avesse l'obbligo di chiedere il consenso della persona ritratta*" (Melzi D'Eril, Vigevani, *cit*., 21).

([8]) Resta, *Libertà della rete e protezione dei dati personali: ancora sul caso Vivi Down*, in via di pubblicazione.

pio, ad indicizzare i contenuti inseriti, realizzando, dunque, un apporto causale alla condotta illecita altrui, penalmente rilevante ai sensi dell'art. 110 c.p. ([9]).

In realtà, però, da una più attenta comparazione dal caso "*Pirate bay*" con il caso "Google" emerge come le due vicende processuali siano profondamente differenti, così come le problematiche giuridiche ad esse sottese. Nel caso "*Pirate bay*", infatti, la Corte di cassazione non si è pronunciata sulla sussistenza di un eventuale obbligo di impedire l'evento ai sensi dell'art. 40 cpv. c.p., ma ha ravvisato un'ipotesi di concorso nel reato, ai sensi dell'art. 110 c.p., per avere l'IP contribuito causalmente alla realizzazione dello stesso, per il tramite di una condotta commissiva.

Anche in relazione alla violazione della normativa sulla *privacy* non è, dunque, ipotizzabile alcuna responsabilità dell'IP ai sensi dell'art. 40 cpv. c.p. Contrariamente a quanto sostenuto da una parte della dottrina, non vi è alcuna contraddizione nella sentenza di primo grado tra le decisioni relative ai due distinti capi d'imputazione, sebbene si approdi a due soluzioni diametralmente opposte ([10]).

Ciò che, infatti, viene ritenuto non solo possibile, ma anche doveroso, dal Tribunale di Milano, ed è proprio ciò su cui si fonda la sentenza di condanna, è l'obbligo riconosciuto in capo all'IP di fornire agli utenti del servizio tutte le necessarie avvertenze in ordine al rispetto della normativa sulla *privacy*. Non un obbligo di controllo, dunque, ma un obbligo di informazione, che sposta decisamente i termini della responsabilità penale, determinandone un sostanzioso ridimensionamento ([11]). E tale obbligo sorgerebbe in capo all'IP dal dettato dell'art. 13 d.lgs. 196/2003, oltre che dal fatto che, secondo il giudice di prime

---

([9]) Scriveva in proposito la Corte di cassazione che "*se il titolare del sito non si limita a ciò, ma fa qualcosa di più – ossia indicizza le informazioni che gli vengono dagli utenti... – il sito cessa di essere un mero "corriere" che organizza il trasporto dei dati. C'è un* quid pluris *in quanto viene resa disponibile all'utenza del sito anche una indicizzazione costantemente aggiornata che consente di percepire il contenuto dei file suscettibili di trasferimento. A quel punto l'attività di trasporto dei file* (file transfert) *non è più agnostica; ma si caratterizza come trasporto di dati contenenti materiale ricoperto dal diritto d'autore. Ed allora è vero che lo scambio dei file avviene da utente ad utente* (peer-to-peer), *ma l'attività del sito* web *(al quale è riferibile il protocollo di trasferimento e l'indicizzazione di dati essenziali) è quella che consente ciò e pertanto c'è un apporto causale a tale condotta che ben può essere inquadrato nella partecipazione imputabile a titolo di concorso ex art. 110 c.p.*" (Cass. pen., sez. III, 49437/2009).

([10]) Si era, invece, espresso nei termini di una contraddizione Catullo, *Ai confini della responsabilità penale: che colpa attribuire a Google*, in *Giur. mer.*, 2011, I, 159.

([11]) Si sostiene in sentenza come "*non esiste, a parere di chi scrive, perlomeno fino ad oggi, un obbligo di legge codificato che imponga agli ISP un controllo preventivo della innumerevole serie di dati che passano ogni secondo nelle maglie dei gestori o proprietari dei siti web, e non appare possibile ricavarlo* aliunde *superando d'un balzo il divieto di analogia* in malam partem, *cardine interpretativo della nostra cultura procedimentale penale*".

cure, Google procederebbe ad un vero e proprio trattamento dei dati personali raccolti dagli *uploader*.

Pur non riconoscendo, come detto più volte, un obbligo giuridico di controllo preventivo dei dati che passano attraverso il servizio fornito agli utenti, rileva lo stesso giudice come non esista nemmeno quella che viene provocatoriamente definita la "*sconfinata prateria di internet*", dove tutto è permesso e niente può essere vietato, pena la scomunica del popolo del *Web*.

A sostegno della propria decisione, il giudice di prime cure richiama proprio la sentenza della Corte di cassazione resa nel caso "*Pirate bay*", sulla base della quale l'IP dovrebbe ritenersi corresponsabile nel reato di cui all'art. 167 qualora non si limiti a fornire un semplice rapporto di interconnessione, ma gestisca i dati in suo possesso, divenendo in qualche modo a tutti gli effetti il titolare del trattamento ([12]).

3. La sentenza d'appello.

La sentenza oggetto del presente commento, al pari di quella di primo grado, è particolarmente complessa ed articolata ([13]).

In primo luogo, anche la sentenza d'appello sottolinea come il riconoscimento di una responsabilità penale ai sensi dell'art. 40 *cpv*. c.p., derivante dall'omesso controllo dei contenuti diffusi in Rete per il proprio tramite, passi necessariamente attraverso l'individuazione, in capo all'IP, di un preciso obbligo giuridico di impedire l'evento e, dunque, attraverso il riconoscimento di una posizione di garanzia.

Ebbene, sottolinea la Corte come nel nostro ordinamento penale non sia rintracciabile alcuna previsione normativa in tal senso, non potendo trovare applicazione, per analogia, la disciplina di cui agli artt. 57 e 57 *bis* c.p. in materia di reati commessi per il mezzo della stampa. Inoltre, non si può ravvisare, in capo all'IP, neanche la possibilità di un pieno ed efficace controllo sulla massa dei video caricati da terzi. Si rileva, in proposito, in sentenza, come "*l'obbligo del soggetto-web di impedire l'evento diffamatorio, imporrebbe allo stesso un filtro preventivo sui dati immessi in rete, che finirebbe per alterarne la sua funziona-*

([12]) Si sottolinea, infatti, come "*non costituisce condotta sufficiente ai fini che la legge impone, "nascondere" le informazioni sugli obblighi derivanti dal rispetto della legge sulla privacy all'interno di "condizioni generali di servizio" il cui contenuto appare spesso incomprensibile, sia per il tenore delle stesse che per le modalità con le quali vengono sottoposte all'accettazione dell'utente*". Ciò fa si che si che si possa concludere circa "*una chiara accettazione consapevole del rischio concreto di inserimento e divulgazione di dati, anche e soprattutto sensibili, che avrebbero dovuto essere oggetto di particolare tutela; non solo, ma anche dell'interesse economico ricollegabile a tale accettazione del rischio e della chiara consapevolezza di quest'ultimo*".

([13]) Per un primo commento sulla sentenza d'appello di veda Ingrassia, *La Corte d'Appello assolve i manager di Google anche dall'accusa di illecito trattamento dei dati personali*, in *www.dirittopenalecontemporaneo.it*.

lità". Come si dirà meglio in seguito, l'esercizio di un simile potere rappresenterebbe, infatti, l'esercizio di un vero e proprio diritto di censura.

Allo stesso tempo, sottolinea la Corte d'Appello come la posizione di garanzia dell'IP non potrebbe derivare nemmeno dalle norme poste a tutela della privacy che, come correttamente osservato, "*sono state emanate a copertura di comportamenti diversi da quelli oggetto di contestazione*".

Infine, a prescindere da una formale previsione normativa, una posizione di garanzia non potrebbe comunque essere riconosciuta in capo all'IP neanche di fatto, altrimenti si finirebbe per richiedere dallo stesso un comportamento inesigibile.

Oltre, però, a confermare quanto già deciso dal giudice di prime cure, la Corte d'Appello riforma la sentenza di primo grado ed assolve gli imputati anche per i reati in materia di tutela di dati personali.

Rileva, infatti, la Corte come la soluzione prospettate dal Tribunale di Milano sia del tutto incongruente, in primo luogo per il semplice fatto che l'art. 13 citato in sentenza non viene richiamato nel testo dall'art. 167 d.lgs. 196/2003. Secondo la Corte, infatti, la norma di cui all'art. 167 sarebbe caratterizzata dalla tipicizzazione della condotta penalmente rilevante in quanto richiede che l'autore del reato abbia agito non rispettando le disposizioni ivi indicate. Ebbene, si sottolinea in sentenza come nessuna delle disposizioni richiamate dall'art. 167 imporrebbe all'IP di rendere edotto l'utente circa l'esistenza ed i contenuti della legge sulla *privacy*. Inoltre, si osserva come la violazione dell'art. 13 sia espressamente sanzionata dall'art. 161 dello stesso d.lgs. 196/2003 e, dunque, non rilevi ai fini dell'applicazione dell'art. 167.

Nella sentenza d'appello si censura anche il fatto che il giudice di primo grado non si sarebbe soffermato ad analizzare il concetto di titolarità del trattamento. "*In effetti*", sostiene la Corte, "*trattare un video, acquisirlo, memorizzarlo cancellarlo, non può significare di per sé trattamento di dati sensibili… Trattare un video non può significare trattare il singolo dato contenuto, conferendo ad esso finalità autonome e concorrenti con quelle perseguite da chi quel video realizzava*". Conseguenza di ciò, è che spetterà solo ed esclusivamente al titolare del trattamento l'obbligo di acquisire il consenso al trattamento dei dati personali. Nel caso specifico, dunque, tale obbligo spetterebbe esclusivamente all'*uploader*. E ciò troverebbe conferma anche nella Giurisprudenza della Corte di cassazione, oltre che in quella della Corte di Giustizia Europea.

Si osserva, infine, come il riferimento al concorso di persone ai sensi dell'art. 110 c.p., contenuto nella lettera B) del capo d'imputazione, preveda una partecipazione attiva nel reato da parte degli imputati, mentre invece, nel caso di specie, si ravvisa un concorso mediante omissione. Trattandosi, però, quello di cui all'art. 167 d.lgs. 196/2003, di un reato di mera condotta, una simile ipotesi di concorso non sarebbe in alcun modo ammissibile ([14]).

([14]) Come anche sottolineato da Manna, *cit*.

La sentenza d'appello si sofferma poi anche sull'elemento psicologico del reato, non condividendosi l'impostazione del giudice di primo grado, il quale aveva confuso il dolo specifico del fine di profitto con la vocazione economica dell'azienda Google. Ponendo, inoltre, il problema della compatibilità tra la forma del dolo eventuale ed il dolo specifico richiesto dalla fattispecie di cui all'art. 167 d.lgs. 196/2003.

4. Alcune considerazioni sulla sentenza d'appello.

Sebbene la sentenza assolutoria sia assolutamente condivisibile, la Corte d'Appello dimostra però una grande confusione, mischiando profili diversi, più o meno fondati.

Si sostiene, infatti, in primo luogo, come la violazione degli obblighi stabiliti dall'art. 13 d.lgs. 196/2003, non essendo tale norma richiamata dalla fattispecie di reato di cui all'art. 167, non possa comportare alcuna responsabilità di carattere penale.

Quanto precede non sembrerebbe, però, in alcun modo condivisibile e ciò perché il richiamo fatto dal giudice di primo grado all'art. 13, che stabilisce un obbligo di informativa sul trattamento, risulta finalizzato esclusivamente a determinare la presenza in capo agli imputati del dolo eventuale legato al trattamento illegittimo di dati personali, e nulla ha a che vedere con la disposizione di cui all'art. 167.

Il ragionamento fatto dal giudice di prime cure è piuttosto chiaro e stupisce che non sia stato compreso nella sua portata: dal momento che non si provvede ad un'adeguata informativa circa gli obblighi in materia di raccolta di dati personali, ne consegue che si accetta il rischio che tali dati vengano raccolti in maniera illegittima. Da qui la presenza del dolo eventuale. Dal momento poi che, secondo il giudice di primo grado, l'attività posta in essere da Google può considerarsi un trattamento di dati a tutti gli effetti, ciò significa che Google ha accettato il rischio di trattare dati raccolti illegittimamente. Si avrebbe, cioè, un trattamento di dati fatto in violazione di quanto disposto dall'art. 23 d.lgs. 196/2003, norma questa espressamente richiamata dalla fattispecie di reato di cui all'art. 167.

Messo da parte il discorso circa il mancato richiamo dell'art. 13 nell'art. 167, ai fini della valutazione della responsabilità degli imputati per violazione della normativa sulla *privacy* occorrerà chiedersi allora se effettivamente l'attività posta in essere da Google possa considerarsi un trattamento di dati e, soprattutto, se l'obbligo di informativa di cui all'art. 13 spetti anche a Google o solamente all'*uploader*.

Ebbene, come anche correttamente evidenziato dal giudice di prime cure, non sembrerebbe esservi dubbio sul fatto che, vista la definizione onnicompren-

siva di cui all'art. 4 d.lgs. 196/2003 ([15]), anche l'attività posta in essere da Google sia da considerarsi un trattamento a tutti gli effetti.

Come già detto più volte, però, non è esigibile dall'IP una valutazione del contenuto di tutte le migliaia di filmati caricati in Rete quotidianamente. Si potrebbe allora ragionare su una ipotetica responsabilità del *provider* solamente se lo stesso venisse riconosciuto il "titolare" del trattamento.

Ebbene, ai sensi del citato art. 4, per "titolare" del trattamento si intende "*la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalita', alle modalita' del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza*". E' proprio sulla base di una simile definizione che l'IP, a meno che non tratti consapevolmente dati personali altrui, non possa ritenersi in alcun modo titolare del trattamento e, dunque, non sia obbligato ai sensi del più volte citato art. 13. Ed in ciò risiede il *vulnus* del ragionamento condotto dal giudice di prime cure. Come, infatti, correttamente osservato dalla dottrina ([16]), tutta la disciplina in materia di *privacy* è volta a regolare il rapporto tra chi raccoglie il dato e colui al quale il dato appartiene. Se è vero, dunque, che l'informativa di cui all'art. 13 può essere rivolta anche alla persona presso la quale i dati sono raccolti, ciò sembra volto esclusivamente a far si che tale comunicazione venga successivamente girata al soggetto interessato.

Al contrario, non si condivide quanto sostenuto dalla Corte d'Appello circa la natura omissiva del concorso di Google nel reato. Come detto più volte, infatti, l'omissione imputata a Google sarebbe solamente quella relativa all'informativa di cui all'art. 13, afferente al solo elemento psicologico del dolo eventuale, mentre il contributo causale posto in essere dall'IP nel caso specifico sarebbe rappresentato da un trattamento attivo dei dati personali.

Si concorda, infine, con quanto sostenuto dalla Corte d'Appello circa il fatto che il giudice di primo grado abbia confuso il dolo specifico del fine di lucro, richiesto dalla fattispecie di reato di cui all'art. 167, con lo scopo commerciale di Google. Come correttamente sottolineato in sentenza, richiamando anche a sostegno la giurisprudenza di legittimità, il dolo specifico richiesto dalla fattispecie contestata appare, infatti, del tutto incompatibile con il dolo generico individuato dal giudice di prime cure. Nel caso di specie, rimane davvero difficile sostenere che Google abbia volontariamente e consapevolmente trattato il video in questione al fine di trarne un profitto. E come sottolineato in proposito da una parte della dottrina, il dolo eventuale viene escluso tutte le volte in cui non vi

---

([15]) Secondo il quale per "trattamento" deve intendersi "*qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati*".

([16]) Melzi D'Eril, Vigevani, *cit.*, 22.

siano elementi che consentano di ricondurre nell'attività dell'IP una specifica attività illecita commessa per il suo tramite, altrimenti si finirebbe per equiparare il dolo eventuale ad una sorta di *dolus in re ipsa* ([17]).

5. Brevi considerazioni conclusive.

Al di là delle specifiche questioni giuridiche, la vicenda Google-Vividown fornisce lo spunto per alcune considerazioni di carattere generale circa la responsabilità penale dell'IP e circa il diritto della Rete.

Di grande interesse risultano, in proposito, le riflessioni fatte da una parte della dottrina che, come detto in precedenza, si è spinta in considerazioni di più ampio respiro. Si osserva, così, come la vicenda giudiziaria di cui ci si occupa abbia evidenziato in maniera impietosa come la normativa penale non disciplini a sufficienza il settore dei *service provider*, imputando ciò non al fatto che la materia non sarebbe di per sé regolamentabile, ma alla mancanza di una concreta domanda di pena da parte della collettività ([18]). Si sostiene, cioè, che la mancanza di un'adeguata regolamentazione di *Internet*, quantomeno dal punto di vista penale, sia dovuta non tanto alla complessità del fenomeno da disciplinare, quanto ad un difetto di percezione del disvalore di determinate condotte. ([19]).

Sottolinea in proposito Catullo, come per comprendere a fondo la portata delle problematiche sottese al caso di specie, ed intervenire a livello normativo, sia necessario soffermarsi attentamente sulla relazione intercorrente tra l'ampliamento della libertà di manifestazione del pensiero conseguente allo sviluppo della Rete e l'affermazione degli operatori, come per l'appunto Google, che consentono l'esercizio di tale libertà. Da una parte, per il tramite dello sviluppo della Rete, si assiste ad un ampliamento smisurato della libertà di manifestazione del pensiero e, dall'altra – ma di questo non ci se ne rende pienamente conto – si assiste allo sviluppo del potere dei soggetti che permettono l'accesso alla Rete e che forniscono gli strumenti tecnici per consentire l'esercizio di tale libertà.

Troppo spesso, infatti, come lamentato dalla citata dottrina, non ci si sofferma a sufficienza sul fatto che ogni traccia che il singolo affida al *Web* venga catalogata e trattata da un motore di ricerca come è, per l'appunto, Google, e che una volta che si è deciso di accedere al *Web* si rinunci a qualsiasi controllo sui dati ivi immessi. Nonostante ciò, però, gli utenti del *Web* sono più portati a per-

---

([17]) Pezzella, *cit.*

([18]) Catullo, *Atto secondo dell'*affaire Google Vivi Down: *società della registrazione e consenso sociale*, in via di pubblicazione.

([19]) D'altra parte, da tempo la dottrina ha posto in stretta relazione l'effettività del sistema penale con il consenso sociale che deve catalizzarsi attorno alle fattispecie di reato. Si veda, più di recente, Musco, *L'illusione penalistica*, Giuffrè, Milano, 2004. Così l'Autore propone di introdurre un *quorum* qualificato dei due terzi del Parlamento per l'approvazione delle nuove fattispecie di reato, in modo tale da garantire la più ampia condivisione delle scelte di criminalizzazione.

cepire il valore "istituzionale" dei soggetti che consentono l'accesso alla Rete e che estendono la loro libertà, piuttosto che non il disvalore di vincoli e controlli.

In un simile contesto, anche la *privacy* non è più avvertita come un diritto da tutelare, ma come un intralcio alla libera conoscenza. E' il prezzo che si deve pagare per l'esercizio delle nostre libertà che, però, finisce allo stesso tempo per comprimerle. Si cede libertà per acquisire libertà e ciò impone di trovare un necessario equilibrio normativo che non passa, però, necessariamente, per la criminalizzazione di qualsiasi attività, ma per un'attenta riflessione tra consenso sociale ed istanza punitiva.

Come prospettato da una parte della dottrina, sarebbe allora opportuno un intervento del legislatore che rafforzi gli obblighi di controllo sull'identificazione di chi scrive o immette filmati in rete, nel rispetto dei principi cardine della normativa italiana e comunitaria sul commercio elettronico e, dunque, sull'insussistenza di un obbligo generale di sorveglianza ([20]). Qualsiasi soluzione si ritenga di adottare, questa non potrà, infatti, non contemperare tutti i diritti e le libertà fondamentali che si incontrano e si scontrano nel territorio di *Internet*. Così, come detto più vote nel corso del presente lavoro, non è ipotizzabile prevedere in capo all'IP un obbligo di controllo preventivo sulle informazioni che passano attraverso il servizio fornito e dei dati trattati. Già in passato si era sostenuto che "*ipotizzare in capo ai* provider *un dovere di controllo del contenuto delle comunicazioni e delle informazioni che passano attraverso i servizi gestiti equivarrebbe, infatti, ad introdurre in* Internet *uno strumento di censura preventiva che non ha eguali in nessun'altra forma di comunicazione e che si porrebbe in palese contrasto con alcune delle libertà fondamentali del nostro ordinamento quali la libertà e la segretezza della corrispondenza di cui all'art. 15 Cost. e la libertà di manifestazione del pensiero di cui all'art. 21 Cost.*" ([21]). D'altra parte, non è un caso che da una parte della dottrina si riconosca un valore particolare alla libertà di manifestazione del pensiero, riconoscendo come il rispetto di tale libertà rappresenti la cifra del livello di democraticità dell'ordinamento ([22]). Proprio per tale ragione sembrerebbe essere oramai fuori di qualsiasi dubbio la possibilità di riconoscere all'IP una posizione di garanzia ai sensi dell'art. 40 cpv. c.p. ([23]).

([20]) Melzi D'Eril, Vigevani, *cit*., 23. La stessa dottrina lamenta, però, come le proposte all'ordine del giorno mostrino una tendenza regressiva ad estendere ad *Internet* le norme sorte per la stampa o la televisione, ispirate alla logica dell'obbligo preventivo di controllo.

([21]) Mi sia consentito, in proposito, di rinviare a Terracina, *La tutela penale del diritto d'autore e dei diritti connessi*, Giappichelli, Torino, 2006, 160 ss.

([22]) Zaccaria, Valastro, *Diritto dell'informazione e della comunicazione*, Cedam, Padova, 2010.

([23]) Si veda, tra tutti, quanto scritto da Seminara, *La responsabilità penale degli operatori su Internet*, in *Dir. inf*., 1998, 751.

Dall'altra parte, però, non è ipotizzabile ritenere che l'IP sia posto al di fuori di qualsiasi vincolo di responsabilità. Così, parte della dottrina ([24]) prova a tratteggiare delle prospettive di riforma su cui costruire una disciplina a tutela dei diritti fondamentali nella Rete, che sia in grado di contemperare tutti i vari interessi in gioco, con particolare riferimento al diritto alla dignità ed alla protezione dei dati personali da un lato ed alla libertà di espressione ed alla segretezza delle comunicazioni dall'altro. Ebbene, una prima soluzione potrebbe essere quella di riconoscere la responsabilità dell'IP che, informato dell'illiceità dei contenuti trasmessi, non si attivi tempestivamente per rimuoverli su richiesta dell'interessato o dell'autorità giudiziaria, pena una responsabilità a titolo di concorso. In tali casi, secondo Resta, sarebbe auspicabile l'introduzione di una fattispecie di reato contravvenzionale, punita esclusivamente a titolo di dolo diretto, con sanzioni interdittive e con pena pecuniaria. Viene, inoltre, fatto riferimento al progetto di legge AC 2318 presentato nel corso della XVI legislatura con il proposito di modificare il d.lgs. 196/2003, riconoscendo il diritto in capo a chiunque abbia interesse alla rimozione o al blocco di dati divulgati illecitamente, di presentare istanza di oscuramento, rimozione, rettificazione, aggiornamento, integrazione o blocco dei contenuti medesimi, direttamente al *provider*. Nell'ipotesi in cui l'IP non intendesse adempiere, il soggetto potrebbe rivolgersi al Garante per la protezione dei dati personali. Si verrebbe in questo modo a creare un sistema volto a responsabilizzare i *provider* nell'immediata rimozione dei contenuti illeciti, senza, però, imporre loro un obbligo preventivo e generalizzato di controllo sui contenuti dei dati diffusi in Rete.

Sarebbe, infine, auspicabile, secondo la medesima dottrina citata, la previsione di una clausola di non punibilità per i *provider* che abbiano adottato sistemi di controllo conformi a criteri previsti in via legislativa, idonei ad impedire la diffusione di informazioni illecite. Una soluzione, quest'ultima, modellata sulla disciplina dei modelli organizzativi di cui al d.lgs. 231/2001.

Peraltro, vale la pena ricordare, come anche rilevato da altra dottrina ([25]), che un istituto simile a quello invocato da Resta è già previsto dalla disciplina sul commercio elettronico. Si tratta della c.d. *notification*, rappresentata dalla comunicazione attraverso la quale gli IP vengono messi a conoscenza dell'illiceità dei contenuti dagli stessi ospitati. Secondo la dottrina da ultimo citata, infatti, non vi può essere esenzione di responsabilità qualora l'intermediario del servizio, posto a conoscenza dell'illiceità dei contenuti caricati dall'utente su segnalazione delle autorità competenti, non si attivi per rimuoverli. Certo, l'IP sarà tenuto a valutare l'attendibilità delle *notification*, se vuole evitare di rendersi inadempiente nei riguardi della propria clientela. Dal momento, però, che l'art. 17 d.lgs. 70/2003, nel quale l'istituto della *notification* è inserito, fa riferimento esplicito all'autorità giudiziaria o amministrativa avente funzioni di vigilanza,

---

([24]) Resta, *Libertà della rete e protezione dei dati personali: ancora sul caso Vividown*, in via di pubblicazione.

([25]) Maggio, *Il diritto di impresa non può prevalere sulla privacy e sulla tutela dei diritti della persona*, in *Riv. dir. ind*., 2011, 2, 47.

saranno proprio tali soggetti gli unici ad essere legittimati a richiedere la rimozione dei contenuti illeciti.

Ebbene, in relazione a quanto precede, occorre muovere alcune osservazioni. In primo luogo non v'è dubbio che nel momento in cui l'IP acquisisca la piena consapevolezza dell'illiceità del materiale trasmesso per il tramite del proprio servizio e non si attivi per rimuoverlo, assuma anche un ruolo attivo colpevole nel trattamento e nella diffusione dello stesso materiale illecito. Si tratta, peraltro, come già detto più volte, di una corresponsabilità ai sensi dell'art. 110 c.p. per una condotta commissiva e non invece, ai sensi dell'art. 40 *cpv*. c.p., per il mancato impedimento dell'evento. L'IP, anche a seguito della segnalazione circa l'illiceità dei dati gestiti, non assume, infatti, una posizione di garanzia, ma diviene responsabile in quanto contribuisce, questa volta dolosamente, alla commissione di un reato. Così, analogamente, lo spedizioniere che, rendendosi conto di trasportare droga o armi prosegua nella propria prestazione diverrà concorrente nel traffico illecito.

Certo, come correttamente sottolineato da Maggio, trattandosi di dati la cui illiceità spesso non risulta palese, occorrerà in primo luogo che l'IP valuti attentamente l'attendibilità della *notification* ed in secondo luogo che valuti attentamente l'illiceità dei dati. Proprio per tali ragioni occorrerà trovare un sistema per contemperare diverse esigenze: da una parte l'esigenza di celerità nella rimozione di dati dal contenuto palesemente illecito e, dall'altra, la garanzia che l'istituto della *notification* non diventi uno strumento di controllo e di censura diffusi.

Spesso, infatti, i danni derivanti da ritardi nella rimozione dei dati possono risultare incalcolabili. Basti pensare proprio al caso in esame. Sebbene, dunque, si concordi in via di massima con quanto sostenuto dalla dottrina da ultimo citata circa il fatto che l'obbligo di rimozione non possa che derivare dalla segnalazione fatta dall'autorità, occorre fare i conti con le patologiche lentezze del nostro ordinamento giuridico. Una soluzione di compromesso potrebbe allora passare attraverso una responsabilizzazione del soggetto che richiede formalmente la rimozione dei dati qualora non intervenga un provvedimento dell'autorità giudiziaria o dell'autorità garante. Tale soggetto dovrà, ad esempio, essere identificabile con certezza, magari inviando la segnalazione per il tramite dell'autorità di pubblica sicurezza e, laddove dovesse riferire circostanze false, ne potrebbe rispondere anche penalmente.

Proprio per le ragioni appena espresse, non si ritiene, invece, di concordare con quanto proposto da Resta circa l'introduzione di una nuova fattispecie di reato di natura contravvenzionale. Al di là, infatti, di quanto sostenuto dalla dottrina circa il reato contravvenzionale ([26]), la nuova fattispecie, così come proposta, non spiegherebbe alcuna efficacia deterrente, tenendo in considerazione il fatto che una contravvenzione punita con la sola pena pecuniaria potrebbe esse-

([26]) D'obbligo il richiamo a Donini, *Il delitto contravvenzionale.* 'Culpa Iuris' *e oggetto del dolo nei reati a condotta neutra*, Giuffrè, Milano, 1993, e a Fondaroli, *Diritto penale e riparazione del danno*, Giuffrè, Milano, 1999.

re estinta con il semplice pagamento dell'oblazione. Ciò comporterebbe, dunque, per gli IP più strutturati ed economicamente solidi, come per l'appunto Google, la monetizzazione del rischio penale.

Non sembra, per altro, plausibile neanche la proposta di prevedere una clausola di non punibilità per i *provider* che abbiano adottato adeguati sistemi di controllo, sulla falsariga di quanto previsto dal d.lgs 231/2001 in materia di responsabilità degli enti da reato. Come già detto in precedenza, la responsabilità dell'IP non deriverebbe, infatti, da una posizione di garanzia e da un obbligo giuridico di impedire l'evento – obbligo che potrebbe ritenersi effettivamente assolto attraverso l'adozione di un adeguato sistema di controllo – ma dall'acquisita consapevolezza di gestire dei dati illeciti. Non si vede, dunque, come l'adozione di un sistema di controllo adeguato possa mitigare tale responsabilità, che sarebbe, invece, la conseguenza di una scelta precisa da parte dell'IP.

L'insussistenza di un obbligo di controllo preventivo in capo ai vertici di google ed il difficile bilanciamento tra diritti contrapposti

di Alessandro Roiati (*)

1. Il fatto, le imputazioni ed il giudizio di primo grado

La vicenda in esame trae origine dalla pubblicazione di un video dal contenuto offensivo sull'apposito portale di *Google* in cui compariva "un ragazzo presumibilmente *down*, in un ambiente scolastico, che veniva schernito e deriso da un gruppo di ragazzi". Le denunce sporte portavano all'attenzione della Procura profili di responsabilità penale anche a carico dei responsabili del sito, in quanto si trattava di un filmato che, non solo era circolato sul *web* tramite *Google Video*, ma non poteva essere passato inosservato, perché aveva conquistato la prima posizione nella categoria "video più divertenti" ed era addirittura finito all'interno della classifica ufficiale dei video più scaricati.

In particolare ai vertici di *Google*[1], da un lato veniva contestato il concorso nella fattispecie aggravata di diffamazione ex artt. 110, 40, comma 2, 595, commi 1 e 2, c.p., attraverso la diffusione del video a mezzo *internet*, senza alcun controllo preventivo sul suo contenuto, dall'altro la violazione degli artt. 110, 167, commi 1 e 2 d. lvo. 30 Giugno 2003 n. 196, perché, al fine di trarne profitto per il tramite del servizio *Google Video*, procedevano al trattamento di dati personali in violazione agli artt. 17, 23 e 26 stesso d. lvo., con relativo nocumento per la persona interessata[2].

Il giudice di primo grado chiamato a pronunciarsi in merito a questa delicata fattispecie, sin da subito oggetto di particolare attenzione da parte dei *media*[3], nella parte motivazionale della sua sentenza metteva in chiara evidenza le istanze configgenti sottese alla vicenda: da un lato la necessità di escludere la possibilità di configurare un generico ed inesigibile obbligo di controllo preventivo sul contenuto dei video pubblicati ogni giorno nella rete; dall'altro i possibili vuoti di tutela derivanti dall'istituzione di una sorta di "immunità sostanziale" per i soggetti responsabili del servizio di pubblicazione e divulgazione *on-line*, pur a fronte dell'avvenuta commissione di determinate fattispecie di reato.

(*) In *Giurisprudenza Italiana*.

[1] Nella fattispecie gli amministratori delegati di *Google Italy* s.r.l., il Responsabile delle *policy* sulla *privacy* per l'Europa (*Global Privacy Counsel*) di *G. Inc*., ed il Responsabile del progetto *Google Video* per l'Europa.

[2] In particolare in violazione dell'art. 13, difettando del tutto l'informativa sulla *privacy* e, per essa, il valido consenso di cui all'art. 23, comma 3; dell'art. 26, venendo in rilievo dati idonei a rivelare lo stato di salute della persona inquadrata; dell'art. 17, per i rischi specifici insiti nel tipo di trattamento, non attivandosi *G. Italy* srl, tramite il prescritto interpello, presso l'Autorità Garante.

[3] Sui rapporti tra diritto penale e *media* cfr. in particolare C.E. PALIERO, *La maschera e il volto. Percezione sociale del crimine ed effetti penali dei* media, in *Riv. it. dir. proc. pen.,* 2006, p. 469 e ss.

La necessità di trovare una ragionevole composizione valoriale attraverso i profili penalistici della vicenda - che icasticamente rappresenta le potenzialità ed i rischi insiti nella diffusione di dati nella rete - ha portato in primo grado ad una soluzione compromissoria, ma viziata da evidenti forzature interpretative che, nei confronti degli apicali di *Google*, per un verso ha escluso il sussistere del concorso omissivo nella fattispecie diffamatoria, per l'altro ha ritenuto sussistente la responsabilità penale per l'illecito trattamento di dati personali[4].

In riferimento al primo aspetto, secondo l'interpretazione dell'accusa, i responsabili di *Google* avevano l'obbligo preventivo di controllo sul contenuto dei video caricati e non avevano posto in essere tutti i filtri possibili, limitandosi ad un sistema di controllo successivo, conseguente alle segnalazione degli utenti; in particolare si riteneva sussistente una posizione di garanzia a carico del sito *web* derivante dagli obblighi giuridici contenuti nella legge sulla *privacy*.

Per il Tribunale però, per lo meno fino ad oggi, non sussiste "un obbligo di legge codificato che imponga un controllo preventivo delle innumerevoli serie di dati che passano ogni secondo, nelle maglie dei gestori dei siti *web*, né appare possibile ricavarlo *aliunde*, superando il divieto di analogia in *malam partem*, cardine interpretativo della nostra cultura procedimentale penale". Nella realtà poi l'obbligo di controllo preventivo pare essere "un *comportamento inesigibile* in ragione delle estreme difficoltà tecniche e delle conseguenze di sostanziale "illegittima" censura che ne potrebbe derivare"[5].

---

[4] Trib. Milano, 12 aprile 2010, n. 1972, pubblicata, tra l'altro, in *Cass. pen*., 2010, p. 3986 e ss., con nota di R. LOTIERZO, *Il caso* Google-Vivi Down *quale emblema del difficile rapporto degli* internet providers *con il codice della* privacy; in *Giur. mer*., 2010, p. 2232, con nota di V. PEZZELLA, *Google Italia, diffamazione e riservatezza: il difficile compito del provider (e del giudice)*, con commento di F.G. CATULLO, *Ai confini della responsabilità penale: che colpa attribuire a Google*, *ivi*, 2011, p.159.; in *Corr. mer*., 2010, p. 960, con nota di L. BEDUSCHI, *Caso* Google*: libertà d'espressione in* internet *e tutela penale dell'onore e della riservatezza*.

[5] Mancando una precisa legislazione in materia, si afferma, la responsabilità penale degli ISP, non può essere costruita al di là dei canoni dell'attuale quadro normativo. Anche se, a parere del giudice di primo grado, si sente l'esigenza di una buona legge sull'argomento, "in quanto *internet* è un formidabile strumento di libera comunicazione, ma ogni esercizio collegato alla libertà non può essere assoluto". Sul punto, a fronte di una letteratura ormai sterminata, cfr. per tutti G. CORRIAS LUCENTE, *Ma i* network providers, *i* service providers *e gli* access providers *rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che gestiscono?*, in *Giur. mer*., 2004, 2523 e ss.; A. INGRASSIA, *Il ruolo dell'*internet service provider *nel ciberspazio: cittadino, controllore o tutore dell'ordine? Risposte attuali e scenari futuribili di una responsabilità penale dei* provider, in *penalecontemporaneo.it.;* A. MANNA, *I soggetti in posizione di garanzia*, in *Dir. inf*., 2010, p. 779 e ss. ; L. PICOTTI, *Fondamento e limiti della responsabilità penale* dei service-providers *in Internet*, in *Dir. pen. proc*., 1999, p. 384; più di recente L. PICOTTI, *I diritti fondamentale nell'uso e abuso dei* social network. *Aspetti penali*, in *Riv. giur. mer.*, 2012,p. 12; F. RESTA, *La responsabilità penale del provider: tra* laissez faire *ed obblighi di controllo*, in *Giur. mer*., 2004, p. 1733.

Al contrario, in relazione ai profili penalistici derivanti dall'illecito trattamento di dati personali, è stato ritenuto provato che il video in questione contenesse allusioni e indicazioni sullo stato di minorità del soggetto e dunque che il video di per sé fosse un dato personale e sensibile, come tale inquadrabile nella previsione dell'art. 167 d. lgs. citato, posto che "*non può esistere in materia una zona franca che consenta a un qualsiasi soggetto di ritenersi esente dagli obblighi di legge nel momento in cui venga in possesso di dati sensibili*".

In questo senso a poco varrebbe la distinzione tra *host provider* e *content provider*, in quanto il proprietario o il gestore di un sito *web* che compia anche solo una delle attività di raccolta, elaborazione, selezione, utilizzo, diffusione, organizzazione dei filmati tratta i dati che gli vengono consegnati e, di conseguenza, assume un dovere di corretta e puntuale informazione agli utenti degli obblighi agli stessi imposti dalla legge. Nella fattispecie andava escluso che la condotta tenuta potesse essere considerata sufficiente ai fini imposti dalla legge, in quanto l'informativa sulla *privacy* era fornita in modo generico ed astratto e comunque "tale da non risultare minimamente utile se non quasi a costituire una sorta di alibi la stessa società"; il giudizio di responsabilità in ordine al reato di illecito trattamento dei dati personali veniva quindi espresso, non sulla base di un obbligo preventivo di controllo sui dati immessi, ma sulla base di un profilo valutativo differente, costituito dalla insufficiente comunicazione degli obblighi di legge all'*uploader*.

Quanto in ultimo al fine di profitto richiesto dalla norma, lo stesso poteva rinvenirsi nell'operatività del sistema di pubblicità basato su parole chiave *AD words*, in quanto rilevatore di una "*accettazione consapevole del rischio concreto di trattamento di dati sensibili*".

2. Il giudizio di secondo grado in merito al concorso omissivo nella fattispecie di diffamazione

La corte d'appello, in riferimento all'ipotesi di concorso nella fattispecie diffamatoria, ha condiviso le valutazioni espresse in primo grado circa l'insussistenza, in capo ai vertici di *Google*, di una posizione di garanzia e di un obbligo di preventivo controllo sui contenuti video ed ha ritenuto di dover assolvere gli imputati anche in relazione alla contestazione riguardante la violazione degli obblighi di trattamento dati ex art. 167 d.lgs. 30 Giugno 2003 n. 196. Al riguardo è opportuno evidenziare sin da ora che la ritenuta insussistenza di un obbligo di controllo sui contenuti video ha costituito *l'elemento dirimente per entrambi i capi di imputazione*[6], finendo per porsi come valutazione assor-

[6] Sul problema dell'individuazione dei beni giuridici sottesi alle norme in materia di dati personali, sul nesso esistente tra detta normativa e salvaguardia della reputazione, nonché sul rischio di un assetto di tutela sbilanciato nel senso della salvaguardia di mere funzioni, cfr. in particolare A. MANNA, *Codice della* privacy*: nuove garanzie per i cittadini nel Testo unico in materia di protezione dei dati personali*, in *Dir. pen. proc.*, 2004, p. 22 e ss.; P. VENEZIANI, *I beni giuridici tutelati dalle norme penali in materia di*

bente rispetto a tutte le ulteriori questioni affrontate, e relative in particolare al concetto di titolarità del trattamento ed alla mancanza del dolo di concorso e del dolo specifico.

Quanto alla prima imputazione, la corte si è limitata ad aggiungere taluni significativi dati: 1) che per sostenere la responsabilità a titolo di omissione in capo ad un *host* o *content* provider, occorre affermare a suo carico un obbligo giuridico di impedire l'evento e quindi da un lato, l'esistenza di una posizione di garanzia, dall'altro la concreta possibilità di effettuare un controllo preventivo; detta posizione di garanzia non può essere ravvisata nel diritto vigente, stante l'assenza di una specifica previsione in tal senso, né la posizione di garanzia di cui trattasi può desumersi da fonte diversa, quale in via esemplificativa quella dettata ex art. 57, e 57-*bis* c.p. in materia di stampa, in quanto si tratterebbe di analogia *in malam partem*; 2) che la presenza di una posizione di garanzia da cui far derivare un obbligo di attivazione, in mancanza della quale far ricorrere la previsione dell'art. 40 c.p., di certo non può essere fatto derivare dalla violazione di norme di legge quali quelle a protezione dei dati personali, che non hanno per oggetto tali condotte e che sono state emanate a copertura di comportamenti diversi da quelli oggetto di contestazione; 3) che in materia di concorso di persone la condotta consistente nel non impedire l'evento, che si ha l'obbligo giuridico di impedire, deve essere accompagnata dal dolo che caratterizza il concorso stesso, da ravvisarsi nella coscienza e volontà di concorrere con altri nella realizzazione del reato.

Gli argomenti addotti risultano in buona parte condivisibili, pur dovendosi considerare la mancata trattazione, relativamente a questo capo di imputazione[7], della preliminare questione riguardante l'ammissibilità di un concorso in forma omissiva, ai sensi dell'art. 40, comma 2, c.p., in una fattispecie commissiva priva di evento naturalistico.

Al riguardo si consideri che la possibilità di applicare cumulativamente le due clausole generali di cui agli artt. 40 cpv. c.p. e 110 c.p. con una disposizione di parte speciale è contestata da quella dottrina secondo cui il principio di legalità consentirebbe, semmai, un'applicazione distinta e successiva, tale da rispettare l'operatività di entrambe[8]. Nello specifico l'operatività del concorso omissivo

---

disciplina dei dati personali, in *La tutela penale della persona*, a cura di L. FIORAVANTI, Milano, 2001, p. 369 e ss.

[7] La questione è invece affrontata, ed in senso negativo, in relazione all'altra imputazione, laddove si afferma "ancora la Corte rileva, che mentre il riferimento all'art. 110 c.p. prevede una partecipazione attiva nel reato da parte degli imputati, la sentenza ed in parte l'accusa, finiscono per ravvisare un concorso costituito da una condotta omissiva. Sotto questo profilo deve però evidenziarsi che trattandosi di reato di pura condotta, non possono ravvisarsi i presupposti per pervenire su queste basi ad un giudizio di responsabilità, essendo la sfera dell'art. 40, comma 2, c.p., limitata ai reati di evento".

[8] Cfr. L. RISICATO, *Combinazione e interferenza di forme di manifestazione del reato: contributo ad una teoria delle clausole generali di incriminazione suppletiva*, Mila-

andrebbe circoscritta alle *fattispecie ad evento naturalistico*[9], là dove l'art. 40 cpv. c.p. svolgerebbe una funzione incriminatrice e le disposizioni sul concorso una mera funzione di disciplina. Di conseguenza «nella compartecipazione mediante omissione al fatto illecito altrui il garante è sempre coautore, perché siamo di fronte a reati di evento naturalistico rispetto a cui il mancato impedimento non può scadere al livello dell'ambigua ed incerta *agevolazione negativa*»[10].

Anche a voler concedere l'ammissibilità di un concorso omissivo in una fattispecie di mera condotta, si sarebbe poi dovuto accertare il *nesso eziologico rispetto al fatto-reato*, ma quest'indagine è stata obliterata sia in primo che in secondo grado, posto che dalle risultanze della perizia disposta all'epoca dei fatti erano esistenti strumenti tecnici utili per l'eliminazione di video illeciti da parte del gestore del servizio, ma "necessitanti anche di ulteriori apposite strutture necessarie per la verifica della liceità o meno del contenuto, e comunque inidonei in senso assoluto a consentire l'individuazione di tutte le casistiche di video illeciti". Di conseguenza, procedendo al giudizio controfattuale caratterizzante l'accertamento del nesso di causalità, si sarebbe agevolmente dovuto concludere che, anche utilizzando la migliore tecnologia disponibile all'epoca dei fatti, non sarebbe stato possibile un adeguato controllo circa il contenuto di tutti i filmati caricati in rete e quindi non sarebbe stato possibile impedire il verificarsi del fatto-reato[11].

Risultano invece del tutto condivisibili le argomentazioni addotte in tema di insussistenza di una *posizione di garanzia avente ad oggetto il preventivo controllo contenutistico* sui dati immessi in rete. Sul punto infatti non può essere accolto l'orientamento giurisprudenziale secondo cui una posizione di garanzia può derivare anche da "una situazione di fatto per precedente condotta illegittima, che costituisca il dovere di intervento" o "dall'esistenza di un potere giuridico o di fatto, attraverso il corretto uso del quale, il soggetto garante sia in grado di attivandosi di impedire l'evento"[12].

---

no, 2001, p. 399 e ss.; nella manualistica cfr. in particolare G. FIANDACA – E. MUSCO, *Diritto penale,* Bologna, 2009, p. 578.

[9] Cfr. G. FIANDACA – E. MUSCO, *op. ult. cit.*, p. 578, secondo cui, considerato che nel caso di realizzazione monosoggettiva dell'illecito omissivo improprio il giudizio di equivalenza va limitato alla fattispecie con evento naturalistico, v'è da chiedersi se tale regola possa essere legittimamente disattesa, allorché il garante sia chiamato a rispondere a titolo di concorso".

[10] L. RISICATO, *La partecipazione mediante omissione a reato commissivo. Genesi e soluzione di un equivoco,* in *Riv. it. dir. proc. pen.*, 1995, p. 1275 e ss..

[11] In realtà la corte ha sovrapposto i profili inerenti alla posizione di garanzia con quelli riguardanti l'accertamento causale, nel momento in cui ha respinto la tesi accusatoria secondo la quale la responsabilità degli imputati deriverebbe dal mancato controllo preventivo sul contenuto dei video, attuabile attraverso l'attivazione di tutti i filtri disponibili, sostenendo che anche l'attivazione di tali dispositivi non sarebbe comunque efficace, a causa dei limiti degli strumenti tecnici, tanto più di quelli utilizzabili al tempo dei fatti.

[12] *Ex plurimus* cfr. Cass., Sez. IV, 6 luglio 2006, n. 32298.

Al riguardo è necessario ribadire che l'estrema genericità di tali assunti si pone in antitesi con le posizioni della dottrina, particolarmente attenta a coniugare la responsabilità per omesso impedimento dell'evento con i limiti sottesi all'osservanza dei principi di legalità e di personalità della responsabilità penale,[13] e soprattutto contrasta apertamente con il principio di *tassatività*, che reclama una puntuale individuazione della stessa posizione di garanzia, in quanto "la caratterizzazione in termini di giuridicità dell'obbligo di impedire l'evento postula il rispetto del principio di legalità in tutte le sue articolazioni"[14]. L'obbligo di garanzia va ricostruito quindi quale "obbligo *giuridico*, gravante su *specifiche categorie predeterminate* di soggetti *previamente* forniti degli adeguati *poteri giuridici*, di impedire eventi offensivi di beni altrui, *affidati* alla loro tutela per l'*incapacità* dei titolari di adeguatamente proteggerli"[15]. Non si può prescindere inoltre dal giudizio circa la necessaria corrispondenza tra il dovere giuridico "impeditivo" ed il simmetrico *potere giuridico*, effettivo e certo, di soddisfare tale pretesa[16], per cui è necessario accertare la compresenza di *effettivi poteri di impedimento* dell'evento e di influenza sul suo decorso causale[17].

In questo senso, nei due giudizi di merito, è stata correttamente esclusa la possibilità di configurare una fattispecie omissiva in capo ai vertici di *Google* attraverso il generico richiamo alla normativa posta a tutela del trattamento dei dati personali, considerato che sarebbe stato necessario rinvenire una posizione di garanzia avente come contenuto specifico proprio l'obbligo giuridico di impedire la commissione del reato altrui[18], non essendo sufficiente a tal fine un generico obbligo di protezione[19].

---

[13] Sul punto, per tutti, F. MANTOVANI, *L'obbligo di garanzia ricostruito alla luce dei principi di legalità, di solidarietà, di libertà e di responsabilità personale*, in *Riv. it. dir. proc. pen*., 2001, p. 340 e ss.

[14] Così I. LEONCINI, *Obbligo di attivarsi, obbligo di garanzia e obbligo di sorveglianza*, Torino, 1999, p. 50 e ss.; F. MANTOVANI, *Diritto penale, Parte generale,* Padova, 2009, p. 163.

[15] Così testualmente F. MANTOVANI, *Diritto penale, cit*., p. 160, che sottolinea altresì le differenze esistenti tra l'obbligo di garanzia e gli altri obblighi di agire.

[16] Così I. LEONCINI, *op. ult. cit*., p. 49. L. BISORI, *L'omesso impedimento del reato altrui nella dottrina e giurisprudenza italiane*, in *Riv. it. dir. proc. pen*., 1997, p. 1367, rileva correttamente che si è dinanzi ad un obbligo di garanzia volto all'impedimento dei reati altrui solamente ove l'ordinamento si faccia carico di conferire, al soggetto che istituisce come garante, *specifici poteri giuridici di impedimento-comando nei confronti del reo*, così ponendo il primo in grado di interferire direttamente (e lecitamente) con l'intera condotta di reato posta in essere dal secondo.

[17] Sul punto I. LEONCINI, *op. ult. cit*., p. 71 e ss.

[18] Al riguardo, in riferimento alla tradizionale dicotomia tra posizioni di protezione e posizioni di controllo, verrebbe in rilievo una terza categoria di posizioni di garanzia caratterizzata da obblighi di impedimento di reati commessi da terzi. Sul punto in particolare G. GRASSO, *Il reato omissivo improprio*, Milano, 1983, p. 327 e ss.; L. BISORI, *L'omesso impedimento del reato altrui nella dottrina e giurisprudenza italiane, cit*., p.

All'assenza di uno specifico dovere giuridico di impedire l'evento, che si salda con l'insussistenza del nesso causale, si aggiunge infine *la mancanza di dolo* che nella fattispecie non attiene solo, come affermato dalla corte, alla mancanza del cd. dolo di concorso, ma inerisce ancor prima alla mancanza di dolo in relazione al fatto tipico in sé considerato, posto che i vertici di *google* non avevano alcuna consapevolezza del contenuto offensivo del filmato video. Non a caso la corte, nell'affermare l'insussistenza della posizione di garanzia, sostiene che la stessa non può desumersi da fonte diversa, quale in via esemplificativa quella dettata *ex* art. 57, e 57-*bis* c.p. in materia di stampa, che prevede una responsabilità per omesso controllo quale *fatto autonomo punito a titolo di colpa, nonché fuori dai casi di concorso*[20].

Nel caso in esame appare del tutto evidente che, se pure fosse stata riconosciuta l'esistenza di una posizione di garanzia in capo ai vertici di *Google* derivante dalla normativa sulla *privacy*, il rimprovero sarebbe al più potuto consistere nel non aver posto in essere *colposamente* il dovuto controllo, fattispecie non punibile in mancanza di apposita disposizione di legge; va respinta con forza infatti la tesi volta a rinvenire, in siffatte evenienze, un'ipotesi di *accettazione del rischio* e quindi di dolo eventuale, che si ridurrebbe ad una sorta di *dolus generalis* ed *in re ipsa*, del tutto privo di contenuto psicologici effettivi e completamente sganciato dalla concreta caratterizzazione della singola fattispecie concreta[21].

3. Il giudizio di secondo grado in merito in merito al trattamento dei dati personali

Per quanto riguarda la violazione degli obblighi di trattamento dati personali, che aveva portato ad un giudizio di condanna in primo grado, sono state ritenute infondate le questioni sollevate in merito alla sussistenza della giurisdizione italiana, in quanto non appare rilevante il luogo in cui sia collocato il *server* sul quale vengono caricati i video, dovendosi avere riguardo al luogo in cui si sono verificati gli effetti pregiudizievoli dell'illecito[22]. Occorre inoltre sottolineare

---

1365 e ss., secondo il quale tale terza categoria può attingere le proprie caratteristiche funzionali da ciascuna delle altre due. Secondo D. PULITANÒ, *Diritto penale*, Torino, 2009, p. 249, però, a ben vedere, nella fattispecie si tratterebbe di un peculiare aspetto della posizione di garanzia di protezione.

[19] G. MARINUCCI – M. DOLCINI, *Manuale di diritto penale. Parte generale*, Milano, 2006, p. 327.

[20] In questa direzione G. FIANDACA – E. MUSCO, *Diritto penale, cit.*, p. 645 e ss.; in giurisprudenza cfr. Cass., Sez. I, 14 luglio 2008, n.35646.

[21] Sul punto, per tutti, S. PROSDOMICI, Dolus eventualis*. Il dolo eventuale nella struttura delle fattispecie penali*, Milano, 1993.

[22] Vedi art. 5.3 della Convenzione di *Bruxelles* del 27 settembre 1968 come interpretato dalla consolidata giurisprudenza della Corte di Giustizia. La corte d'appello sostiene inoltre che l'evento del caricamento del *server*, ammesso che si verifichi negli U.S.A., è di per sé solo potenzialmente generatore di danno, ma privo di efficacia dannosa, che si verifica solo nel momento in cui i contenuti vengono diffusi nell'area di

che essendo *Google Italy* soggetto giuridico stabilito nel territorio della Stato, nei suoi confronti trova applicazione la disciplina in materia di dati personali ex art. 5, comma 1, codice *privacy*.

Quanto al merito della vicenda la corte affronta in primo luogo la questione del ruolo svolto da *Google Video* all'epoca dei fatti, sostenendo che "l'evoluzione della rete informatica mondiale sembra avere superato nei fatti la figura di mero prestatore di servizio che delineava tale soggetto come del tutto estraneo rispetto alle informazioni memorizzate, sia a livello di gestione che di regolamentazione contrattuale con i destinatari del servizio". Viene in rilievo in particolare un'ulteriore categoria denominata di *hosting attivo*, cioè di prestatore di servizi non neutra rispetto all'organizzazione ed alla gestione dei contenuti degli utenti, caratterizzata anche dalla possibilità di un finanziamento economico attraverso l'inserimento di inserzioni pubblicitarie: "orbene tutti gli elementi valutati nel caso - la possibilità del filtraggio, della rimozione, dell'individuazione di contenuti tramite parole chiave, dell'indicizzazione dei contenuti e della eventuale utilizzazione a fini pubblicitari - portano a ritenere che *google video* non possa che essere qualificata quantomeno come un *hosting* attivo".

Individuata in tal modo la posizione di *google* in merito al caricamento dei filmati, la corte si preoccupa di escludere, anche per il prestatore di servizi che fornisca *hosting* attivo, la possibilità di procedere ad una efficace verifica preventiva di tutto il materiale immesso dagli utenti, poiché "tale comportamento non può essere ritenuto doveroso, in quanto *non esigibile* per la complessità tecnica di un controllo automatico e comunque, demandare ad un *internet provider* un dovere/potere di verifica preventiva, appare una scelta da valutare con particolare attenzione in quanto non scevra da rischi, poiché potrebbe finire per collidere contro forme di libera manifestazione del pensiero".

Nel caso di specie veniva in considerazione il reato di illecito trattamento di dati personali, per la violazione dell'art. 167 d. lgs. 30 Giugno 2003 n. 196 e degli artt. 23, 17 e 26 ivi richiamati, ma la responsabilità degli imputati, esclusa la sussistenza di un obbligo preventivo di *sorveglianza sui contenuti* di quanto immesso in rete, è stata fatta derivare dalla carenza di una corretta puntuale e doverosa informazione agli utenti delle norme poste a tutela della *privacy*, ex art. 13 d. lgs. citato.

La corte d'appello però ha prontamente rilevato l'incongruenza della scelta operata dal giudice di primo grado, costituita dal fatto che "il citato art. 13 non è neppure richiamato nel testo dell'art. 167 e nessuna delle disposizioni ivi incluse impone all'*Internet Provider* di rendere edotto l'utente circa l'esistenza ed i contenuti della legge della *privacy*"[23], dovendosi altresì considerare che

---

mercato ove la parte danneggiata esercita i suoi diritti, nella specie appunto il territorio italiano (cfr. Cass., Sez. III, 29 settembre 2009, n. 49437).

[23] Si rammenta inoltre che, secondo quanto sostenuto dallo stesso Garante della *privacy*, l'art. 13 riguarda le informazioni che l'ISP deve dare all'utente in merito alle "sue" modalità di trattamento, cioè su ciò che fa l'ISP con i dati di chi utilizza la piatta-

l'eventuale violazione del medesimo art. 13 viene sanzionata *esclusivamente in via amministrativa* dall'art. 161. Oltre a ciò è stato ritenuto decisivo il concetto di *titolarità del trattamento*: "la responsabilità per il trattamento dei dati è legata al mancato adempimento di specifiche condizioni che rendono lecito l'uso di tali dati, ma tali condizioni non possono che essere messe in capo al titolare, al "*controller*" dei dati medesimi. In effetti trattare un video, acquisirlo, memorizzarlo, cancellarlo, non può significare di per sé trattamento di dati sensibili". Nella fattispecie l'*uploader*, caricando il video, assumeva la responsabilità del trattamento dei dati personali, e pertanto su di lui incombeva l'obbligo di chiedere ed ottenere il consenso prescritto[24], così come previsto anche dalla normativa sul commercio elettronico, in cui si indica che: "il prestatore non è responsabile delle informazioni memorizzate...a condizione che detto prestatore non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita"[25].

Un ulteriore imprescindibile argomento viene individuato *nell'insussistenza dell'elemento soggettivo* del reato contestato, in quanto è necessario operare una netta distinzione tra il dolo specifico richiesto dalla norma ed il generico fine di profitto costituito dalla vocazione economica dell'azienda *Google*[26]. L'attività dell'azienda nei suoi molteplici servizi non può che essere considerata lecita e non può essere assunta a prova della sussistenza del dolo specifico nella fattispecie concreta, tanto più nell'ambito di un servizio gratuito quale era *Google Video* ed in assenza di *link* pubblicitari associati allo specifico video: "la mancanza di un dolo specifico emerge poi dalla ragionevole certezza che gli imputati non fossero preventivamente a conoscenza del contenuto del filmato e dell'immissione del dato personale non lecitamente trattato".

Si pone da ultimo un problema di compatibilità tra la forma del dolo eventuale - individuata in capo agli imputati per avere serbato una "*voluta disatten-*

---

forma. Cfr. al riguardo A. INGRASSIA, *Il ruolo dell'*internet service provider *nel cyberspazio, cit.*, p. 10.

[24] Cfr. in senso conforme Cass., Sez. III, 17 novembre 2004, n.5728, in linea anche con la giurisprudenza della Corte di Giustizia Europea che, in un caso di pubblicazione di dati personali su *internet*, ha ritenuto titolare del trattamento il soggetto che aveva provveduto all'*uploading*: "è la persona che crea, invia o carica i dati *on line* che deve essere ritenuto il titolare del trattamento dati e non la parte, il provider che fornisce gli strumenti". Si consideri infine che la relazione al Parlamento Europeo in merito alla responsabilità giuridica degli intermediari *internet* 8 giugno 2000, addirittura vieta, tenendo a mente l'art. 15 del D.L.vo 70/03, "agli Stati membri di imporre agli intermediari Internet l'obbligo generale di controllare le informazioni che si trasmettono o si archiviano ovvero l'obbligo generale di cercare attivamente fatti o circostanze atte a indicare il proseguimento di attività illegali".

[25] Sui rapporti tra *privacy* e commercio elettronico, quali macrocategorie del tutto indipendenti l'una dall'altra, ma che possono avere punti di interconnessione in determinati casi, cfr. in particolare G. CASSANO, *Google V. Vividown. Responsabilità "assolute" e fine di Internet?*, in *Vita not.*, 2/2010, p. 10 e ss.

[26] Cfr. Cass., Sez. III, 24 maggio 2012, n. 23798.

zione" nelle politiche societarie relative al trattamento della *privacy*, al fine dell'ottenimento di buoni risultati di mercato - ed il dolo specifico richiesto dalla norma in oggetto. La soluzione in senso positivo, fondata per lo più su una valutazione eticizzante, volta a censurare le scelte di politica aziendale sorrette da un precipuo fine di lucro, non appare accettabile, in quanto la struttura della fattispecie di cui all'art. 167 Codice *privacy* postula la necessaria partecipazione psichica intenzionale e diretta del soggetto al raggiungimento di un profitto[27].

4. Riflessioni a margine della vicenda e prospettive de jure condendo

Dato atto dell'insussistenza – *de jure condito* – di un dovere di puntuale verifica e controllo da parte dei vertici aziendali dell'*internet service provider* (ISP) che diffonde i contenuti video nella rete, resta da porsi l'interrogativo circa l'opportunità o meno di configurare a suo carico precipue ipotesi di responsabilità penale, nella prospettiva di un necessario contemperamento di esigenze contrapposte ma di pari rango costituzionale: da un lato garantire la libertà di espressione e di circolazione di dati e informazioni nel *web*, dell'altro evitare che contenuti lesivi di diritti della persona vengano veicolati in *internet*, finendo col configurare fattispecie di reato rese particolarmente offensive della straordinaria capacità diffusiva della rete. In particolare il possibile coinvolgimento del *provider* sul fronte della responsabilità può discendere dalla sue stesse caratteristiche di soggetto organizzato che consente l'ingresso di determinati contenuti e che li veicola nel ciberspazio in maniera sempre più evoluta e complessa, nonché trovare ulteriore spinta - quantomeno un un'ottica di politica criminale - in considerazione del fattore costituito dall'anonimato, che spesso determina vuoti di tutela incolmabili altrimenti.

Al riguardo in dottrina sono stati individuati almeno tre possibili paradigmi di responsabilizzazione penale[28], modulati in virtù del diverso assetto di tutela degli interessi sottesi: 1) equiparazione dell'ISP al comune cittadino, con conseguente responsabilità penale circoscritta alle sole ipotesi di concorso doloso nell'altrui condotta criminosa, senza alcun obbligo di controllo e/o di collaborazione nella repressione degli illeciti; 2) attribuzione all'ISP del ruolo di *controllore dei contenuti immessi nella rete*, con un modello di responsabilità incentrato sul reato omissivo improprio e sul mancato impedimento del reato altrui; 3) attribuzione all'ISP del ruolo di *tutore dell'ordine* nel ciberspazio, con l'imposizione dell'obbligo di denuncia degli illeciti di cui viene a conoscenza, di rimozione del materiale illegittimo e di collaborazione nell'individuazione degli autori, secondo il paradigma di tutela costituito dal reato omissivo proprio.

Orbene, se per un verso si ritiene necessario respingere l'imposizione di penetranti obblighi di controllo preventivo in capo all'ISP, che svilirebbero il diritto alla libertà di manifestazione del pensiero e che farebbero assurgere il prestatore di servizi ad improprio strumento di censura per conto

---

[27] Cfr. Cass., Sez. I, 14 ottobre 1994, in *Cass. pen.*, 1996, p. 2177.

[28] A. INGRASSIA, *Il ruolo dell'*internet service provider *nel ciberspazio, cit.*, p. 5 e ss.

dell'ordinamento[29], per l'altro si ritiene certamente opportuno che dalla particolare posizione assunta dall'ISP derivino peculiari obblighi in merito all'individuazione degli autori del reato ed alla eliminazione e/o riduzione delle conseguenze dannose da esso derivanti; occorre però - ed è questo il *punctum dolens* della questione in esame - domandarsi se la violazione di tali obblighi debba attingere al piano di tutela penale o se debba invece, come pare preferibile, rimanere per lo più circoscritta al piano civilistico e/o amministrativo, attraverso il ricorso a sanzioni pecuniarie non meno dissuasive[30].

Al riguardo non si può prescindere dal considerare il d.lgs. 70/2003, attuativo della direttiva 2000/31/CE e per lo più restrittivo dell'ambito di responsabilità per gli ISP, che all'art. 16, in riferimento alle attività di memorizzazione duratura dei dati pubblicati in rete (cd. *hosting*), ben distingue i piani di tutela, posto che in riferimento alla responsabilità penale prevede un'esenzione della responsabilità per l'ISP ove non sia effettivamente a conoscenza del fatto che l'informazione o l'attività memorizzata sia illecita, mentre sul piano risarcitorio, ritiene sufficiente la cognizione di fatti o di circostanze che rendano manifesta l'illiceità dell'attività o dell'informazione[31]; a norma dell'art. 17 inoltre il *provider* non è assoggettato ad un obbligo generale di sorveglianza, né ad un obbligo generale di ricercare fatti o circostanze che indichino la presenza di attività illecite.

Il *discrimen* tra rilevanza penale e non viene tracciato in considerazione della *effettiva conoscenza* del materiale illecito da altri pubblicato, salvo l'intervento sui dati memorizzati, che potrà portare all'applicazione delle comuni regole del concorso di persone nel reato; di conseguenza il piano della tutela penale può opportunamente operare solo in relazione a ben precise fattispecie - espressamente tipicizzate - quali, ad esempio, la mancata rimozione di contenuti specificatamente segnalati come offensivi[32], e quindi limitatamente a condotte dovero-

---

[29] G. FORNASARI, *Il ruolo della esigibilità nella definizione della responsabilità penale del* provider, in *Il diritto penale dell'informatica nell'epoca di internet*, L. PICOTTI (a cura di), Padova, 2004, p. 431.

[30] In merito fondamentale il contributo di F. STELLA, *Giustizia e modernità*, Milano, 2003, p. 9 e ss., secondo cui occorre cercare di rispondere alla domanda "se le vittime del presente, del passato e del futuro, possano davvero vedere assicurata una tutela adeguata dal diritto penale, classico o moderno che sia, o se la meta di una tutela adeguata non possa e non debba, invece, essere raggiunta utilizzando il potenziale inutilizzato degli altri settori dell'ordinamento, primo fra tutti il diritto civile o amministrativo… Le vittime della "modernità" non riescono a trovare una tutela piena ed adeguata: e quando si tenta di apprestare una qualche tutela con il processo penale, ciò avviene pagando il prezzo del danno, intollerabile per la società, costituito dalla condanna degli innocenti".

[31] Detta limitazione della responsabilità non opera però in riferimento alle materie espressamente indicate nell'art. 1 del medesimo decreto, tra cui sono menzionate anche le disposizioni in tema di *privacy*.

[32] In relazione al principio del *notice and takedown* cfr., G. CASSANO, *op. cit.*, p. 7 e ss. In riferimento alle norme esistenti che impongono di inibire l'accesso al materiale rivelatosi illecito, di inibire la prosecuzione di attività che violino il diritto d'autore,

se da cui scaturisce un obbligo giuridico di attivarsi, e non in considerazione di un evento-reato da impedire in virtù del proprio *status* di garante. Per la restante parte non si considera possibile e nemmeno auspicabile - a fronte dell'indefinita e scarsamente controllabile massa di dati che in ogni momento affluisce nei *server* - ricorrere all'*extrema ratio* sanzionatoria che, tra l'altro, finirebbe col porsi in contrasto con l'art. 27, comma 1, Cost., non solo nel suo significato più autentico di *responsabilità per fatto proprio colpevole*, ma anche nel suo significato minimo di *divieto di responsabilità per il fatto altrui*.

Pare opportuno invece considerare se in taluni casi, e limitatamente al piano risarcitorio, possa configurarsi un obbligo di controllo - *rectius* di *selezione attraverso appositi programmi filtro* - sui contenuti immessi nel *web*, tenendo altresì conto della dimensione transnazionale del fenomeno e della attuale normativa di riferimento, per lo più volta a deresponsabilizzare, anche sul fronte civilistico, gli intermediari dell'informazione a mezzo *internet*[33]. In merito, se è vero che dell'indebita diffusione di contenuti offensivi risponde direttamente l'*uploader* in quanto titolare del trattamento dati ed in quanto richiedente il servizio di diffusione nella rete, è altrettanto vero che di frequente, ed in particolare attraverso procedure informatiche che garantiscono l'anonimato[34], possono verificarsi significativi vuoti di tutela per le persone offese dall'illecita diffusione di contenuti sul *web*[35].

In riferimento a dette fattispecie un obbligo di risarcimento del danno potrebbe operare, *in via sussidiaria ed eventuale*, laddove il *provider* non abbia adottato gli strumenti tecnologicamente più avanzati, e limitatamente ai casi in cui questi si sarebbero rivelati idonei a rinvenire e rimuovere i contenuti offensivi immessi nel *web*; in tal modo si indurrebbe il soggetto che gestisce ed organizza il servizio di pubblicazione dati nella rete alla corretta ed efficace adozione di tutti gli strumenti che la tecnologia mette a disposizione per prevenire la

---

nonché agli obblighi di collaborazione con il centro nazionale per il contrasto della pedopornografia *in internet* istituito presso il Ministero dell'Interno, cfr. L. PICOTTI, *Commento all'art. 600* ter *III comma c.p.*, in A. CADOPPI (a cura di), *Commentario delle norme contro la violenza sessuale e contro la pedofilia*, Cedam, 2004, p. 210 e ss.; R. FLOR, *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di internet*, Giuffrè, 2010, p. 456 e ss.

[33] Cfr. F. DI CIOMMO, *Programmi-filtro e criteri di imputazione/esonero della responsabilità* on-line. *A proposito della sentenza* Google/Vivi Down, in *dir. informaz. e informatica*, 2010, p. 833 e ss.

[34] Sul tema cfr. S. SEMINARA, *Considerazioni su privacy, anonimato ed internet*, in *La tutela penale della persona, cit.*, p. 362 e ss., in cui si afferma che "su questa situazione si innestano due esigenze contrapposte: da un lato, il diritto all'anonimato in rete come diritto della libertà di manifestazione del pensiero e della *privacy*; dall'altro lato, l'interesse ad impedire l'anonimato in rete per la sicurezza delle transazioni commerciali e per la persecuzione dei reati. Dinanzi a tale alternativa, l'orientamento attualmente dominate a livello comunitario è nel senso di riconoscere il diritto all'anonimato, temperato dall'obbligo del *provider* di procedere all'identificazione dell'utente".

[35] Sul punto cfr. F. Di CIOMMO, *op. ult. cit.*, p. 830 e ss.

diffusione di contenuti illeciti, con ciò giungendo ad una ragionevole composizione degli interessi coinvolti, parimenti di rilievo costituzionale[36].

Si verrebbe così a configurare un sistema indirizzato verso il raggiungimento della migliore prevenzione concretamente esigibile e maggiormente equilibrato nella distribuzione dei rischi e dei relativi costi; come in tale in grado di ridurre, da un lato le indebite forzature interpretative – soprattutto sul piano penalistico – determinate dall'avvertito pericolo di possibili vuoti di tutela, dall'altro l'indubbia sperequazione oggi esistente, a parità di scopo, tra operatori della carta stampata ed operatori del w*eb*[37].

[36] Traendo spunto dal caso di specie, in cui l'offesa alla persona veniva particolarmente amplificata dall'inclusione del video nelle apposite classifiche "video più scaricati-video più divertenti", l'eventuale obbligo risarcitorio verrebbe inoltre a modularsi anche in relazione al livello di diffusione del contenuto immesso nella rete, con ciò favorendo una maggiore attenzione su quei contenuti che, attraverso il processo di trattamento e selezione svolto dall'ISP, assumono una particolare visibilità ed abitualmente determinano l'inserimento di *spot* pubblicitari a fine di profitto.

[37] F. DI CIOMMO, *op. ult. cit.*, p. 834. In merito si consideri anche che, sulla base della normativa esistente, correttamente la Cassazione ha escluso l'applicabilità dell'art. 57 c.p., non solo ai direttori di periodici *on-line*, ma anche agli *access provider*, agli *hosting provider* ed ai coordinatori di *blog* e *forum*, in quanto *internet*, sebbene mezzo di comunicazione, non può essere ricondotto al concetto di carta stampata, se non previo ricorso ad un'interpretazione analogica in *malam partem*. Cfr. Cass., Sez. V, 16 luglio 2010, n. 35511.

Atto secondo dell'*affaire Google Vivi Down*: società della registrazione e consenso sociale

di Francesco Giuseppe Catullo (*)

1. Le censure alla sentenza di primo grado

L'*affaire Google Vivi Down*, dopo il processo di primo grado e le censure dell'opinione pubblica che sono seguite, è pervenuto al giudizio di appello.

L'oggetto del dibattito che ha acceso l'attenzione dei media, degli addetti al settore e degli operatori del diritto è stata la "questione del governo di internet"[1].

Avverso la decisione del Tribunale di Milano, che ha ravvisato una responsabilità penale ai sensi dell'art. 167 d.lg. 30 giugno 2003, n. 196 in capo a rappresentanti legali di *Google Italy s.r.l.*, per aver omesso di fornire chiare e puntuali informazioni ai propri *uploaders*, si sono sollevati i giudizi critici della stampa e della collettività che hanno ravvisato, nel principio ricavabile dalla sentenza, una reazione liberticida agli sforzi di uno dei più importanti *service provider* del mondo a migliorare le possibilità e le forme di espressione di ciascuno.

Ciò che è risultato chiaro nello sviluppo del predetto *affaire* è che la normativa penale non ha disciplinato a sufficienza il settore dei *service provider* non perché non regolamentabile, quanto piuttosto per la mancanza di una concreta domanda di pena da parte della collettività. Più precisamente, i consociati che utilizzano i *service provider*, percependo più vantaggi che svantaggi dal loro uso, sono poco interessati a chiedere che vengano disciplinate le attività di questi ultimi anche se finissero ad incamerare giorno dopo giorno milioni di dati personali.

Il Giudice di primo grado, ponendosi in contro tendenza al descritto sentire, ha ravvisato l'opportunità di criminalizzare la condotta di *Google*, ma per giustificare il predetto convincimento ha dovuto forzare le categorie giuridiche di

---

(*) In *Cassazione Penale*.

[1] Nella specie, *Google Video* per più di due mesi aveva diffuso sulla Rete un filmato realizzato dagli alunni di una scolaresca che, senza aver raccolto il consenso della persona rappresentata, gravemente ne offendeva la reputazione. Il citato filmato veniva rimosso da *Google Video* a circa due mesi di tempo dalla sua inserzione on-line e a ventiquattrore ore di distanza dal momento in cui un privato cittadino ed un agente di P.S. formalmente avvisavano la redazione del noto motore di ricerca della presenza del video *de quo* nel proprio spazio virtuale di competenza. La condotta rilevante penalmente che viene contestata ai responsabili di *Google Italia s.r.l.* sarebbe quella di aver gestito il servizio offerto da *Google Video*, omettendo di fornire ai propri inserzionisti telematici chiare e puntuali informazioni sulla corretta modalità del trattamento dei dati personali; avrebbero fatto ciò al fine di raccogliere un numero sempre più elevato di filmati per accrescere l'interesse al servizio da parte di eventuali acquirenti di spazi pubblicitari su Internet. Cfr. Catullo, *Ai confini della responsabilità penale: che colpa attribuire a Google?*, in *Giur. mer.*, 2011, p. 159 ss.

cui disponeva sino a consegnare una struttura motivazionale insufficiente a superare il vaglio del gravame.

Attraverso cinque argomentazioni, di cui ciascuna assorbente la successiva, la Corte di appello di Milano ha censurato le motivazioni del giudizio di primo grado, riconducendo la fattispecie di cui all'art.167 D.lgs. n. 196/03 entro i confini naturali oltre cui ogni altra interpretazione sarebbe valutata in violazione di legge.

Prima argomentazione.

Premesso che l'art. 167 D.lgs. n. 196/03 richiede esplicitamente che l'autore del reato abbia agito non rispettando le disposizioni indicate nel suo precetto e che tra queste disposizioni non è previsto l'art. 13 D.lgs. n. 196/03, la responsabilità degli imputati per il reato di *Trattamento illecito di dati* non può essere fatta derivare "dalla carenza di una puntuale e doverosa informazione agli utenti delle norme poste a tutela della privacy" ex art. 13 D.lgs. n. 196/03. A giudizio della Corte, è stata incongruente la scelta operata dal Tribunale meneghino in quanto nessuna disposizione citata dall'art. 167 D.lgs. n. 196/03 impone all'Internet *service provider,* di rendere edotto l'utente circa l'esistenza ed i contenuti della legge sulla privacy.

Seconda argomentazione

Il soggetto responsabile del reato di cui all'art.167 D.lgs. n. 196/03 non può essere *Google*, ma l'*uploader*, che caricando il video, si assume la responsabilità del trattamento dei dati personali della persona ritratta. Inoltre, la normativa sul commercio elettronico, che costituisce unitamente alla normativa sulla privacy un quadro giuridico coerente e completo, specifica che "il prestatore non è responsabile delle informazioni memorizzate … a condizione che detto prestatore non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita … e che non agisca immediatamente per rimuovere le informazioni medesime".

Terza argomentazione

Poiché il reato di cui all'art. 167 D.lgs. n. 196/03 è un reato di mera condotta ed il concorso dei responsabili di *Google* nel reato posto in essere dall'*uploader* si è sostanziato in una omissione, non è possibile pervenire "ad un giudizio di responsabilità per i primi, essendo la sfera dell'art. 40 comma 2 c.p. limitata ai reati di evento".

Quarta argomentazione

Non sussiste l'elemento soggettivo del reato contestato, in quanto l'estensore della sentenza di primo grado ha confuso il dolo specifico previsto per il reato di cui all'art. 167 D.lgs. n. 196/03 con il fine di profitto costituito dalla palese vocazione economica di *Google*. Poiché l'attività commerciale della predetta azienda è lecita, questa "non può essere assunta a prova della sussistenza del dolo".

Quinta ed ultima argomentazione

La struttura della fattispecie di cui all'art. 167 D.lgs. n. 196/03, postulando la necessaria partecipazione psichica intenzionale e diretta del soggetto al rag-

giungimento del profitto (dolo specifico), è incompatibile con la forma del dolo eventuale contestato ai prevenuti.

2. Il *prezzo* per poter manifestare liberamente il pensiero

I passaggi motivazionali della sentenza in commento risultano chiari e coerenti nel superare la costruzione operata dal Giudice di primo cure e nel contempo si palesano sensibili nel comprendere il significato del giudizio di quest'ultimo. La Corte di appello afferma perciò che, pur considerando non condivisibile l'impostazione seguita dal Tribunale, la ritiene ugualmente di "buon senso".

Sembra quasi che tra le trame della motivazione annotata, il Giudice del gravame mentre da una parte sottolinea l'assenza di una normativa atta a disciplinare la responsabilità penale del *service provider* e l'impossibilità di forzare quella disponibile senza incorrere in violazione di legge, dall'altra esprima un giudizio favorevole sull'opportunità di intervenire penalmente avverso i predetti operatori.

Cogliendo quest'ultimo spunto, sollevato prima dal Tribunale e successivamente dalla Corte di appello, è opportuno domandarsi per quale motivo la condotta di un *service provider* meriterebbe di essere sanzionata penalmente nel momento in cui provveda alla registrazione e all'utilizzo di dati personali conformandosi ad un protocollo di sicurezza minimale.

Per rispondere al quesito necessita soffermarsi sulla relazione intercorrente tra l'ampliamento della libertà di manifestazione del pensiero e l'affermazione degli operatori che gestiscono i sistemi di registrazione atti a consentire l'esercizio della prima. Qualsiasi iscrizione che il singolo affida al web viene catalogata e trattata da un motore di ricerca come per esempio *Google*, così come chi decide di aprire un profilo *Facebook* immette nella pagina una serie di contenuti personali e non, comunque identificativi dell'inserzionista; e ancora, ogniqualvolta si decide di iscriversi in un portale di servizi *online* è necessario indicare i propri dati personali, come ancora risultano tracciabili le preferenze di navigazione collegate all'utilizzo di un determinato indirizzo IP (c.d. *Click-stream*).

E' stato scritto che viviamo nella società della registrazione; o più precisamente, nella società delle comunicazioni che vengono iscritte, dove la volatilità delle parole e dei processi si trasforma nella solidità e permanenza degli oggetti sociali[2]. La tecnologia permette di documentare atti, fatti ed eventi e di regi-

[2] Ferraris, *Manifesto del nuovo realismo*, Laterza, 2012, p. 75, che - dopo aver differenziato gli *oggetti naturali* (come per esempio gli uragani i fiumi e le montagne che esistono nello spazio e nel tempo indipendentemente dai soggetti) dagli *oggetti sociali* (come le crisi economiche, i biglietti aerei e i matrimoni che esistono nello spazio e nel tempo dipendentemente dai soggetti) - afferma che la legge costitutiva di quest'ultimi è "*Oggetto = Atto Iscritto*. Vale a dire che un oggetto sociale è il risultato di un atto sociale (tale da coinvolgere almeno due persone, o una macchina delegata e una persona) che

strarli per un tempo indeterminato. Le esperienze così vengono estrapolate dai contesti generanti per essere affidati all'indiscrezione del pubblico del web che le condivide alla stregua di oggetti.

Con la registrazione volontaria[3] o involontaria di dati da parte dell'utente delle tecnologie si affida qualcosa di sé al gestore del supporto che la tratta.

Quest'ultimo vende sensazioni libertarie al prezzo della rinuncia di parte della propria determinazione. L'iscrizione, infatti, non solo vincola il suo autore o il rappresentato della registrazione ad un fatto che non conoscerà oblio, attribuendo un potere ricattatorio a chiunque decidesse di utilizzarlo contro chi lo ha prodotto o contro chi è stato immortalato, ma consente anche di favorire il controllo e la governabilità della comunità che si affida alle registrazioni. Il trattamento di milioni di dati personali permette di prevedere e definire i binari aggregativi e normalizzanti lungo cui la società dell'informazione (ma sarebbe meglio definirla della registrazione) si struttura.

Un'infinità d'iscrizioni legate all'identità e alle scelte degli aggregati di questa società vengono gratuitamente affidati agli operatori di sistema che incrementano potere[4], appropriandosi e gestendo informazioni secondo modalità un tempo prerogative esclusive dello Stato[5].

Il potere quindi si diffonde ai soggetti che gestiscono le registrazioni con un meccanismo più artificioso rispetto a quello accentrato esclusivamente nell'istituzione statale. In quest'ultima, la gestione ed il condizionamento esercitato dal potere è sempre risultato chiaramente riconoscibile, prescindendo dal fatto che esso venga o meno esercitato[6]. Nessun consociato metterebbe in dubbio che lo Stato è il detentore del potere politico e che per difenderlo si farebbe supportare dal ricorso alla forza.

Con riferimento, invece, agli operatori che raccolgono registrazioni, il meccanismo di riconoscimento risulta più complesso, in quanto gli utenti della rete

---

si caratterizza per essere registrato, su un pezzo di carta, su un file di computer, o anche solo nella testa delle persone implicate nell'atto".

[3] Ferraris, *Documentalità. Perché è necessario lasciare tracce*, Laterza, 2009, p. 208.

[4] Battelle, *Google e gli altri. Come hanno trasformato la nostra cultura e riscritto le regole del business*, Raffaello Cortina Editore, 2006, p. 25, secondo cui "Se Google e le altre società dello stesso tipo sanno quello che vuole il mondo, le più potenti organizzazioni cominciano ad interessarsi a loro e gli individui più vulnerabili temono questa minaccia. Incisi nel silicio degli oltre 150.000 server di Google ci sono i clickstrem agonizzanti di un gay malato di AIDS, le silenziose intenzioni di un potenziale costruttore di bombe, le briciole di pane digitali di un serial killer. Attraverso società come Google e i risultati che offrono, l'identità digitale di un individuo viene immortalata e può essere recuperata su richiesta. Per il momento – mi ha assicurato Sergey Brin, uno dei fondatori di Google – queste richieste non vengono né avanzate né soddisfatte. Ma di fronte a simili e potenti pressioni quanto potrà durare?".

[5] Ferraris, *Documentalità. cit.*, p. 218.

[6] Searle, *Creare il mondo sociale. La struttura della civiltà umana*, Raffaello Cortina Editore, 2010, p. 194.

sono indotti a individuare in essi il valore istituzionale di chi estende le libertà del singolo e non certo il disvalore di chi ne vincola e controlla il libero arbitrio. In breve, detti operatori sono riconosciuti ed accettati dai loro utilizzatori come istituzione positiva perché questi ultimi sono portati a riconoscere in loro solo gli aspetti positivi dell'opera, non le conseguenze perniciose, sino al punto di individuare nella privacy non più un diritto da difendere e tutelare, ma una minaccia alla libera conoscenza[7].

3. È il tempo di pretendere una maggiore disciplina per i service provider?

Il riconoscimento e la fiducia accreditati a chi agevola la comunicazione su internet avvengono, come precedentemente sostenuto, quasi con inconsapevolezza[8], in quanto rimanendo abbagliati dagli enormi vantaggi offerti dalla tecnologia applicata ad Internet si è meno portati a riflettere che si è accettato un sistema di società in cui ogni utente esercita potere sull'altro[9] e tutti sottostanno al potere di chi raccoglie registrazioni.

Per valutare che responsabilità riconoscere ai citati operatori, non si potrà prescindere dal rapporto intercorrente tra consenso sociale e istanza punitiva[10]. Affinché l'intervento penale risulti efficace è necessario che sia legittimato, ossia che lo Stato intervenga con forza laddove la comunità ne faccia istanza. Se la sanzione intervenisse a reprimere fatti di soggetti che godono dell'approvazione collettiva, la risposta punitiva potrebbe essere considerata, dalla comunità, iniqua tanto da meritare censure informali, che minerebbero la forza prescrittiva della norma violata.

La conclusione deducibile da siffatta premessa è che finché gli operatori che offrono servizi su Internet saranno percepiti dall'opinione pubblica come alfieri della libertà e dell'emancipazione, ogni statuizione giudiziale che andrà a criminalizzare il loro operato non potrà mai essere sostenuta dal consenso sociale.

---

[7] Riva, *Psicologia dei nuovi media*, Il Mulino, 2008, p. 228.

[8] Foucault, *Il soggetto e il potere, in La ricerca di Michael Focault. Analitica della verità e storia del presente*, La casa Usher, Firenze, 2000, p. 277 ss., secondo cui le persone sanno quello che fanno, ma non sanno cosa comporta quello che fanno.

[9] Searle, *Creare il mondo sociale. La struttura della civiltà umana*, cit., p. 212, che si chiede "Chi esercita il potere sui chi?" per poi rispondersi "chiunque accetti i presupposti del Background, e sappia che questi presupposti sono ampiamente diffusi nella comunità, può esercitare potere su chiunque violi tali presupposti".

[10] Donini, *Europeismo giudiziario e scienza penale. Dalla dogmatica classica alla giurisprudenza-fonte*, Giuffrè, 2011, p. 77 che afferma "La magistratura, in generale, realizza oggi un rapporto diretto fra il potere pubblico e i singoli cittadini: ciò che la scienza giuridica non ha mai fatto e la politica ufficiale ha ormai smesso di fare da tempo. La magistratura <<compensa il "deficit democratico" della decisione politica ormai votata alla pura gestione e dà alla società quel referente simbolico sempre meno identificabile nel parlamento>>; essa si rende *interprete dei diritti* di tutti, e talora delle minoranze, spesso contro le ragioni particolari o prevaricatrici della politica ufficiale, e lo fa "dal basso", cioè partendo dai casi, dalle pretese dei singoli interessati.

Sintetizzando quanto argomentato in precedenza:

1) operatori come Google, Facebook e altri hanno inaugurato nuove frontiere di libertà per l'utente della rete, in cui questi può manifestare gli aspetti reali e/o virtuali della personalità;

2) l'utente della rete percepisce il godimento di maggiori possibilità;

3) l'aumento della libertà di manifestazione del pensiero e della possibilità di accedere ad una illimitata fonte di conoscenza risulta proporzionale all'incremento di potere degli operatori di cui al punto 1), nella misura in cui questi raccolgono e dispongono di milioni di informazioni personali;

4) i predetti operatori, pur di raccogliere il maggior numero d'iscrizioni, ottemperano alle prescrizioni a tutela della privacy e degli altri diritti aggredibili da pubblicazioni *on line* secondo un protocollo minimale;

5) gli utenti della rete, pur di beneficiare dei vantaggi di cui ai punti 1) e 2), consapevolmente rinunciano a parte della propria privacy ed inconsapevolmente forniscono informazioni ai suesposti operatori, divenendo involontariamente bersaglio o di potenziali ricatti o di campagne persuasive, che possono trasformarli da soggetti critici in passivi destinatari di promozioni pubblicitarie;

6) qualsiasi intervento penale atto a punire l'omissione di controlli o finalizzato ad imporre più severe prescrizioni nella fase di raccolta delle informazioni da parte dei predetti operatori, può risultare delegittimato dal consenso sociale se va a pregiudicare i vantaggi conseguiti dagli utenti della rete, descritti ai punti 1) e 2);

7) in merito alla questione relativa alla responsabilità penale dei Service provider, la domanda che bisogna porsi non deve essere né quella di "come punire" la condotta degli operatori che omettono di eseguire controlli sul materiale pubblicato *online* o ottemperano in maniera poco diligente alle prescrizioni impartire in tema di privacy, né quella di chiedersi "se le predette condotte perfezionino reati".

Ciò su cui, invece, ci si deve interrogare è "*che cosa si deve tollerare come crimine? O ancora: che cosa sarebbe intollerabile non tollerare?"* [11].

Alla luce di quanto sostenuto nella sentenza in commento, si può concludere affermando che il giudizio espresso dal Tribunale di primo grado può essere considerato di 'buon senso', che tuttavia non è sostenibile dalla normativa penale disponibile senza incorrere in violazione di legge e che attualmente la raccolta di dati personali da parte di soggetti come *Google* non può essere criminalizzata, almeno finché non si dimostri che quest'ultimo, pur di incrementare gli accessi al proprio servizio, consapevolmente abbia acconsentito alla registrazione e al mantenimento d'iscrizioni illecite o dal contenuto illecito.

---

[11] Foucault, *Nascita della biopolitica. Corso al Collège de France (1978-1979)*, (2004), Feltrinelli, 2012, p. 211, che individua il problema della penalità nelle domande di Becker, in *Crime and Punishment: An Economic Approch*, in *Journal of Political Economy*, 2, 1968, p.40 "How many offenses should be permitted and how many offenders should go unpunished?".

La tutela dei minori dal cyberbullismo
non passa attraverso la condanna di Google

di Maurizio De Giorgi (∗)

1. Google / Vividown: il fatto non sussiste.

La sentenza resa dalla prima sezione penale della Corte d'Appello di Milano, depositata il 27 febbraio 2013, manda assolti con la formula "perché il fatto non sussiste" i tre manager di Google Italia che, nel febbraio 2010 erano stati condannati, in primo grado, per la diffusione nella rete internet di un filmato che riprendeva un giovane studente disabile di Torino mentre veniva vessato, e malmenato, da un gruppo di compagni di scuola. Assolti, già in primo grado, dalle accuse di diffamazione, i dirigenti di Google Italia erano stati condannati a 6 mesi di reclusione (pena sospesa) per violazione della privacy (si imputava ai tre di aver, in concorso omissivo tra loro, violato, tra le altre norme, anche l'art. 167 d.lgs. 30 giugno 2003, n. 196 con relativo nocumento per la persona interessata) ([1]).

La questione, come noto, ha suscitato vasta eco ([2]) tra gli operatori del diritto e tra gli operatori di internet perché lungi dal "molto rumore per nulla", secondo la citazione utilizzata dalla sentenza di primo grado, si è di fronte ad una vicenda molto complessa ed articolata che attiene, come affermano i Giudici di appello, alla questione del "governo di internet"; per la sua esatta qualificazione giuridica e per la sua soluzione, impone ai giudici di perimetrare l'ambito della responsabilità penale degli operatori di internet ([3]).

(∗) In *Questioni di diritto di famiglia*.

([1]) "La condotta penalmente rilevante che viene riconosciuta in capo ai responsabili di Google Italia s.r.l. sarebbe quella di aver gestito il servizio offerto da Google Video, omettendo di fornire (colpevolmente) ai propri inserzionisti telematici chiare e puntuali informazioni sulla corretta modalità del trattamento dei dati personali, con riferimento a quei dati appartenenti alle persone che compaiono nel video, diverse da quelle che tale video hanno immesso nella rete; avrebbero fatto ciò al fine di raccogliere un numero sempre più elevato di filmati per accrescere l'interesse al servizio da parte di eventuali acquirenti di spazi pubblicitari su Internet, in tal modo concretizzandosi il dolo specifico richiesto dall'art. 167 d.lgs. 196/2003", Giuseppe Cassano, Google v. Vividown. responsabilità "assolute" e fine di internet?, in Vita Notarile, 2/2010, 2

([2]) Si consideri che dallo stesso episodio sono scaturiti tre procedimenti penali: nel primo i ragazzi che hanno trattato illecitamente i dati del soggetto ripreso sono stati condannati per violazione dell'art. 167 d.lgs. 196/2003; nel secondo procedimento chi aveva l'obbligo di impedire il fatto illecito altrui, ossia l'insegnante dei ragazzi essendo stato il video girato in Istituto tecnico di Torino, è stata condannata; il terzo procedimento è quello a carico degli amministratori di Google Italy s.r.l..

([3]) Si è precisato in dottrina: "La disciplina della responsabilità dei providers è attualmente dettata dal d. legis. n. 70/2003 (artt. 14-17) che ha pressoché recepito la direttiva comunitaria n. 2000/31/CE dell'8.6.2000 con l'intento di regolamentare la responsabilità degli operatori intermediari in modo unitario superando le divergenti normative nazionali e le diverse interpretazioni dei giudici territoriali. Il legislatore comunitario ha

2. Quale responsabilità in capo ad un *host* o *content* provider.

Secondo il Collegio di Appello "per sostenere la responsabilità a titolo di omissione in capo ad un *host* o *content provider*, occorre affermare a suo carico un obbligo giuridico di impedire l'evento e quindi, da un lato l'esistenza di una posizione di garanzia, dall'altro la concreta possibilità di effettuare un controllo preventivo".

Con riferimento alla posizione di garanzia, in maniera peraltro concorde rispetto a quanto già sostenuto dal Giudice di primo grado, la Corte sottolinea come essa non possa essere ravvisata nel diritto vigente in assenza di una specifica previsione in tal senso, di là da ogni riferimento all'auspicabilità, o meno, di una normativa che colmi questo vuoto legislativo.

Né tale posizione di garanzia può desumersi da fonte diversa, quale, in via esemplificativa, quella dettata ex art. 57, e 57 bis c.p. in materia di stampa, in quanto si tratterebbe di analogia *in malam partem*.

Con riferimento alla "concreta possibilità di effettuare un controllo preventivo" argomenta, ancora, la Corte come non possa essere ravvisata la possibilità effettiva e concreta di esercitare un pieno ed efficace controllo sulla massa dei video caricati da terzi, visto l'enorme afflusso di dati.

Affermare l'operatività di un obbligo del soggetto - web di impedire l'evento illecito, imporrebbe allo stesso un filtro preventivo su tutti i dati immessi in rete, con ciò finendo per alterarne la sua stessa funzionalità ([4]).

Anche sotto questo profilo appare condivisibile la conclusione a cui era pervenuto il Tribunale secondo cui si finirebbe per richiedere un comportamento inesigibile e di conseguenza non perseguibile penalmente ai sensi dell'art. 40 cpv. c.p..

Né, si aggiunga, la presenza di una posizione di garanzia da cui far derivare un obbligo di attivazione, in mancanza della quale far ricorrere la previsione dell'art. 40 c.p., può essere fatto derivare dalla violazione di norme di legge,

---

introdotto una disciplina generale sulla responsabilità dei providers, distinguendoli per tipologia di funzioni: semplice trasporto di informazioni, c.d. mere conduit (art. 14); memorizzazione temporanea ed automatica di informazioni, c.d. caching (art. 15); memorizzazione di informazioni fornite dal destinatario del servizio, c.d. hosting (art. 16). In tal modo, si differenziano le condizioni che integrano la responsabilità dell'intermediario in base al ruolo effettivamente svolto nel contesto dell'illecito. Nel quadro complessivo della responsabilità del provider ha un'importanza fondamentale l'art. 17 (d. legis. n. 70/2003). La norma stabilisce il fondamentale principio dell'assenza di un obbligo generale di sorveglianza sulle informazioni che esso trasmette o memorizza, nonché dell'inesistenza di un obbligo preventivo di ricercare i fatti o le circostanze che indichino la presenza di attività illecite", Emanuela Andreola, Profili di responsabilità civile del motore di ricerca, in La nuova giurisprudenza civile commentata n. 2/2012, 129.

([4]) Va escluso, secondo la Corte d'Appello, che nel periodo settembre - dicembre 2006 fosse esistente ed operante una tecnologia di filtraggio preventivo compiutamente idoneo ad identificare automaticamente i contenuti illeciti di un video.

quali quelle a protezione dei dati personali, che non hanno per oggetto tali condotte e che sono state emanate a copertura di comportamenti diversi da quelli oggetto di contestazione.

La sentenza si innesta così nel solco segnato dalla maggior parte della dottrina che, all'indomani della sentenza di primo grado, *rectius* all'indomani della formulazione dell'accusa, si è espressa sulla materia ([5]).

3. Competenza e giurisdizione.

La sentenza conferma la competenza territoriale – e quindi la possibilità di decidere nel merito della causa – del Tribunale di Milano (come già era avvenuto in primo grado), in quanto la società Google Italy ha sede a Milano e la condotta contestata riguarda tale società.

Allo stesso modo la giurisdizione – cioè l'astratta possibilità di giudicare un fatto di reato – è quella italiana perché, indipendentemente dalla localizzazione dei server, gli effetti pregiudizievoli del reato sono accaduti in Italia.

I Giudici di Appello, sul punto, si richiamano all'orientamento interpretativo della Suprema Corte (Cass. pen., sez. III, 23 dicembre 2009, n. 49437), nonché della giurisprudenza capitolina (Trib. Roma - sez. IX civile, ord. 15 – 16 dicembre 2009) secondo cui l'evento del caricamento del server è di per sé solo potenzialmente generatore di danno, ma privo di efficacia dannosa, che si verifica solo nel momento in cui i contenuti vengono diffusi nell'area di mercato ove la parte danneggiata esercita i suoi diritti, nella specie appunto il territorio italiano.

D'altra parte – evidenzia ancora la Corte - non fa venire meno la giurisdizione del giudice nazionale, neppure la circostanza che la condotta di partecipazione sia stata posta in essere all'estero quando una parte della condotta comune abbia luogo in Italia (Cass. pen., sez. V, 20 ottobre 2008, n. 39205) ([6]).

Secondo i giudici d'appello è corretta l'individuazione degli imputati come coloro ai quali attribuire le presunte condotte illecite, in quanto:

• Drummond e De Los Reyes erano legali rappresentanti di Google Italy e Drummond era "Vicepresidente e Legale Rappresentante di Google Inc., nonché Vicepresidente di Google International";

([5]) Giuseppe Cassano e Alfonso Contaldo, Identità digitale e tutela della privacy, Diritti della persona, internet e responsabilità dei soggetti intermediari – speciale, in Il Corriere Giuridico, spec. 1/2010, 5 ss.; Giuseppe Cassano. Google v. Vividown, *op. cit.*; Francesco Giuseppe Catullo, Ai confini della responsabilità penale: che colpa attribuire a Google, in Giurisprudenza di merito 1/2001, 159 ss.; Francesco Di Ciommo, Programmi-filtro e criteri di imputazione/esonero della responsabilità on-line. A proposito della sentenza Google/Vivi Down, in Il diritto dell'informazione e dell'informatica, f. 6/2010, 829 ss.

([6]) Si richiama in sentenza il principio di diritto per il quale il giudice italiano rimane competente a conoscere della diffamazione, compiuta mediante l'inserimento nella rete telematica internet, di frasi offensive e/o immagini anche nel caso in cui il sito web sia stato registrato all'estero purché l'offesa sia stata percepita da fruitori che si trovano in Italia (Cass. pen., sez. V, 27 dicembre 2000, n. 4741).

• Arvind era responsabile del progetto Google Italy.

Per quanto riguarda la posizione di Fleischer, invece, non viene data alcuna argomentazione.

4. Trattamento dei dati personali: il ruolo dell'*uploader*.

La sentenza riconosce applicabile a Google Italy la disciplina Italiana del trattamento dei dati personali in quanto detta società rientra nella nozione di strumento anche non elettronico, così come previsto dall'art. 5, comma 2, D.Lgs. n. 196/2003 (norma che menziona gli "strumenti situati nel territorio dello Stato anche diversi da quelli elettronici").

Più in particolare si afferma che la categoria dell'*hoster* attivo non è contemplata da alcuna norma di legge italiana o comunitaria, ma è assolutamente vero che l'attività svolta da Google è diversa da quella prevista dal legislatore comunitario nell'oramai lontano anno 2003.

Infatti, le possibilità di filtraggio, rimozione, selezione e raccolta materiale, indicizzazione a fini pubblicitari, dimostrano ampiamente che Google Video è un *hoster* attivo.

Detto ciò, deve essere esclusa la responsabilità per il prestatore di servizi che fornisca un servizio di *hosting* attivo, in quanto anche per tale soggetto va esclusa *ipso facto* la possibilità di procedere ad una efficace verifica preventiva di tutto il materiale immesso dagli utenti.

Altro passaggio fondamentale della sentenza consiste nell'evidenziare che il titolare del trattamento è solo l'*uploader*.

E cioè a dire, con riferimento al caso concreto, era onere dell'*uploader* che caricando il video si assumeva la responsabilità del trattamento dei dati personali chiedere, ed ottenere, il consenso prescritto da parte del soggetto ripreso nel video e tale soggetto, da parte sua, doveva ricevere l'informativa sugli obblighi di legge da parte del medesimo *uploader* (Cass. pen., sez. III, 15 febbraio 2005, n. 5728).

Sul punto si richiama anche la giurisprudenza della Corte di Giustizia Europea che, in un caso di pubblicazione di dati personali su internet, ha ritenuto titolare del trattamento il soggetto che aveva provveduto all'*uploading* (affermando che: "è la persona che crea, invia o carica i dati on line che deve essere ritenuto il titolare del trattamento dati e non la parte, il *provider*, che fornisce gli strumenti").

È poi pacifico che la valutazione dei fini di un'immagine all'interno di un video in grado di qualificare un dato come sensibile o meno, implica un giudizio semantico e variabile che certamente non può essere delegato ad un procedimento informatico.

Se a ciò si unisce la circostanza che la direttiva sul commercio elettronico (Direttiva n. 70/2003) – la cui esegesi per dirsi corretta deve essere operata in un *unicum* con la disciplina sulla *privacy* (D.Lgs. n. 196 cit.) – chiarisce che non vi è alcun obbligo di controllo preventivo, diventa allora evidente che la valuta-

zione del contenuto trasmesso in rete compete al titolare e che il titolare non può essere certamente individuato in Google Italy.

5. Art. 167 Codice della *privacy*: il dolo specifico.

Il colpo di grazia all'impianto accusatorio, sotto il profilo dell'elemento soggettivo del reato contestato, viene dato dalla sentenza nella parte in cui chiarisce che non è rinvenibile il dolo specifico richiesto dalla norma (art. 167 Codice della privacy) giusta l'assenza di qualsiasi riscontro di un vantaggio direttamente conseguito dagli imputati grazie alla condotta dagli stessi tenuta nell'ambito di un servizio gratuito quale era quello offerto, ed in assenza di link pubblicitari associati allo specifico video oggetto del procedimento penale ([7]).

La Corte, superando l'argomentare del giudice di primo grado, sottolinea come l'attività dell'azienda, nei suoi molteplici servizi, non può che essere considerata lecita e non può essere assunta a prova della sussistenza del dolo.

La Corte supera anche – accedendo ad una opzione interpretativa di segno negativo – il problema della compatibilità tra la forma del dolo eventuale (dalla sentenza di primo grado individuata in capo agli imputati per avere serbato una "voluta disattenzione" nelle politiche societarie relative al trattamento della *privacy*, al fine dell'ottenimento di buoni risultati di mercato) ed il dolo specifico richiesto dalla norma dell'art. 167 cit..

La soluzione in senso positivo, non è accettabile, in quanto la struttura della fattispecie di cui all'art. 167 Codice privacy postula la necessaria partecipazione psichica intenzionale e diretta del soggetto al raggiungimento di un profitto.

([7]) Secondo la Suprema Corte: "si è (…) al cospetto di un reato di pericolo effettivo e non meramente presunto (..) con il risultato che la illecita utilizzazione dei dati personali è punibile, non già in sé e per sé, ma in quanto suscettibile di produrre nocumento (cosa che, ovviamente, deve essere valutata caso per caso) alla persona dell'interessato e/o al suo patrimonio" (Cass. pen., sez. III, 15 giugno 2012, n. 23798). Ed ancora "Il D.Lgs. n. 196 del 2003, art. 167, ha tipizzato il (…) nocumento, da intendersi, sia riferito al soggetto stesso, che al suo patrimonio, come condizione obiettiva di punibilità (introducendo anche un dolo specifico di danno)" (Cass. pen., sez. V, 02 dicembre 2011, n. 44940). Si vedano anche: Cass. pen., sez. III, 29 settembre 2011, n. 35296; Cass. pen., sez. III, 4 maggio 2011, n. 17215; Trib. Taranto, sez. II, 11 luglio 2012; Trib. Ruvo di Puglia, 19 gennaio 2009.

Esclusa la responsabilità penale di Google per violazione di dati personali da parte di materiale multimediale immesso da terzi

di Elena Bassoli (*)

1. Introduzione

Le particolari caratteristiche tecniche di Internet rendono spesso problematica l'individuazione e la punizione del responsabile di illeciti commessi attraverso la rete.

Se da un lato l'utente che accede ad un sito lascia sempre una traccia identificabile, d'altra parte non è impossibile che il responsabile riesca ad utilizzare segretamente un terminale normalmente utilizzato da un altro utente, o ad appropriarsi di un'altra identità "telematica", reale o fittizia; inoltre, il responsabile potrebbe essere difficilmente perseguibile, ad esempio in quanto si trova all'estero; infine la repressione degli illeciti commessi attraverso Internet pone sempre l'annoso problema del foro competente, che talora viene individuato nel luogo da cui è stato inviato il testo o l'immagine, talora in quello in cui si trova il server che ospita il sito, talora, ancora, nel luogo da cui il testo o l'immagine è stato ricevuto .

Per questa ragione si punta a coinvolgere nell'attività di controllo i providers , accollando agli stessi la responsabilità di quanto viene immesso, diffuso o scambiato in rete attraverso i servizi di comunicazione messi a disposizione .

Tuttavia considerare l'Internet provider in qualche modo responsabile delle violazioni commesse da un qualsiasi utente tramite il suo server appare sproporzionato rispetto alla concreta necessità di individuare un soggetto responsabile della violazione. Vi possono essere sì delle responsabilità, ma dovute principalmente all'imperizia nello svolgere una preventiva analisi del soggetto che intende immettere contenuti in rete .

Le tecnologie di Internet consentono di inviare messaggi, immagini, filmati ed ogni altro tipo di comunicazione all'interno di piattaforme multimediali, come quella del caso che ci occupa, oppure *forum*, *blog*, *newsgroup*, *mailing list*, *chat line*, e di costruire pagine Web personali.

Tutte le forme di limitazione pensate o pensabili verso Internet sono inutili in quanto è praticamente impossibile pensare ad Internet come ad uno strumento censurabile. Tuttavia ciò comporta il rischio che diverse violazioni possano verificarsi sui siti della rete[1].

(*) In *Rivista penale*.

[1] Tra i possibili illeciti commessi su Internet si possono individuare diversi casi, ad esempio la violazione delle norme sul diritto d'autore, che si realizza quando documenti, immagini ed altre opere protette vengono riprodotte e pubblicate sulla rete senza la necessaria autorizzazione da parte dell'autore o del titolare dei diritti su di esse; la diffamazione, mediante l'invio di materiale offensivo su un sito della rete; la violazione delle norme contro lo sfruttamento sessuale dei minori, con la pubblicazione di materiale pedopornografico; la violazione delle norme sull'ordine pubblico, con la pubblicazione, ad esempio, di materiale di stampo terroristico; la violazione del diritto alla tutela

Vi sono così periodici tentativi di configurare in capo al provider forme di responsabilità oggettiva che però hanno incontrato la più netta opposizione da parte degli operatori del settore e anche di buona parte della dottrina più attenta.

2. Le questioni pregiudiziali: giurisdizione e competenza vs. a-territorialità di Internet

La sentenza qui in oggetto affronta diverse interessanti tematiche attinenti il reato di trattamento illecito di dati personali ai sensi del d. lgs. 196/2003 e la responsabilità dei provider per l'ormai noto caso Google-Vividown, approdato ormai all'epilogo del suo secondo grado con la sentenza della Corte d'Appello di Milano del dicembre scorso.

La prima sezione della Corte di Appello di Milano ha, in parziale riforma della precedente statuizione di primo grado[2], ritenuto di assolvere tre dirigenti della società Google, già ritenuti non colpevoli di concorso nel reato di diffamazione, dalle residue accuse di trattamento illecito di dati personali ex. D. lgs. 196/2003.

Nel 2010 i tre responsabili del colosso americano erano stati condannati a sei mesi per violazione della privacy: il verdetto che aveva fatto il giro del mondo, anche perché si trattava del primo processo, in ambito internazionale, ai dirigenti di un Internet provider per la pubblicazione di contenuti sul web[3].

Lo scorso dicembre, però, la prima sezione della Corte d'appello di Milano ha ribaltato il giudizio, assolvendo i tre manager "perché il fatto non sussiste" e confermando anche il proscioglimento per un quarto dirigente che rispondeva solo di diffamazione: un'accusa già caduta in primo grado.

La sentenza d'appello conferma anzitutto che la competenza territoriale – e quindi la possibilità di decidere nel merito della causa – è del Tribunale di Milano, in quanto la Società Google Italy ha sede a Milano e la condotta contestata riguarda tale società.

Allo stesso modo la giurisdizione – cioè l'astratta possibilità di giudicare un fatto di reato – è quella Italiana perché, indipendentemente dalla localizzazione dei server, gli effetti pregiudizievoli del reato sono accaduti in Italia.

Secondo i giudici d'appello è corretta anche l'individuazione degli imputati come coloro ai quali attribuire le presunte condotte illecite, in quanto i due erano i legali rappresentanti di Google Italy e il terzo era "Vicepresidente e Legale Rappresentante di Google Inc., nonché Vicepresidente di Google International".

---

dei dati personali, che si ha quando dati riservati o segreti relativi ad un individuo o ad un'organizzazione vengono resi pubblici su un sito Internet, la concorrenza sleale, nel caso di informazioni false o diffamatorie messe in rete tra imprese concorrenti; la violazione delle norme sulla protezione dei marchi e dei nomi a dominio, la sostituzione di persona.

[2] G. CAMERA, O. POLLICINO, *La legge è uguale anche sul web. Dietro le quinte del caso Google-Vividown*, Milano, 2010.

[3] G. SARTOR, M. VIOLA, *Il caso Google-Vividown tra protezione dei dati e libertà di espressione* on line, in Dir. Inf., Giuffré, 2010, 645.

Inoltre, è applicabile la disciplina della privacy Italiana a Google Italy in quanto la società italiana può rientrare nella nozione di strumento, anche non elettronico, così come previsto dall'art. 5 comma 2 della Legge Privacy.

In astratto, secondo questo articolo, è applicabile la legge italiana o quando il trattamento è svolto da soggetti stabilito nel territorio italiano, o quando il trattamento è effettuato da un soggetto che, seppur straniero, impiega comunque strumenti situati nel territorio dello Stato.

I giudici hanno ritenuto di confermare quanto assunto già dal giudice di prime cure affermando che la condizione risultava soddisfatta poiché in Italia vi era la sede di Google Italy, la controllata italiana di Google Inc., nonostante i server fossero collocati negli Usa[4].

Peraltro la soluzione adottata in merito alla giurisdizione non risulta del tutto condivisibile se solo si pone mente al fatto che lo stesso Garante della Privacy[5] in passato ha affermato che l'elaborazione dei dati effettuata da Google negli Stati Uniti, anche con dati trasmessi da *utenti italiani, non è soggetta alla legge italiana. L'importanza di questo aspetto appare ictu* oculi di decisiva rilevanza; ed infatti se la questione pregiudiziale fosse stata accolta in questi termini la decisione sarebbe risultata *tranchante* di ogni altro aspetto di merito.

3. Sulla diffamazione

Dal punto di vista dell'analisi delle prove, il Procuratore Generale non fornisce elementi in grado di cambiare la decisione di primo grado, e quindi di ribaltare il giudizio di assoluzione in merito al reato di diffamazione.

E ciò perché si ritiene, anche in accordo con il d. lgs. 70/2003 sul commercio elettronico, in attuazione della direttiva 31/2000[6], che non possa esistere, ai sensi del diritto vigente, una posizione di garanzia (e cioè un obbligo di impedire eventi offensivi di beni altrui) ex art. 40 c.p. in capo a Google in quanto, nel periodo settembre-dicembre 2006, non esisteva né un obbligo giuridico di impedire l'evento né meccanismi di controllo sui contenuti immessi in rete in grado di poter far sorgere una qualsiasi forma di obbligo[7].

Già il giudice di prime cure aveva inoltre rilevato come in capo agli imputati mancasse il dolo, vale a dire la coscienza e volontà di concorrere con altri nella realizzazione del reato[8].

---

[4] Peraltro i controlli sui contenuti caricati su tale piattaforma sono effettuati in Irlanda dalla controllata Irlandese di Google Inc.

[5] Provv. Garante Privacy 3.11.2009, rinvenibile all'url http://www.garanteprivacy.it.

[6] Sui rapporti tra direttiva europea e norme di recepimento degli Stati membri cfr. R. BOCCHINI, *La responsabilità civile degli intermediari del commercio elettronico. Contributo allo studio dell'illecito plurisoggettivo permanente*, Napoli, 2003.

[7] G.M. RICCIO, *Profili di responsabilità civile dell'Internet Provider*, Salerno, 2000, 78.

[8] G. PINO, *Tra anarchia e caccia alle streghe. Alterne vicende della libertà di manifestazione del pensiero in Internet*, in "Ragion pratica", 2001, 133.

Il fatto che vi sia stata remissione di querela da parte dell'Associazione Vividown nell'ambito del primo grado di giudizio, non fa diventare inammissibile l'appello del Pubblico Ministero poiché l'assoluzione in primo grado, confermata dai giudici d'appello, è sicuramente un risultato migliore rispetto alla dichiarazione di estinzione del reato per intervenuta remissione della querela.

Nello stesso filone di esclusione della responsabilità del provider per diffamazione si inserisce la sentenza 20 agosto 2007 del Tribunale Civile di Lucca[9], al quale la ricorrente si era rivolta per chiedere, ex art. 700 c.p.c., la rimozione, a cura e spese di controparte, di alcuni giudizi ed espressioni apparse su un newsgroup non moderato, relative a prodotti della stessa, ritenute diffamatorie e lesive del suo onore e decoro.

Il Giudice, richiamando il D.Lgs. n. 70/2003 sul c.d. "commercio elettronico", ribadisce l'esclusione della responsabilità per il contenuto dei messaggi sia in capo al mero fornitore di servizi di connessione ad Internet, sia per l'operatore che consente l'accesso al newsgroup cos' motivando: "*diversamente si verrebbe ad introdurre una nuova ed inaccettabile ipotesi di responsabilità oggettiva, in aperta violazione alla regola generale di cui all'art. 2043 c.c. che, come è noto, fonda la responsabilità civile sulla colpa del danneggiante*".

Quindi, anche in materia di messaggi pubblicati su newsgroup, non sussiste un obbligo generale di sorveglianza del provider sulle informazioni che trasmette o memorizza.

Il Giudice, inoltre, nell'escludere il carattere diffamatorio dei messaggi relativi al prodotto commercializzato dal ricorrente, il quanto manifestazioni del diritto di critica, richiama l'orientamento per cui l'eventuale natura diffamatoria del messaggio va valutata alla stregua non solo delle espressioni utilizzate, ma anche del tipo di comunicazione: nella specie, i messaggi vengono ritenuti corretti anche perché "*inseriti in un forum, e dunque in linea con i toni informali che caratterizzano lo scambio diretto di opinioni su Internet*".

4. Aspetti tecnici dell'attività degli intermediari di Internet: Google Video è un Hosting Provider Attivo

La categoria dell'*Hoster* attivo non è contemplata da alcuna norma di legge italiana o comunitaria, ma è assolutamente vero che l'attività svolta da Google è diversa da quella prevista dal legislatore comunitario nell'oramai lontano anno 2000.

Di ciò anche il giudicante pare essersi reso conto soprattutto quando afferma che la posizione di Google si pone a metà strada tra quella dell'*hosting provider* e quella del *content provider*.

Così la Corte d'Appello rileva come l'evoluzione della rete informatica mondiale sembra però avere superato nei fatti la figura di mero prestatore di servizio, che veniva elaborata all'epoca della citata direttiva e che delineava tale soggetto come del tutto estraneo rispetto alle informazioni memorizzate, sia a

[9] http://www.altalex.com/index.php?idnot=39009, con nota di Panfili.

livello di gestione che di regolamentazione contrattuale con i destinatari del servizio.

Oggi, i servizi offerti dall'Isp non si limitano al processo tecnico che consente di attivare e di fornire l'accesso alla rete ma, come nel caso del *content provider*, arrivano ad offrire la possibilità di immettere contenuti propri o di terzi nella rete e dunque non possono non essere chiamati a rispondere secondo le comuni regole di responsabilità in materia di trattamento dei dati.

Nella sentenza si arriva a delineare un'ulteriore categoria denominata di *hosting attivo*, cioè di prestatore di servizi non neutra rispetto all'organizzazione ed alla gestione dei contenuti degli utenti, caratterizzata anche dalla possibilità di un finanziamento economico attraverso l'inserimento di inserzioni pubblicitarie.

Questa categoria in realtà, non è presente in alcuna norma di legge ma risulta fondata su una costatazione fattuale del ruolo svolto dall'Isp, è frutto dell'elaborazione di numerose pronunzie in materia di responsabilità.

Secondo il d. lgs. 70/2003 sono individuabili tre principali categorie di operatori telematici.

La prima riguarda i "connection provider" (o Isp), ossia quei soggetti che forniscono agli utilizzatori di Internet l'accesso alla Rete. Vi sono poi i "server provider", i quali mettono a disposizione uno spazio di memoria sui siti Internet. Normalmente le due figure appena delineate coincidono. La terza categoria interessa i "content provider", vale a dire una categoria eterogenea di soggetti che forniscono la documentazione elettronica caricata su un sito affinché possa essere visualizzata. Si possono ricordare, tra gli altri, gli autori delle opere multimediali, chi scrive *e-mail* o messaggi ovvero partecipa, ad esempio, a gruppi di discussione .

E proprio in ragione dell'attività svolta dai prestatori il legislatore ha ritenuto di dover diversificare le responsabilità di cui ai tre articoli sopra menzionati.

Si è così inquadrata, all'art. 14, la figura di *mere conduit*, consistente nel servizio di mero trasporto delle informazioni, si pensi ai servizi di accesso alla rete che consentono la trasmissione di informazioni. in questo caso per il prestatore, in via generale, vige l'assenza di un obbligo di verifica del contenuto delle informazioni che vengono memorizzate, o trasmesse sui propri *server* e si subordina la responsabilità alla sussistenza di diverse condizioni, quali l'aver originato la trasmissione, l'aver selezionato il destinatario della trasmissione oppure aver selezionato o modificato le informazioni trasmesse.

Tale scelta, sia a livello europeo, sia nazionale, è frutto della considerazione che l'intermediario di servizi Internet di accesso, è assimilabile al ruolo svolto da una compagnia telefonica (*carrier*) e, quindi, non responsabile dei contenuti di una eventuale comunicazione digitale lesiva di diritti. questa conclusione si ricollega ad analoga conclusione cui si è pervenuti oltreoceano con una pronuncia Usa della Corte Suprema del 2000.

In tale occasione, relativa ad un caso di diffamazione a mezzo Internet, il collegio ha confermato la sentenza della corte d'appello dello stato di New

York, secondo la quale il provider (Prodigy) è stato il semplice veicolo attraverso cui è transitato il messaggio offensivo, sicché avendo un ruolo passivo, vale a dire non essendo l'autore del reato, assimilabile a quello di una compagnia telefonica, non è stato riconosciuta la sua responsabilità in ordine ai contenuti della comunicazione digitale offensiva.

Nel caso disciplinato dall'art. 15, invece, relativo all'attività di *caching*, si è esclusa la responsabilità del provider in ordine alla memorizzazione automatica e temporanea effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta.

L'esclusione della responsabilità, ad ogni modo, è condizionata al rispetto di cautele ed obblighi da parte del provider, così come previsto dal considerando 33 della direttiva, sostanzialmente riassumibili nel divieto di modificare le informazioni veicolate, nell'obbligo di rimuovere prontamente le informazioni una volta che il fornitore del servizio sia stato messo al corrente della loro illiceità, nell'astenersi dal compromettere l'uso della tecnologia diffusa in quel dato momento per risalire alle destinazioni delle informazioni, nel disabilitare l'accesso o rimuovere le informazioni su ordine dell'autorità amministrativa o giudiziaria.

All'art. 16, che disciplina l'attività di memorizzazione permanente (hosting) è previsto che il provider sia responsabile delle informazioni lesive di altrui diritti se era al corrente che l'attività o l'informazione erano illecite o di fatti o circostanze che non rendevano manifesta l'illegalità dell'attività o dell'informazione o se, non appena al corrente di tali fatti, non abbia agito immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

Già la giurisprudenza di merito aveva escluso la responsabilità del provider «che si limiti a ospitare sul proprio server una tabella di informazioni caricatavi da un proprio cliente, e costituente violazione di un altrui diritto d'autore»

Peraltro, nel caso che qui ci occupa, le possibilità di filtraggio[10], rimozione, selezione e raccolta materiale, indicizzazione a fini pubblicitari, dimostrano ampiamente che Google Video è un Hoster attivo[11].

Detto ciò, la responsabilità[12] prevista dal capo di imputazione A) è stata dal giudice di secondo grado esclusa anche per il prestatore di servizi che fornisca un servizio di hosting attivo, in quanto anche per tale soggetto va ritenuta insus-

[10] Circa l'utilizzazione dei filtri da parte dei *provider*, cfr. J.P. SEMITSU, *Burning Cyberbooks in Public Libraries*: *Internet filtering software vs. The first amendement*, 52 Stan. L. Rev 509, 2000.

[11] Nel 2006 Google aveva acquistato YouTube e Google Videos aveva quindi assunto la funzione prevalente di motore di ricerca dei filmati.

[12] F. DI CIOMMO, *Internet* (responsabilità civile), voce dell'Enc. Giur. Treccani, Aggiornamento 2002 Roma, 2002.

sistente *ipso facto* la possibilità di procedere ad una efficace verifica preventiva di tutto il materiale immesso dagli utenti[13].

A questo riguardo si osserva come il monitoraggio di tutte le attività svolte in rete sia praticamente impossibile, e che in ogni caso richiederebbe un impiego di mezzi e di personale tali da consentire solo agli operatori maggiori, più forti economicamente, di rimanere sul mercato; infine la responsabilità del provider finirebbe con l'attribuire funzioni censorie e di controllo preventivo, incompatibili con le garanzie della libertà di manifestazione del pensiero, costituzionalmente garantite dall'art. 21 Cost.

5. Il trattamento illecito di dati personali: Google non è titolare dei dati

Le violazioni compiute su Internet sono disciplinate in Italia da una serie di disposizioni a seconda del tipo di illecito.

Per attribuire una responsabilità all'Internet provider per fatti commessi da terzi si è fatto inizialmente ricorso alle norme sulla responsabilità dell'editore di una testata giornalistica ed in particolare all'art. 57 c.p.([14]), relativo ai reati commessi a mezzo di stampa, equiparando il gestore di un sito Internet ad un responsabile editoriale e attribuendogli l'obbligo di verificare la legittimità di tutto il materiale pubblicato sul proprio server, compreso quello inviato da terzi.

Nell'evidenziare che il titolare del trattamento è solo l'uploader, la Corte sottolinea che la valutazione di un'immagine in grado di qualificare o meno un dato sensibile implica un giudizio semantico che non può essere certamente legato ad un procedimento informatico. Se a ciò si unisce la circostanza che la direttiva sul commercio elettronico (Direttiva n. 70/2003) – da leggere unitamente alla disciplina sulla privacy – chiarisce che non vi è alcun obbligo di controllo preventivo, diventa evidente che la valutazione del contenuto trasmesso in rete compete al titolare e che il titolare non può essere certamente Google Italy.

Parte della dottrina ha fatto inoltre riferimento all'art. 30 della Legge n. 223/90[15] che attribuisce gli stessi obblighi dell'editore di una testata giornalisti-

---

[13] G. PASCUZZI, *Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche*, Bologna, 2003, 127, che si pone invece a favore di una responsabilità dei provider.

[14] Art. 57 c.p.: *Reati commessi col mezzo della stampa periodica*. Salva la responsabilità dell'autore della pubblicazione e fuori dei casi di concorso, il direttore o il vicedirettore responsabile, il quale omette di esercitare sul contenuto del periodico da lui diretto il controllo necessario ad impedire che col mezzo dalla pubblicazione siano commessi reati, e' punito, a titolo di colpa, se un reato e' commesso, con la pena stabilita per tale reato, diminuita in misura non eccedente un terzo. Art. 57-*bis* c.p. Reati commessi col mezzo della stampa non periodica. Nel caso di stampa non periodica, le disposizioni di cui al precedente articolo si applicano all'editore, se l'autore della pubblicazione è ignoto o non imputabile, ovvero allo stampatore, se l'editore non e' indicato o non e' imputabile.

[15] Legge 6 agosto 1990, n. 223 Pubblicata nella Gazzetta Ufficiale della Repubblica italiana del 9 agosto 1990, n. 185" recante "Disciplina del sistema radiotelevisivo pubblico e privato.

ca al gestore di una radio o di una televisione. Il provider sarebbe quindi corresponsabile dell'illecito del terzo utente sulla base di una sorta di *culpa in vigilando*, consistente nel mancato adempimento dell'obbligo di monitoraggio del materiale inviato sul proprio server, obbligo sancito appunto dagli artt. 57 c.p. e 30 della Legge n. 223/90.

Tuttavia le previsioni di cui alla l. 47/1948 devono trovare applicazione solo nel caso in cui il sito Internet sia registrato come testata.

Con l'art. 17, rubricato "assenza dell'obbligo generale di sorveglianza" sembra essersi attuato il definitivo superamento di alcune posizioni della giurisprudenza in materia tendenti a configurare in capo all'Isp una *culpa in vigilando* identica a quella che grava sul responsabile editoriale di un organo di stampa[16]. Contro l'ammissibilità di tale posizione già ostava una consolidata giurisprudenza della corte di cassazione, in materia penale[17] in base alla quale, ai fini della configurabilità di una fattispecie criminosa come reato commesso con il mezzo stampa, le definizioni di "stampa" e "stampati" fornite dall'art. 1 della legge 8 febbraio 1948, n. 47 non sono suscettibili di interpretazione analogica e/o estensiva: né la rete, dunque, né un sito *web* potevano essere correttamente configurati come "stampa".

Ad analoga conclusione può giungersi a proposito della posizione dottrinale, ormai anch'essa ampiamente superata, di ricorrere non all'istituto della *culpa in vigilando*, quanto a quello della responsabilità c. d. oggettiva per lo svolgimento di attività pericolose *ex* art. 2050 cod. civ. peraltro richiamato dallo stesso d. lgs. 19672003 in materia di violazione dei dati personali, in base alla quale il *provider* era responsabile civilmente per fatto illecito nel caso in cui un utente avesse arrecato ad altri un danno ingiusto e l'Isp non provasse di aver adottato preventivamente tutte le misure idonee per evitare tale danno, tra cui si faceva rientrare il monitoraggio delle informazioni che transitavano o venivano depositate sul *server*. tale posizione era stata oggetto di critiche sulla base della inequiparabilità dell'attività di prestazione di servizi posta in essere dall'Isp alle attività pericolose generalmente riconosciute da dottrina[18] e giurisprudenza[19].

---

[16] Si allude all'ordinanza adottata l'8 agosto 1996 dal tribunale di Napoli nella quale il *provider* è stato ritenuto responsabile a titolo di colpa per aver "autorizzato, consentito o comunque agevolato il comportamento illecito di un utente" che aveva diffuso in rete messaggi promozionali contenenti nomi e marchi appartenenti a società concorrenti, realizzando così un atto di concorrenza sleale.

[17] Cass. Pen. 3.2.89, *GP*, 1990, II, 74 in tema di videocassette registrate.

[18] F. GIOIA, *I soggetti dei diritti*, in Aida, XI, 83-84, 2002.

[19] Da rilevare, che, in ogni caso, lungi dall'irresponsabilità totale dell'intermediario, vige comunque una tutela, ad esempio per l'autore di opere immesse in Internet, così come riconosciuto, oltreché dalla stessa direttiva (considerando n. 59), anche da parte della dottrina (F. GIOIA, cit.) che rileva come «*la stessa direttiva (2001/29) riconosce tuttavia ai titolari dei diritti la facoltà di chiedere un provvedimento inibitorio contro un provider che consenta violazioni in rete da parte di un terzo contro opere protette, e questo anche ove gli atti svolti dall'intermediario siano soggetti ad eccezione ai sensi dell'art. 5*». Quanto sopra evidenziato è reso possibile dalla stessa direttiva 2000/31/ce

Anche la giurisprudenza si è mostrata finora alquanto riluttante a interpretare il dettato normativo in modo così estensivo: si è infatti ritenuto che l'attribuzione al provider di "obblighi di controllo e di verifica dell'attività svolta dall'utente sul sito", se da un lato manifesta "l'avvertita esigenza di consentire, sempre, di fronte alla commissione di un fatto illecito, l'individuazione di almeno un soggetto responsabile" d'altra parte appare "di difficile se non impossibile attuazione, a fronte, sempre, dei meccanismi di funzionamento della rete, risolvendosi in una forma di trasferimento del rischio dell'attività sul soggetto più facilmente identificabile ed aggredibile ed attribuendo oltretutto al provider l'improprio compito di stabilire se interrompere o meno il servizio fornito all'utente, effettuando cosi valutazioni soggettive circa l'illiceità dell'attività svolta dall'utente, azioni che di sicuro non competono a tali soggetti[20].

Quindi le disposizioni riguardanti gli articoli 2050 cod. civ.[21] e 2051 cod. civ.[22] non sono spesso configurabili con l'attività del provider poiché presuppongono un effettivo potere di controllo sull'attività o sulla cosa. La giurisprudenza sembra quindi orientata ad applicare i principi generali della responsabilità civile di cui all'art. 2043 cod. civ. [23] che impone la distinzione caso per caso in base al servizio fornito[24].

Interessante al proposito appare l'ordinanza 8 agosto 1996 del Tribunale di Napoli[25] con la quale venne affermata la responsabilità extracontrattuale ex art. 2043 cod. civ. di un utente colpevole di aver diffuso in rete messaggi promozionali contenenti nomi e marchi appartenenti a società concorrenti.

Il giudice di Napoli riconobbe gli estremi della concorrenza sleale per il diretto responsabile dei messaggi e la compartecipazione colposa in capo al provider, assimilabile ad un responsabile editoriale che va equiparato quale organo di stampa a un sito Internet.

---

che, pur sancendo in linea generale l'irresponsabilità dei *provider*, ha lasciato comunque liberi gli stati membri di prevedere un meccanismo giurisdizionale che impedisca il perpetuarsi di una violazione quando il *provider* abbia un qualche tipo di controllo sulle informazioni che veicola.

[20] AA.VV., *Percorsi di diritto dell'informazione,* Giappichelli editore, 2006.

[21] Art. 2050 **"**Responsabilità per l'esercizio di attività pericolose". Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, e tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno.

[22] Art. 2051 **"**Danno cagionato da cosa in custodia". Ciascuno e responsabile del danno cagionato dalle cose che ha in custodia, salvo che provi il caso fortuito.

[23] Art. 2043 "Risarcimento per fatto illecito". Qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno.

[24] R. D'ARRIGO, *Recenti sviluppi in tema di responsabilità degli Internet Services Providers*, Giuffré, 2012, *passim*.

[25] G. CASSANO - F. BUFFA, *Responsabilità del content provider e dell'host provider*, al'url http://www.altalex.com/index.php?idnot=5686.

La scelta del giudice di Napoli è apparsa da subito difficilmente condivisibile, stante l'impossibilità pratica di controllare ogni messaggio inviato su un server[26], se è vero, come è vero che le comunicazioni su un sito Internet avvengono normalmente in modo automatico senza alcun intervento del provider.

Un'altra importante ordinanza è quella del Tribunale di Roma del 4 luglio 1998 con la quale una banca chiedeva la rimozione di affermazioni ritenute lesive pubblicate su un newsgroup gestito dalla società Pantheon e ospitato sul sito Internet di Agorà Telematica. Il giudice ritenne in tale occasione però che non esistessero gli estremi per agire nei confronti del provider e del responsabile (webmaster) del gruppo di discussione, dal momento che costoro si erano limitati a mettere a disposizione uno spazio senza esercitare alcun controllo sui contenuti. La decisione di Roma è dunque importante per aver negato che un gestore di un sito Internet abbia un diretto obbligo di controllo sul materiale inviato dai suoi utenti.

Napster è il nome del sito che all'inizio del nuovo millennio impegnò i giudici statunitensi in una complessa controversia avente ad oggetto l'applicazione delle norme americane sul copyright.

La vicenda, costituisce l'emblema di una delle possibili e più frequenti violazioni che possono essere commesse attraverso la rete dai suoi utilizzatori .

È opportuno precisare che per quanto riguarda fattispecie come quella in esame, il nostro ordinamento prevede forme di reazione, sia in sede penale, sia civile. Invero la possibilità di porre sotto sequestro determinate pagine web dà adito a non pochi dubbi in ragione dell'effetto reale perseguito da tale misura, vale a dire l'apprensione di una determinata *res*.

In caso di lesioni di diritti commesse attraverso un sito, e, affinché queste possano essere contestate nei confronti del gestore del servizio di internet provider è necessario provare l'elemento della colpa. Sicché si dovrà dimostrare che il gestore era a conoscenza dei comportamenti illeciti commessi attraverso i servizi offerti, e per giunta, occorrerà dimostrare che non si sia adoperato al fine di far cessare le attività illecite[27].

La Corte di Appello rileva che l'art. 13 Codice Privacy, in tema di obbligo di informare l'interessato, non prevede il dovere di informare quest'ultimo riguardo alla possibile violazione dei diritti dei terzi; del resto, l'art. 13 non è neppure richiamato dall'art. 167 in tema di trattamento illecito dei dati, ma solo dall'art. 161, norma per la cui violazione è prevista solamente una sanzione amministrativa.

---

[26] Non pare neppure corretto il ricorso per analogia alla figura del responsabile editoriale con il conseguente riconoscimento di un obbligo di controllo sul materiale pubblicato. Una responsabilità concorsuale del provider per fatti commessi da terzi potrebbe essere riconosciuta soltanto in presenza di un comportamento consapevole, che concretamente agevoli l'illecito del terzo.

[27] A. VISTOSI, *Applicabilità del ricorso ex art. 700 c.p.c. ad internet. Caratteristiche del web ed esigenze processuali a confronto: il leitmotiv dell'atipicità*, in E. BASSOLI (a cura di), "Come difendersi dalla violazione dei dati su Internet", Maggioli, 2012, 485.

Come invece affermato nel corso del giudizio dal Prof. Pizzetti, già Presidente del Garante della privacy in un parere *pro-veritate* emesso su richiesta della difesa in data 29.11.12, la responsabilità del trattamento dei dati è legata al mancato adempimento di specifici obblighi che sono rinvenibili esclusivamente in capo al titolare. Nel caso specifico, il titolare del trattamento dei dati del D. L. era G. L., vale a dire il soggetto che ha caricato il video sulla piattaforma *Google Video*.

Nell'evidenziare che il titolare del trattamento è solo l'*uploader*, la Corte sottolinea che la valutazione di un'immagine in grado di qualificare o meno un dato sensibile implica un giudizio semantico che non può essere certamente legato ad un procedimento informatico[28].

Se a ciò si unisce la circostanza che il d. lgs. sul commercio elettronico (Direttiva n. 70/2003) – da leggere unitamente alla disciplina sulla privacy – chiarisce che non vi è alcun obbligo di controllo preventivo[29], diventa evidente che la valutazione del contenuto trasmesso in rete compete al titolare e che tale qualifica non possa certamente imputarsi a *Google Italy*[30].

Inoltre, il concorso di persone espresso nel capo B) di imputazione tramite il richiamo all'art. 110 c.p., prevede necessariamente una partecipazione attiva nel reato di tutti i concorrenti, ma in realtà poi quella che viene contestata è una condotta sostanzialmente omissiva[31].

Da ultimo, sotto il profilo dell'elemento soggettivo del reato[32], la sentenza chiarisce che non è rinvenibile il dolo specifico richiesto dalla norma[33], in quanto manca qualsiasi riscontro di un vantaggio direttamente conseguito grazie alla condotta tenuta e nell'ambito del servizio gratuito quale era Google Video.

---

[28] Sulla utilizzabilità dei filtri da parte dei provider cfr. F. DI CIOMMO, *Programmi filtro e criteri di imputazione/esonero della responsabilità on line. A proposito della sentenza Google/Vivi Down*, Dir. Inf., Giuffré, 2010, 829.

[29] G. FACCI, *La responsabilità extracontrattuale dell'internet provider*, in Resp. Civ. e prev., 2002, 265, che ravvisa una sorta di responsabilità per attività pericolosa per i provider che consentano agli utenti di mantenere l'anonimato.

[30] Sull'obbligo di rimozione del materiali illeciti appena il provider ne abbia notizia, cfr. Trib. Grand Paris, 20 novembre 2000, con nota di P. COSTANZO, e ancora G. CASSANO, F. BUFFA, *Responsabilità del content provider e dell'host provider*, in Corr.giur., 2003, 77.

[31] S. RODOTÀ, *Libertà, opportunità, democrazia e informazione, in Internet e Privacy: quali regole?*, Atti del convegno di Roma 8-9 maggio 1998 dal tema "Cittadini e Società dell'Informazione, suppl. n. 1 al Bollettino n. 5 del Garante Privacy, 1998, 15.

[32] F. DI CIOMMO, *Diritti della personalità tra media tradizionali e avvento di internet*, in G. COMANDÉ (a cura di), "Persona e tutele giuridiche", Utet, 2003, 3.

[33] Sull'imputabiltà solo per colpa, con esclusione di qualunque colpa oggettiva in capo agli intermediari cfr. A. PIERUCCI, *La responsabilità del* provider *per i contenuti illeciti della Rete*, in Riv. Crit. Dir. Priv., 2003, 143.

La mancanza di un dolo specifico emerge poi dalla ragionevole certezza che gli imputati non fossero preventivamente a conoscenza del contenuto del filmato e dell'immissione del dato personale non lecitamente trattato[34].

Conclusioni

In definitiva, la Corte d'appello milanese pare aver, allo stato dell'arte tecnico e prescindendo da auspici legislativi *de jure condendo*, aver assunto l'unica possibile corretta soluzione in merito soprattutto al secondo capo di imputazione, che è poi l'elemento centrale della pronuncia giurisprudenziale.

Il ragionamento logico-giuridico si presenta immune da vizi per quanto concerne la mancata qualifica in capo a Google, di "titolare del trattamento", come descritto dall'art. 4 del d. lgs. 196/2003.

Una leggera perplessità potrebbe invece riguardare la scarna motivazione in ordine all'esclusione di responsabilità per la privacy policy del sito in merito all'informativa sulla tutela dei dati personali e al *disclaimer* sulle responsabilità in capo all'utente che carichi materiali in violazione di disposizioni legislative vigenti.

Una maggiore attenzione a tale aspetto, sottolineato invece nella sentenza meneghina di primo grado, sarebbe stata una buona occasione per fare luce su questo adempimento, così spesso trascurato. È vero infatti che l'accusa non mise in relazione l'art. 13 con il correlato articolo 161 cod. privacy, suo legittimo riferimento sanzionatorio, ma dagli atti risultava evidente ciò che l'accusa voleva affermare: il mancato rispetto dell'informativa, non nei confronti dei soggetti danneggiati, ovviamente, ma nei confronti degli uploader, veri titolari del trattamento.

Deve invece essere dato atto della coerente ricostruzione ordinamentale in merito agli intermediari dell'informazione in Internet, partendo dall'esclusione dell'analogia in *malam partem* in campo penale, si è così fatto riferimento alle norme civilistiche e al combinato disposto del d. lgs. 196/2003 e del d. lgs. 70/2003.

[34] Cfr. In senso conforme Cass. S.U. 27/03/2008 in Cass. Pen. 2008 n.12. e Cass. Sez. IV 18/09/2009 n.47997 Rv. 245742

La sempre verde tentazione di sostituirsi al legislatore

di Pasqualino Silvestre (∗)

1. Brevi considerazioni generali.

La sentenza n°1972/2010 della Sesta Sez. del Tribunale di Milano[1], ed il pronunciamento emesso in gravame della suddetta con il provvedimento che si annota[2], hanno costituito uno dei primi banchi di prova sui quali è stata testata la completezza di tutela dei vigenti strumenti normativi nei confronti dei reati che possono realizzarsi sul *web*, specie in tema di tutela della *privacy* e della corretta gestione dei dati personali. Evidenziando come possano essere potenziali autori di reati informatici non solo dei soggetti privati non identificabili ed ubicati in qualsiasi parte del mondo, (come di frequente si verifica per le frodi

---

(∗) In *Giurisprudenza di merito*.

[1] Per il dispositivo e le motivazioni della sentenza di primo grado si veda: Trib. Milano, sez. IV**,** 12 aprile 2010, n°1972, in *Foro it*., 2010, 5, II, p.279. Numerosi i contributi in argomento tra i quali, in particolare: A. MANNA, *La prima affermazione a livello giurisprudenziale della responsabilità penale dell'*internet provider*: spunti di riflessione fra diritto e tecnica* in *Giur.Cost.*, 2010, 2, p.1840; G. CASSANO, *Riflessioni a margine di un convegno sul caso* Google/Vividown in *Riv.pen.*, 2010, 10, p.1017; R. LOTIERZO, *Il caso Google – Vivi Down quale emblema del difficile rapporto degli internet providers con il codice della privacy* in *Cass.Pen*. 2010, 11, p.3986, ; F. DI CIOMMO, *Programmi filtro e criteri di imputazione/esonero della responsabilità online. A proposito della sentenza Google/Vividown*, in *Dir.Inf.*, 2010, p.829; C. ROSSELLO, *Riflessioni De Jure Condendo In materia di responsabilità del provider*, in *Dir.Inf.*, 2010, p.617; V. PEZZELLA, *Google Italia, diffamazione e riservatezza: il difficile compito del provider (e del giudice)* in *Giur.Mer.*, 2010, p.2232;. F. G. CATULLO. *Ai confini della responsabilità penale: che colpa attribuire a Google*? in *Giur.Mer.*, 2011, 1, p.159; G. CAMERA - O. POLLICINO, *La legge è uguale anche sul web. Dietro le quinte del caso Google-Vividown*, Milano, 2010.

[2] Tra i primi commenti in argomento si possono indicare i seguenti lavori tuttora in corso di pubblicazione: G. CASSANO, *Google–Vividown. Assoluzione in Appello e … "tanto rumore per nulla"*, in *Dir.Giust.*; A. MACRILLÒ, *Caso Google –Vivi Down: negato in appello il concorso omissivo nel delitto ex art. 167 d.lgs. 196/03*, in *Riv.Pen.*; F. G. CATULLO, *Atto secondo dell' affaire Google vivi down: società della registrazione e consenso sociale* in *Cass.Pen*.; F. RESTA, *Libertà della rete e protezione dei dati personali: ancora sul caso Vivi Down*, in *Ind.Pen.*; E. FALLETTI: *Internet, filtraggio, dignità: quale bilanciamento nella protezione della libertà di espressione*? In *Corr.Giur*.; D. TERRACINA, *Commento a Corte di appello di Milano – sentenza n. 8611 del 21.12.12*, in *Dir.pen.proc*.; M. DE GIORGI, *La tutela dei minori dal Cyberbullismo non passa attraverso la condanna di Google* in *Quest.Dir.Fam*.; E. BASSOLI, *Esclusa la responsabilità penale di Google per violazione di dati personali da parte di materiale multimediale immesso da terzi*, in *Arc.Pen*.; A. ROIATI, *L'insussitenza di un obbligo di controllo preventivo in capo ai vertici di GOOGLE ed il difficile bilanciamento tra i diritti contrapposti*, in *Riv.Pen*.

on-line) ma anche, come ipotizzato nel caso di specie, degli *internet providers* operanti in tutto il mondo quali ad esempio *GOOGLE*[3].

Il caso in oggetto, cosi, ha messo alla luce l'insufficienza della disciplina penale del settore dei *service providers*[4], evidenziando sia un ostacolo, tanto concettuale che linguistico, all'esatta percezione dei ruoli, dei compiti e delle responsabilità dei vari operatori ed intermediari del settore (si veda la distinzione tra *content provider, service provider, caching provider, hoster, uploader*[5]); sia una difficoltà ontologica nell'elaborazione di un eventuale criminalizzazione delle condotte: specie per quanto attiene al profilo della reale percezione del disvalore penale delle stesse, tanto da parte dei soggetti attivi che passivi.

Le analisi giuridiche e sociologiche condotte partendo dall'*incipit* tematico fornito dalle sentenze in commento, infatti, hanno fatto emergere in modo inequivocabile come il contesto dei *providers* sia stato sino ad ora caratterizzato dalla mancanza di una concreta domanda di pena da parte della collettività[6], collettività che, considerando diffusamente *internet* quale lo strumento che per eccellenza garantisce a tutti il pieno esercizio della più ampia libertà, e non solo di quella di manifestazione del pensiero, sembra vedere con sospetto gli interventi volti a circoscrivere l'esercizio delle facoltà esercitabili *on line*[7].

Ciò che ha determinato il successo della rete, infatti, è proprio la infinita possibilità di trovare ed immettere notizie, di dare e ricevere informazioni, comunicare e condividere sensazioni, conoscenze e pensieri, con una pluralità potenzialmente illimitata di persone, navigando nei contesti e nei luoghi più disparati, pur rimanendo al sicuro delle proprie mura domestiche. In conclusione, secondo il sentire comune, nel mondo virtuale tutti sono realmente liberi perché

---

[3] Per un approccio anche comparatistico al problema si veda: E. FALLETTI, *op.ult.cit*, §4°, ed ampia bibliografia ivi riportata.

[4] Per la dottrina in argomento si veda: F. RESTA, *La responsabilità penale del provider: tra laissez faire ed obblighi di controllo*, in *Giur.Mer*., 2004, p.1733; G. CORRIAS LUCENTE, *Ma i network providers, i service providers e gli access providers rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che gestiscono?*, in *Giur.Mer*., 2004, 2523 e ss.; A. INGRASSIA, *Il ruolo dell'internet service provider nel ciberspazio: cittadino, controllore o tutore dell'ordine? Risposte attuali e scenari futuribili di una responsabilità penale dei provider*, in *Penalecontemporaneo.it.;* L. PICOTTI, *Fondamento e limiti della responsabilità penale dei service-providers in Internet*, in *Dir.Pen.Proc*., 1999, p.384; ID, *I diritti fondamentale nell'uso e abuso dei social network. Aspetti penali*, in *Riv.Giur.Mer.*, 2012, p.12; A. MANNA, *I soggetti in posizione di garanzia*, in *Dir.Inf.*, 2010, p.779 e ss.

[5] Difficoltà spesso anche terminologiche non essendo alla maggior parte degli utilizzatori neanche intellegibili, quasi come se si parlasse di un linguaggio di esclusivo appannaggio di moderni scribi, le terminologie tecniche sottese alle diverse qualifiche e dai differenti ruoli.

[6] Così: F. CATULLO, *Atto secondo dell'affaire Google -Vivi Down*: Società della registrazione e consenso sociale, *op.cit*. p.5.

[7] In argomento confronta: D. TERRACINA, *op.cit*., p.2 del manoscritto, nonché F, CATULLO, *op.loc.ult.cit*.

ciascuno può essere ciò che vuole e dire liberamente ciò che pensa, senza la percezione di correre alcun rischio. Una malintesa accezione del concetto di libertà, troppo spesso associata ad una inconscia sensazione che il proprio agire nel mondo virtuale sia sostanzialmente deresponsabilizzato.

Il mondo virtuale, non solo rende difficile la percezione della potenzialità lesiva di proprie condotte in danno dei terzi, ma il desiderio di fruire delle illimitate risorse del *web*, nella maggioranza dei casi, non sembra associarsi ad una reale consapevolezza dei rischi e degli oneri che ciascuno volontariamente assume per accedere a tali potenzialità. E stato cosi correttamente rilevato[8] che la fiducia (quando non addirittura le fede) riposta nei *service provider* che hanno reso possibile la massificazione della comunicazione su *internet* agevolandone l'utilizzo, avviene da parte degli utenti quasi con incoscienza, poiché gli stessi, essendo sostanzialmente focalizzati sulla fruizione dei vantaggi offerti dal *world wide web* e dalle sue innumerevoli applicazioni, "*sono meno portati a riflettere sull'aver accettato un sistema di società in cui ogni utente esercita potere sull'altro e tutti sottostanno al potere di chi raccoglie registrazioni*". Dati suffragati dall'evidenza fornita dalla scienza medica di come le dipendenze da *Internet* e *social network* siano oramai incluse tra le psicopatologie recensite nel *Diagnostic and statistical manual of mental disorders* IDSM nella più recente edizione del 2013[9].

In riferimento alla fruizione di *internet*, per dirla con Michel Foucault, è dunque quanto mai vero che "*le persone sanno quello che fanno, ma non sanno cosa comporta ciò che stanno facendo*", non avvedendosi con adeguata contezza degli atti dispositivi della propria *privacy* che vengono automaticamente a verificarsi nel momento in cui l'utente del *web* aderisce ad un *social network*, finendo immancabilmente per essere "schedato" dallo stesso, anche a prescindere dai limiti di protezione prescelti[10]. Non a caso siti *web* come *YouTube*, che consentono la visualizzazione e la condivisione di video, i siti di *file sharing*, che abilitano i partecipanti a condividere e scambiare gratuitamente *files* di ogni tipo, i *social network* (come *Facebook* e *Linkedin*) ed i *microblogging* (quali ad esempio *Twitter*) sembrano continuare ad avere un costante incremento di iscrizioni.

La conclusione deducibile da siffatta premessa è che finché gli operatori che offrono servizi su *internet* saranno percepiti dall'opinione pubblica come garan-

---

[8] F. CATULLO, *op.loc.ult.cit*, ed ivi, per maggiori approfondimenti, rimando alle opere di J. BATTELLE, *Google e gli altri. Come hanno trasformato la nostra cultura e riscritto le regole del business*, Milano, 2006, p.25; J. R. SEARLE, *Creare il mondo sociale. La struttura della civiltà umana*, Milano, 2010, p.194, G. RIVA, *Psicologia dei nuovi media*, Bologna, 2008, p. 228.

[9] In argomento, tra tutti: S. GREENFIELD: *Living on line is changing our brains*; *new scientist, www, newscientist, com/article/mg21128236.400, retrieved*, 12 *June* 2012.

[10] A. MACRILLO', *Caso Google Vivi-Down, negato in appello il concorso omissivo ex art. 167 D. Lgs., 196/2003*, *op.cit*. p.1.

ti della libertà e dell'emancipazione dei singoli individui, secondo la malintesa accezione dei concetti dinanzi illustrata, ogni statuizione giudiziale che andrà a criminalizzare il loro operato non potrà mai essere sostenuta dal contesto sociale[11]. Non a caso, già a livello linguistico[12], i vocaboli *web* e *net* significano letteralmente "*ragnatela"* e "*rete"*: concetti che rimandano al vincolo cui soggiace chi si trova al loro interno restandone in un modo o in un altro avvinto, forse più di quanto non ineriscano alla correlazione di opportunità e risorse.

L'approccio, anche dogmatico, alla *ciber* criminalità, dunque, si rileva sempre ricco di problematiche estremamente eterogenee, poiché le peculiarità specifiche del mondo virtuale sono da sempre foriere di grandi difficoltà di adattamento, molto spesso prima mentale che tecnico, delle categorie logiche del diritto penale "tradizionale" alle caratteristiche del *web*[13].

Tali peculiarità e le eventuali carenze di tutela, tuttavia, non devono indurre gli interpreti del diritto a cedere alla tentazione di sostituirsi al legislatore sopperendone le inadeguatezze, tentazione sempre verde, specie quanto determinati eventi si connotano per una attenzione mediatica particolarmente rilevante[14].

2. Il fatto, le imputazioni ed i due gradi di giudizio.

La vicenda in esame ha avuto vita dalla pubblicazione in *internet* sul sito *http://video. Google.it* nella sezione "video divertenti" di un filmato della durata di circa 3 minuti in cui compariva "*un ragazzo presumibilmente down, in un ambiente scolastico, che veniva schernito e deriso da un gruppo di ragazzi*". Sulla vicenda sporgevano denuncia-querela tanto l'associazione Vivi Down, cui il disabile apparteneva, che il padre del ragazzo, portando all'attenzione della Procura, oltre che i comportamenti vessatori e di dileggio subiti dal giovane, anche profili di responsabilità penale a carico dei responsabili del sito, e del *provider*, trattandosi di un filmato che, "*non solo era circolato sul web tramite Google Video, ma non poteva essere passato inosservato, perché aveva conquistato la prima posizione nella categoria "video più divertenti" ed era addirittura finito all'interno della classifica ufficiale dei video più scaricati*".

---

[11] Cosi, ancora, F. CATULLO, *op.loc.ult.cit.*

[12] Oltre che nel noto *Tractatus logicus filosoficus*, interessanti riflessioni sul tema sono presenti anche in: L. WITTGENSTEIN, *Conversazioni annotate da Oets K. Bouwsma*, Milano, 2005, *passim*; e ID, *Causa ed effetto. Lezioni sulla libertà del volere*, a cura di A. Voltolini, Torino, 2006, *passim*.

[13] Particolarmente interessante sul tema: D. TERRACINA, *Neuroscienze e diritto penale: la crisi di effettività dei sistemi penali e la mancata percezione del disvalore delle condotte costituenti reato. Il caso particolare dei reati aventi ad oggetto beni intangibili*, Roma, 2011*;* il quale evidenzia come il cervello umano, per ragioni evoluzionistiche, sembri non percepire il reale disvalore di condotte quali lo scaricare da *internet* un *file* protetto da *copyright*.

[14] In argomento, di recente, M. DONINI, *Europeismo giudiziario e scienza penale. Dalla Dogmatica classica alla giurisprudenza–fonte*, Milano, 2011, p.77. e, prima ancora, C. E. PALIERO, *La maschera ed il volto. Percezione sociale del crimine ed effetti penali nei media*, in *Riv.it.dir.proc.pen.*, 2006, p.469 e ss.

Veniva cosi inoltrata istanza di punizione, ma anche nei confronti degli amministratori delegati di *Google Italy* s.r.l., del responsabile delle *policy* sulla *privacy* per l'Europa della *Google Inc*., e del Responsabile del progetto *Google Video* per l'Europa, cui venivano contestati, da un lato, il concorso omissivo nella fattispecie aggravata di diffamazione ex artt. 110, 40, comma 2, 595, commi 1 e 2, c.p., per aver reso possibile la diffusione del video a mezzo *internet*, omettendo qualsivoglia controllo preventivo sul suo contenuto; dall'altro la violazione degli artt. 110, e 167, commi 1 e 2, del D. Lvo. 30 Giugno 2003 n. 196, perché, al fine di trarne profitto per il tramite del servizio *Google Video*, procedevano al trattamento di dati personali in violazione agli artt. 17, 23 e 26 stesso D. Lvo., con relativo nocumento per la persona interessata[15].

Il giudice di prime cure, pur manifestando una particolare sensibilità per il rispetto degli oggetti di tutela giuridica lesi nella vicenda,[16] assolveva gli imputati dai reati contestati nel primo capo di imputazione: evidenziando l'insussistenza di un obbligo di legge codificato che imponesse un controllo preventivo dei dati trattati dai gestori dei siti *web* e che tale obbligo non si sarebbe neanche potuto ricavare da altre fonti, costituendo tale operazione una so-

---

[15] L'art. 17 del codice *privacy* prevede testualmente che «*Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritt*i». Secondo l'art. 23, invece, il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato che può riguardare l'intero trattamento ovvero una o più operazioni dello stesso. Il comma 3 prevede che «*Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'art. 13*». Infine, secondo l'art. 26, «*I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare*». I commi successivi di cui si compone l'art. 26 regolano i casi in cui non è prevista la prestazione del consenso. Non era dunque presente nel capo di imputazione, come correttamente evidenziato nella sentenza di appello, alcun richiamo all'art. 13 del medesimo decreto, pur invocato nella sentenza di primo grado. Errore evidenziato, tra gli altri da D. TERRACINA, *op.loc.cit*.; A, MACRILLO', *op.loc.cit*.; G.M. RICCIO, *op.loc.cit*., F. RESTA, *op.loc.cit*.

[16] Si veda in argomento: P. VENEZIANI, *I beni giuridici tutelati dalle norme penali in materia di disciplina dei dati personali*, in *La tutela penale della persona*, a cura di L. FIORAVANTI, Milano, 2001, p. 369 e ss; A. MANNA, *Codice della privacy: nuove garanzie per i cittadini nel Testo unico in materia di protezione dei dati personali*, in *Dir.pen.proc*., 2004, p. 22 e ss.;

stanziale violazione del il divieto di analogia in *malam partem* "*cardine interpretativo della nostra cultura procedimentale penale*"[17]. *Ad adiuvandum*, inoltre, si evidenziava come l'imposizione di un obbligo di controllo preventivo sull'incessante flusso di dati in transito su di un sito come Google, costituisse un comportamento inesigibile in ragione delle estreme difficoltà tecniche e delle conseguenze di sostanziale censura che ne sarebbe potuto derivare.

Al contrario, in relazione al reato di illecito trattamento di dati personali, riteneva accertato che il video in questione contenesse allusioni e indicazioni sullo stato di minorità del soggetto e dunque che fosse, di per sé, un dato personale e sensibile, come tale inquadrabile nella previsione dell'art. 167 D. Lgs. 196-2003, in base all'argomentazione che "*non può esistere in materia una zona franca che consenta a un qualsiasi soggetto di ritenersi esente dagli obblighi di legge nel momento in cui venga in possesso di dati sensibili*". Così operando si considerava ultronea la distinzione tra *host provider* e *content provider*, statuendo che il proprietario o il gestore di un sito *web* che compia anche una sola attività (tra quelle di raccolta, elaborazione, selezione, utilizzo, diffusione, organizzazione dei filmati tratta i dati che gli vengono consegnati), assuma per ciò solo un dovere di informare in modo puntuale e corretto gli utenti sugli oneri che la legge impone ai *providers* ai sensi dell'art. 13 D.Lgs. Disposizione, quest'ultima, utilizzata ai fini della condanna pur senza essere stata mai formalmente contestata[18].

Sulla base di tale *dictum* si escludeva che le modalità di trattamento dei dati effettuato dagli imputati potesse essere considerato sufficiente ai fini del rispetto dalla legge sulla *privacy*, in quanto la relativa informativa era stata fornita in modo generico ed astratto e comunque "*tale da non risultare minimamente utile se non quasi a costituire una sorta di alibi la stessa società*". Il giudizio di responsabilità in ordine al reato di illecito trattamento dei dati personali, quindi, veniva espresso, non sulla base dell'omissione di un obbligo preventivo di controllo sui dati immessi *on line*, ma sulla base dalla insufficiente comunicazione degli obblighi di legge all'*uploader*.

In tale ricostruzione lo specifico fine di profitto richiesto dalla norma era da ultimo rinvenuto nell'operatività del sistema di pubblicità basato su parole chiave *ADWords*, sistema considerato evidenza probatoria di una "*accettazione consapevole del rischio concreto di trattamento di dati sensibili*", con il conseguente configurarsi dell'elemento soggettivo del reato contestato come un *sui generis* dolo specifico-eventuale.

La Corte d'appello, in riferimento all'ipotesi di concorso nella fattispecie diffamatoria, contestata nel capo a) dell'imputazione, ha condiviso le valutazioni espresse in primo grado circa l'insussistenza, in capo ai vertici di *Google*, di una posizione di garanzia e di un obbligo di preventivo controllo sui contenuti

[17] Vedi, *infra*, §3.
[18] Vedi, *ante*, nota n°15.

video, suffragando la statuizione di primo grado[19]. Cosi all'assenza di uno specifico dovere giuridico di impedire l'evento, che comporta l'insussistenza del nesso causale, si è aggiunta *la mancanza di dolo* che nella fattispecie non attiene solo, come affermato dalla Corte, alla mancanza del cd. dolo di concorso, ma inerisce ancor prima alla mancanza di volontarietà in relazione al fatto tipico in sé considerato, poiché i vertici di *Google* non avevano alcuna consapevolezza del contenuto offensivo del filmato video.

Nel caso in esame, infatti, è stato correttamente rilevato[20] che, ove fosse stata riconosciuta l'esistenza di una posizione di garanzia in capo ai vertici di *Google* derivante dalla normativa sulla *privacy*, il rimprovero sarebbe al più potuto consistere nel non aver posto in essere *colposamente* il dovuto controllo. Fattispecie che, a sua volta, avrebbe comportato la necessità di una presa di posizione in chiave anche dogmatica sulla ammissibilità teorica di un concorso colposo nell'altrui reato doloso[21]. Fatta sempre salva l'eventualità che avesse prevalso la tentazione di aggirare l'ostacolo sopperendo all'eterogeneità degli elementi soggettivi di un siffatto concorso mediante l'usuale strumento del dolo eventua-

---

[19] Alle considerazioni già svolte dal giudice di primo grado la Corte di appello ha tuttavia aggiunto alcune precisazioni così riassumibili: 1) che per sostenere la responsabilità a titolo di omissione in capo ad un *host* o *content* provider, occorre affermare a suo carico un obbligo giuridico di impedire l'evento e quindi da un lato, l'esistenza di una posizione di garanzia, dall'altro la concreta possibilità di effettuare un controllo preventivo (p.22 sent.); 2) che la detta posizione di garanzia non può essere ravvisata nel diritto vigente, stante l'assenza di una specifica previsione in tal senso, né la posizione di garanzia di cui trattasi può desumersi da fonte diversa, quale in via esemplificativa quella dettata ex art. 57, e 57-*bis* c.p. in materia di stampa, in quanto si tratterebbe di analogia *in malam partem*; (p.23 sent.); 3) che la presenza di una posizione di garanzia da cui far derivare un obbligo di attivazione, in mancanza della quale far ricorrere la previsione dell'art. 40 c.p., non può essere fatta derivare dalla violazione di norme di legge quali quelle a protezione dei dati personali, non avendo le stesse per oggetto tali condotte ed essendo state emanate a copertura di comportamenti diversi da quelli oggetto di contestazione; 4) che in materia di concorso di persone la condotta consistente nel non impedire l'evento, che si ha l'obbligo giuridico di impedire, deve essere accompagnata dal dolo che caratterizza il concorso stesso, da ravvisarsi nella coscienza e volontà di concorrere con altri nella realizzazione del reato (p.24 sent.).

[20] A. ROIATI, *op.loc.ult.cit.*

[21] Sul tema: L. RISICATO, *Combinazione ed interferenza di forme di manifestazione del reato, contributo ad una teoria delle clausole generali di incriminazione suppletiva*, Cedam, Padova, 2001 Cap. 3°, p.375 e ss.; ID., *La partecipazione mediante omissione a reato commissivo, genesi e soluzione di un equivoco*, in *Riv.It.Dir.Proc.Pen.* 1995, fasc.4°, pag.1267 e ss. Su posizioni dottrinali analoghe seppur con differenti sfumature: LUCA BISORI, *L'omesso impedimento del reato altrui nella dottrina e nella giurisprudenza italiane*, in *Riv.It.Dir.Proc.Pen*., 1997, fasc. 4°, pag.1339 e ss; P. SEMERARO, *Il concorso mediante omissione nel reato*, in *Ind. Pen., Nuova Serie*, anno IX- n°2, Maggio-Agosto 2006, p.583 e ss; G. FIANDACA - E. MUSCO, *Diritto Penale Parte Generale*, Bologna, 2001, pag.550 ss.

le, per mascherare sotto il *nomen juris* di dolo delle vere e proprie forme di colpa o, peggio ancora, di responsabilità oggettiva da *versari in reillicita*[22].

Quanto al secondo capo di imputazione, afferente all'illecito trattamento dei dati, la Corte di appello di Milano ha censurato le motivazioni del giudizio di primo grado, attraverso cinque argomentazioni[23]:

1) Premesso che l'art. 167 D.lgs. n. 196/03 richiede esplicitamente che l'autore del reato abbia agito non rispettando le disposizioni indicate nel suo precetto e che tra queste disposizioni non è previsto l'art. 13 D.lgs. n. 196/03, la responsabilità degli imputati per il reato di *Trattamento illecito di dati* non può essere fatta derivare "*dalla carenza di una puntuale e doverosa informazione agli utenti delle norme poste a tutela della privacy*" *ex* art. 13 D.lgs. n. 196/03. Nessuna disposizione citata dall'art. 167 D.lgs. n. 196/03 impone all'Internet *service provider*, di informare l'utente circa l'esistenza ed i contenuti della legge sulla *privacy*.

2) Il soggetto responsabile del reato di cui all'art.167 D.lgs. n. 196/03 non può essere *Google*, ma l'*uploader* che, caricando il video, si assume la responsabilità del trattamento dei dati personali della persona che viene ripresa. Inoltre, la normativa sul commercio elettronico, che costituisce unitamente alla normativa sulla *privacy* un quadro giuridico coerente e completo, specifica che "*il prestatore non è responsabile delle informazioni memorizzate … a condizione che detto prestatore non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita … e che non agisca immediatamente per rimuovere le informazioni medesime*".

3) Poiché il reato di cui all'art. 167 D.lgs. n. 196/03 è un reato di mera condotta ed il concorso dei responsabili di *Google* nel reato posto in essere dall'*uploader* si è sostanziato in una omissione, non è possibile pervenire "*ad un giudizio di responsabilità per i primi, essendo la sfera dell'art. 40 comma 2 c.p. limitata ai reati di evento*".

4) Non sussiste l'elemento soggettivo del reato contestato, in quanto l'estensore della sentenza di primo grado ha confuso il dolo specifico previsto per il reato di cui all'art. 167 D.lgs. n. 196/03 con il fine di profitto costituito dalla palese vocazione economica di *Google*. Poiché l'attività commerciale della predetta azienda è lecita, questa "*non può essere assunta a prova della sussistenza del dolo*".

5). La struttura della fattispecie di cui all'art. 167 D.lgs. n. 196/03, postulando la necessaria partecipazione psichica intenzionale e diretta del soggetto al raggiungimento del profitto è incompatibile con la forma del dolo eventuale contestato ai prevenuti.

In conclusione è possibile evidenziare come l'insussistenza di un obbligo di controllo sui contenuti video abbia costituito *l'elemento dirimente per entrambi*

---

[22] Sia consentito fare rinvio sul tema a P. SILVESTRE, *Piccole note a margine di un grande tema. Considerazioni brevi sul dolo eventuale*, in *Giust.Pen.*, 2011, p.432 e ss. Vedi *infra* §3.

[23] Così efficacemente schematizzate da F. CATULLO, *op.loc.cit*.

i capi di imputazione finendo con l'assorbire tutte le ulteriori questioni affrontate[24], presumibilmente non solo per l'evidente fallacia di un pronunciamento che si fosse orientato in senso contrario, quanto anche per la maggiore problematicità che l'approfondimento della corretta operatività del dolo eventuale in tali fattispecie avrebbe ulteriormente comportato.

3. La sempre verde tentazione del giudice di rendersi legislatore, giurisprudenza creativa, concorso omissivo e dolo eventuale.

Il caso oggetto della nostra rapida analisi, documenta una delle ipotesi in cui il vaglio della Corte di appello ha consentito di ricondurre la fattispecie indicate nel capo di imputazione entro i confini naturali oltre cui ogni altra interpretazione si sarebbe rileva *contra legem.*

La stesso, tuttavia, può costituire un utile terreno di riscontro degli automatismi in cui rischia di incorrere chi esercita l'oneroso compito dello *ius dicere*, la dove debba far fronte ad una richiesta di pena per accadimenti che, pur non essendo sussumibili in alcuna fattispecie di reato positivamente prevista dal legislatore, sembrino tuttavia colpire la collettività suscitandone l'estemporanea indignazione, soprattutto su influenza dei media. L'*horror vacui* della lacuna normativa potrebbe generare quasi un senso di frustrazione dovuto all'impossibilità di rendere giustizia, come evincibile dalla già citata dichiarazione, quasi di sfogo, pronunciata la giudice del Tribunale di Milano la dove dichiarava: "*non può esistere in materia una zona franca che consenta a un qualsiasi soggetto di ritenersi esente dagli obblighi di legge nel momento in cui venga in possesso di dati sensibili*"

In tali casi, il giudice, il quale è pur sempre un uomo che, immancabilmente, percepisce le pressioni che il mondo esterno gli pone, rimanendone in qualche modo condizionato nel giudizio, può essere scosso dalla tentazione, umanamente comprensibile, di fare comunque giustizia tramite l'esercizio della facoltà di interpretazione delle norme che l'Ordinamento gli attribuisce: terreno quanto mai impervio, essendo spesso particolarmente labile il discrimine che consente di discernere un interpretazione estensiva da una sostanzialmente novativa.

In tale orizzonte non è difficile scorgere il pericolo che si finisca con il cadere in una "*giurisprudenza creativa*[25]" e da lì in una vera e propria *supplenza*

---

[24] In tal senso A. ROIATI, *op.loc.cit.*

[25] Sul punto: G. FIANDACA, *op.cit., passim*, secondo il quale, con la giurisprudenza creativa, si da sostanzialmente riconoscimento ad un interpretazione dinamica della fattispecie incriminatrice la quale, anche attraverso una preventiva ed astratta ricostruzione estensiva del bene giuridico, consente al giudice di operare una corrispondente dilatazione dei requisiti costruttivi del reato, cosi da elidere ogni insorgente preoccupazione politico criminale. In questa ottica il giudice sarebbe chiamato a costruire, più che rinvenire, le regole del diritto applicabili, assumendo il "*controllo penale*" ed accentuando il suo "*ruolo di istituzione di garanzia deputato a scongiurare il pericolo di una dittatura della maggioranze politiche, pur se democraticamente elette*". Ruolo di garanzia, ci si consenta di rilevarlo, che è tuttavia più presunto che accertato e che, in ogni

giudiziaria che, ancorandosi a forzature interpretative del dato normativo, approdi ad un *uso alternativo del diritto penale*[26].

In verità la discrezionalità valutativa dell'interprete nella sussunzione della fattispecie concreta nella normativa astratta e la possibilità di riconoscere valore ad alcuni fattori extratestuali o di contesto, deve servire esclusivamente per una migliore ricostruzione del dato del reale, senza che per questo il giudice possa vedersi riconosciuto un potere generativo nella selezione delle condotte rilevanti; compito che in un diritto penale del fatto, incentrato sulla garanzia posta dall'art. 25, comma 2°, della Costituzione, gli è precluso. La ricerca in funzione incriminatrice dei presupposti impliciti ad una norma extrapenale[27], quali il richiamo a disposizioni della legge privacy non munite di sanzione penalistica, infatti, costituirebbe un ampliamento degli elementi della fattispecie di reato che è compito esclusivo del legislatore realizzare. Si andrebbe a ledere altrimenti il principio di legalità e con esso il principio di divisione tra i poteri dello Stato[28] oltre, ovviamente, al principio di precisione delle norme penali che, come ha puntualizzato la Corte Costituzionale con la sentenza 364 del 1988, è "*presidio della libertà e della sicurezza*" del cittadino il quale solo "*in leggi precise e chiare, contenenti riconoscibili direttive di comportamento, può trovare in ogni momento cosa gli è lecito e cosa gli è vietato*". [29]

---

caso, non sembra presentare alcun contrappeso autenticamente idoneo a mettere a riparo da eventuali arbitri e derive autoritarie dei garanti stessi, tra l'altro non resi oggetto di alcuna investitura popolare. In tema anche: R. RAMPIONI, *op.cit*., p. 73; O. DI GIOVINE, *l'interpretazione del diritto penale, tra creatività e vincolo alla legge*, Milano, 2006, p.295.

[26] Quello di "*uso alternativo del diritto*" è un concetto, sviluppatosi soprattutto negli anni settanta, che postulava la necessità di mettere in atto il tentativo di interpretare il diritto esistente, di fonte legislativa o giurisprudenziale, a tutela degli interessi economici della classe sociale assunta come più debole, cioè il proletariato. Tentativo teorizzato e compiuto da larga parte della dottrina e della giurisprudenza italiane, la maggior parte delle quali di orientamento marxista. In una rinnovata prospettiva solidarista e progressista il diritto penale si sarebbe dovuto impiegare in chiave anti-egemonica, e dunque secondo uno schema alternativo a quello tradizionale concepito come strumento delle classi dirigenti borghesi per legittimare e mantenere il proprio *status quo* ed il proprio potere. Si veda in tema: B. LEONI, *Lezioni di filosofia del diritto*, raccolte da M. L. BAGNI, Catanzaro, 2003, pp.242-246.

[27] Cfr.: G. BETTIOL, *Scritti giuridici, le tre ultime lezioni brasiliane, Sul problema della fattispecie penale*, Padova, 1987, in *Collana di studi penalistici*, vol.1, 1987, p.11.

[28] G. MARINUCCI – E. DOLCINI, *op.ult.cit*., p.119, che rilevano come altrimenti lo "*Stato delle leggi*" rischierebbe di trasformarsi in uno "*Stato dei giudici*". Per una posizione diametralmente opposta: B. LEONI, *La libertà e la legge, op.loc.ult.cit.* p.169, in cui l'Autore pone al centro del diritto la figura del giudice e non il legislatore.

[29] C. COST. 24 marzo 1988, n°364, in *Giur.Cost*., 1988, p.1513. Per approfondimenti su tale fondamentale pronunciamento: si rinvia a D. PULITANO', *Una sentenza storica che restaura il principio di colpevolezza*, in *Riv.it.dir.proc.pen*., 1988, p.686 e ss; F. C. PALAZZO, *Ignorantia legis: vecchi limiti ed orizzonti nuovi della colpevolezza*, in *Riv.it.dir.proc.pen*., 1988, p.920; L. STORTONI, *L'introduzione nel sistema penale*

La condotta che costituisce reato, dunque, deve essere espressamente contenuta ed chiaramente esplicitata nella norma di legge violata dal soggetto agente; puntualmente indicata al soggetto che ne riceve l'imputazione, e non speculativamente ricavata con un processo interpretativo del giudicante. Processo che, pur essendo pienamente legittimo in altri rami del diritto e, *a fortiori*, nella teoria generale della norma[30], non può esserlo in materia penale in quanto palesemente in contrasto con il divieto di analogia in *malam partem* e con il principio di tassatività e determinatezza[31] come pure riconosciuto, in parte, dal giudice di primo grado[32].

Tanto premesso appare evidente come, nel pronunciamento oggetto dell'appello, si sia fatto ricorso ad entrambi i meccanismi usualmente utilizzati nella "creazione giurisprudenziale" del diritto: 1) quello della combinazione cumulativa dell'art. 40 cpv., e dell'art. 110 del c.p., ad una norma incriminatrice di parte speciale (contestato formalmente nel primo capo di imputazione ed, implicitamente, anche nel secondo) e 2) quello del ricorso al dolo eventuale per ricondurre nell'alveo del doloso l'elemento soggettivo di una condotta di per se intrinsecamente colposa: come sarebbe avvenuto in riferimento al reato di cui all'art. 595, comma 1 e 3, c.p., ove fosse stato ritenuto sussistente il nesso di causalità materiale, e come il giudice di primo grado ha effettivamente fatto nel pronunciare la condanna per il reato di cui all'art.167, comma 1 e 2, D. Lgs. 196/03.

Riguardo alla prima metodologia deve essere rilevato che la possibilità di applicazione congiunta dei due moltiplicatori di incriminazione più pervasivi del codice penale con una disposizione di parte speciale è contestata dalla dottrina che, a ragione, la ritiene contrastante con il principio di legalità[33]: specie la

---

dell'errore scusabile di diritto: significati e prospettive, in *Riv.it.dir.proc.pen.*, 1988, p.1313; M. GUARDATA, *L'ignoranza della legge penale dopo l'intervento della Corte Costituzionale: prime impressioni*, in *Cass.Pen.*, 1988, p.1152; G. FLORA, *La difficile interpretazione del principio di colpevolezza, riflessioni per l'anniversario della sentenza della Corte Costituzionale sull'art. 5 c.p.*, in *Giur.It.*,1989, VI, p.337; F. MANTOVANI, *ignorantia legis, scusabile ed inescusabile*, in *Riv.it.dir.proc.pen.*, 1990, p.379; F. MUCCIARELLI, *Errore e dubbio, dopo la sentenza della Corte Costituzionale 364/1988* in *Riv.it.dir.proc.pen.*, 1996, p.223.

[30] Nella quale, come noto, è riconosciuta validità di fonte anche al ricorso ai principi generali dell'Ordinamento oltre che alla consuetudine e alla desuetudine. Vedi G. GAVAZZI, *Elementi di teoria del diritto*, II^ed., Torino, 1987, p.47 e s.,

[31] Sul punto: G. BETTIOL, *op.loc.ult.cit.*

[32] Vedi, *supra*, §1, p.4.

[33] Cfr.: L. RISICATO, *op.loc.cit.*, p. 399 e ss.; ID: *La partecipazione mediante omissione a reato commissivo. Genesi e soluzione di un equivoco*, in *Riv.it.dir.proc.pen.*, 1995, p. 1275 e ss; G. FIANDACA – E. MUSCO, *Diritto penale*, Bologna, 2009, p. 578 ss. In argomento confronta anche: I. LEONCINI, *Obbligo di attivarsi, obbligo di garanzia e obbligo di sorveglianza*, Torino, 1999; F. MANTOVANI, *L'obbligo di garanzia ricostruito alla luce dei principi di legalità, di solidarietà, di libertà e di responsabilità personale*, in *Riv.it.dir.proc.pen.*, 2001, p. 343 e ss.;

dove il contributo causale omissivo dovesse rilevarsi animato da un elemento soggettivo eterogeneo rispetto a quello della componete commissiva[34]. Nello specifico l'operatività del concorso omissivo andrebbe circoscritta alle *fattispecie ad evento naturalistico*, là dove l'art. 40 cpv. c.p. svolgerebbe una funzione incriminatrice demandando alle disposizioni sul concorso una mera funzione disciplinare il meccanismo sanzionatorio. Non a caso, dunque, quando la giurisprudenza ha necessità di "forzare" tale evidenza, ricorre all'espediente di considerare quale evento che impegna la responsabilità dell'omittente ex art. 40 cpv, c.p., non il reato commesso con condotta attiva dal concorrente, ma il fatto in se che questi abbia commesso un reato che l'esercizio dei poteri correlati alla titolarietà della posizione di garanzia avrebbe potuto evitare. Il che produce la conseguenza che, nella compartecipazione mediante omissione al fatto illecito altrui, il garante venga sostanzialmente punito per la facilitazione negativa del fatto illecito del terzo, secondo uno schema assimilabile a quello dell'agevolazione colposa, e spesso senza che sia accertato il suo reale ruolo di coautore (anche nella logica dell'elemento soggettivo) come dovrebbe essere sempre richiesto di fronte a reati di evento naturalistico.

Quanto al *dolus eventualis*, è oramai noto come lo stesso sia stato definitivamente riconosciuto da parte della recente giurisprudenza delle Sezioni Unite[35] come "*una figura di costruzione giurisprudenziale e dottrinale*", che "*non forma oggetto di una testuale previsione legislativa*", la cui costruzione, proprio perché non disciplinata dal legislatore: "*è rimessa all'interprete ed è ben possibile che per particolari reati assuma caratteristiche specifiche*"[36].

Un riconoscimento di inesistenza[37] cui non ha fatto seguito l'espunzione del *dolus eventualis* dall'ordinamento per radicale idiosincrasia con il fondamentale principio di legalità, quanto il riconoscimento "*al passo con i tempi*"[38] della sua discrezionale costruibilità in concreto secondo le contingenti necessità del caso.

A margine di tale statuizione non resta che considerare come sia quantomeno singolare che, con lo svilupparsi dell'interpretazione teleologicamente[39] indiriz-

---

[34] Si veda G. GRASSO, *Il reato omissivo improprio*, Milano, 1983, *passim*.

[35] Si fa riferimento alla sentenza SS. UU., n°12433 del 26 novembre 2009 (dep. 30 marzo 2010), edita in *Cass.Pen.*, n°7/8 2010, pp. 2548 e ss., con nota di M. DONINI: *Dolo eventuale e formula di Frank nella ricettazione. Le Sezioni unite riscoprono l'elemento psicologico*, pp. 2555 e ss.

[36] Ed ancora che: "*non c'è ragione di ritenere che* (il dolo eventuale) *possa riferirsi al solo evento del reato e che l'atteggiamento nel quale si fa consistere non possa riguardare anche i presupposti*".

[37] P. SILVESTRE, *op.loc.ult.cit.*

[38] Per la distinzione tra "*diritto penale classico*" e "*diritto penale moderno*", si veda M. DONINI: *Il volto attuale dell'illecito penale. La democrazia penale tra differenziazione e sussidiarietà*, Milano, 2004, p.97 e ss.

[39] Su tale indirizzo: G. BETTIOL, in *Scritti giuridici*, Padova, 1966,1980,1984, nonché ID.: *Sistemi e valori nel diritto penale*, Padova, vol.I°, p.491, ID., *Diritto penale*, rivisto ed integrato da M. PETTOELLO MANTOVANI, Padova, 1983, p.83; A. PAGLIARO, *Teleologismo e finalismo nel pensiero di G. Bettiol*, in *Riv.it.dir.proc.pen.*,

zata del codice penale in conformità ai principi della Carta Costituzionale, e la conseguente necessità di affermare con pienezza la costituzionalità del principio di colpevolezza e della personalità della responsabilità penale, la dottrina e la giurisprudenza abbiano pensato di poter superare gli *empasse* sistematici della divergenza tra il voluto ed il realizzato ricorrendo al dolo eventuale per legittimare, sotto il profilo soggettivo, molte di quelle fattispecie in cui prima trovavano applicazione differenti forme di responsabilità oggettiva, più o meno manifesta. Quasi come se si fosse perfezionato uno scambio di etichette in cui si finisce con lo spostare la responsabilità oggettiva dalla causalità alla colpevolezza: estendendo il contenuto del dolo ad ambiti applicativi più propriamente appartenenti alla colpa[40].

Cosi, senza bandire formalmente la responsabilità oggettiva da nesso causale dal diritto positivo o ammetterne la necessaria conservazione, si ipertrofizza l'applicazione del dolo eventuale sino a renderlo una sorta di responsabilità oggettiva operante sull'elemento soggettivo[41]. Mentre nella prima, pero, si riconosceva espressamente che il soggetto era punito per essere stato una causa o concausa materiale dell'evento tipico a prescindere dal suo elemento psicologico, con un giudizio di responsabilità basato su di un substrato comunque materialmente verificabile e proprio per questo "oggettivo"; nella "*responsabilità oggettiva soggettivizzata*" tale elemento psicologico, già difficilmente accertabile sul piano empirico, è creato di volta in volta dall'interprete, generando una forma di colpevolezza polimorfa soggetta ad adeguarsi al caso concreto in funzione della pena che un generico concetto di adeguatezza sociale sembra rendere necessario irrogare.

Nel caso giurisprudenziale in analisi, da ultimo, la necessità politico criminale di non lasciare esenti da pena i presunti autori di un reato perpetrato ai danni di un disabile, sembra avere indotto il giudice di prime cure a concludere che gli imputati avessero agito con un dolo specifico-eventuale. Due forme di dolo ontologicamente incompatibili[42] essendo, la prima, caratterizzata dalla propensione finalistica verso un fine voluto, correlato al verificarsi dell'evento giuridico tipico, e la seconda, dall'accettazione del rischio (discrezionalmente quantificabile quanto a frequenza statistica di possibile o probabile verificazione, in coe-

---

fasc.I., 2008, pp.31-39; G. DE FRANCESCO, *teleologismo e dommatica nella ricostruzione delle figure di divergenza dell'esecuzione del reato*, Torino, 1998.

[40] Per tutti si vedano: G. FORTE, *Ai confini fra dolo e colpa: dolo eventuale o colpa cosciente*? In *Riv.it.dir.proc.pen.*, 1999, *passim*. ID., *Dolo eventuale e colpa cosciente, tra divieto d'interpretazione analogica ed incostituzionalità*, in *Riv.it.dir.proc.pen.*, 2000, vol.II°; L. EUSEBI, *appunti sul confine tra dolo e colpa nella teoria del reato*, in *Riv.it.dir.proc.pen.*, 2000, p.1089 e ss.

[41] Ciò sia per la maggior efficacia politico criminale dell'istituto, sia per la maggior tassatività della definizione codicistica della colpa che offre minor spazio alle forzature interpretative cui con maggiore facilità sembra prestarsi il dolo.

[42] *Ex pluribus*: L. PICOTTI, *Il dolo specifico. Un'indagine sugli 'elementi finalistici' delle fattispecie penali*, Milano, 1993, p.596-611.

renza a quanto previsto dalle SS.UU.) di un evento non voluto e non finalisticamente perseguito, che si verifichi in esito ad una propria attività lecita, altrimenti si avrebbe un dolo diretto.

L'incompatibilità dei due elementi soggettivi, inoltre, riguarda anche i fini dei singoli istituti sul piano politico criminale, essendo il dolo specifico, nell'uso fattone nel diritto moderno post-autoritario, volto a restringere il possibile alveo della punibilità dell'agente, con conseguente aggravio nell'onere probatorio dell'accusa; ed il dolo eventuale al fine diametralmente opposto di estensione del dolo all'area applicativa della colpa, normativizzandone il concetto al fine di semplificarne l'accertamento probatorio[43]. Sul piano puramente dogmatico[44] (o in contesti normativi quali quello del diritto tedesco dove non vi è una definizione positiva del dolo, quale quella contenuta nell'art.43 del c.p., italiano) le due forme del normale titolo di imputazione soggettiva potrebbero teoricamente coesistere quando l'eventualità del dolo si riferisse ad elementi del reato diversi dal fine[45]. Trasponendo tale riflessione nel concreto, tuttavia, si avrebbe un unico fatto di reato animato da due doli eterogenei quanto all'oggetto e al fine perseguito, con l'evidente antinomia di un oggetto del dolo che sarebbe in alcuni dei suoi elementi, voluto, ed, in altri, accettato come rischio.

In conclusione, la necessità del giudice di dover far ricorso agli strumenti normativi indicati, dovrebbe costituire per lo stesso un campanello d'allarme che rammenta l'incombere del rischio di un interpretazione iper-estensiva, analogica o creatrice, tentazione sempre da evitare, anche ove si fosse animati dai più encomiabili e condivisibili fini di rendere giustizia sopperendo alla sciatteria di un legislatore pigro o distratto.

La via dell'inferno, d'altronde, è sempre lastricata di buone intenzioni[46].

---

[43] In argomento, diffusamente, G. P. DEMURO, *Il dolo*, vol.II°, *l'accertamento*, Milano, 2010, *passim*; e più di recente ID, *Sulla flessibilità concettuale del dolo even*tuale, in *Dir.pen.cont. – Riv.trim*., 1, 2012, p.142.

[44] Vedi anche: P. SILVESTRE, *op.loc.cit.*, p.445.

[45] Cosi: F. MANTOVANI, *Diritto Penale. Parte generale*, VII ed., Padova, 2011, pp.326-327.

[46] K. MARX, *Il Capitale*, lib.I, sez.II. cap.5, §2.

Internet, filtraggio, dignità: quale bilanciamento nella protezione della libertà di espressione?

di Elena Falletti (∗)

1. Introduzione.

La vicenda è internazionalmente nota e concerne la condanna penale somministrata in primo grado a carico di tre alti dirigenti di Google Italy e Google Europe per la pubblicazione online di un video di scherno di un giovane disabile filmato durante l'orario scolastico in una scuola torinese, durante il quale altresì veniva esplicitamente irrisa una nota associazione a tutela delle persone portatrici di handicap[1]. Le riflessioni effettuate tanto dal giudice di primo grado quanto da quelli d'appello dimostrano il disagio della giurisprudenza nei confronti della Rete, sulla sua presunta "mutata natura" e, soprattutto, dei fornitori di servizi nonché del ruolo che le loro piattaforme avrebbero assunto nei tempi più recenti, ovvero quella di host attivi. I provider, infatti, non si limiterebbero più a offrire uno spazio virtuale per lo scambio di informazioni, ma interverrebbero attivamente attraverso la predisposizione di inserzioni pubblicitarie ovvero possibilità di votare e classificare i contenuti. È sufficiente ciò a far assumere al gestore della piattaforma un ruolo paragonabile a quello editoriale tradizionale? Successivamente all'analisi coordinata delle due pronunce ambrosiane, si propongono alcune osservazioni sul tema alla luce della giurisprudenza comparata, spesso contraddittoria sul punto.

(∗) In *Corriere Giuridico*.

1 Trib. Milano, 12 aprile 2010. Moltissimi furono i commenti della dottrina, tra questi si ricordano: G. Camera, O. Pollicino, La legge è uguale anche sul web. Dietro le quinte del caso Google-Vividown, Milano, 2010; F. Di Ciommo, Programmi filtro e criteri di imputazione/esonero della responsabilità online. A proposito della sentenza Google/Vividown, in Dir. Inf. Informatica, 2010, 829; C. Rossello, Riflessioni De Jure Contendo In Materia Di Responsabilità Del Provider, ibidem, 617; V. Pezzella, *Google Italia, diffamazione e riservatezza: il difficile compito del provider (e del giudice)* in *Giur. Mer.*, 2010, 2232; R. Lotierzo, Il caso 'Google-Vivi Down' quale emblema del difficile rapporto degli 'internet providers' con il codice della privacy, Cass. Pen., 2010, 3994; G. Cassano, Google v. Vividown. responsabilità "assolute" e fine di internet?, in Vita Notarile, 2/2010, 2. Mentre nella dottrina internazionale si segnalano: G. Sartor, M. G. de Azevedo Cunha, The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents, 2010, http://ssrn.com/abstract=1604411; L. Shaw, Hate Speech in Cyberspace: Bitterness without Boundaries, 25 ND J. L. Ethics & Pub Pol'y 279, (2011), 292; R. Mendez, Google in Italy, International Data Privacy Law, 2011, 137; N. C. N. Hampson, The Internet Is Not a Lawless Prairie: Data Protection And Privacy In Italy, 34 B.C. Int'l & Comp. L. Rev. 477, (2012), 477; B. van der Sloot, F. Zuiderveen, Borgesius, Google and Personal Data Protection, in A. López-Tarruella (ed.), Google and the Law: Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models, The Hague, 2012, 89.

2. La sentenza del Tribunale di Milano

Ai fini di presentare una visione d'insieme della questione, sommariamente si rammentano le motivazioni della sentenza di primo grado del giudice unico del Tribunale di Milano. Esse si possono suddividere in tre filoni principali: a) l'applicabilità della legge italiana alla fattispecie e la competenza del giudice ambrosiano; b) la violazione della disciplina in materia di privacy; c) l'assoluzione dall'imputazione del reato di diffamazione.

Per quanto concerne il primo punto, il giudice di prime cure afferma che il trattamento dei dati costituisce un *working in progress* il quale esaurisce il suo completamento in tempi e luoghi diversi, tanto all'estero (dove i materiali vengono caricati sui server dell'ISP), tanto in Italia, dove è avvenuto parte del trattamento dei dati, nonché dove si sono manifestati gli effetti pregiudizievoli dell'illecito[2].

La parte più discussa della sentenza di primo grado concerne la condanna dei tre rappresentanti di Google a sei mesi di reclusione (con le attenuanti generiche e la diminuente del rito) per la violazione della legge italiana sulla privacy riguardante il trattamento illecito di dati personali. Il giudicante argomenta che i dati trattati da Google, poiché emergenti dalla visione del video, sono dati sensibili essendo in grado di informare il pubblico sullo stato di salute dell'involontario protagonista del filmato. Inoltre, il giudice si sofferma sull'incapacità della persona raffigurata a dare validamente il proprio consenso al trattamento dei dati inerenti le informazioni più intime della sua sfera personale. Lo studente avrebbe dunque subito una doppia lesione: nella propria dignità e nella propria riservatezza[3]. Alla base degli elementi emersi, il giudicante ha ritenuto integrata da un punto di vista oggettivo la fattispecie prevista dall'art. 167 del Codice della privacy per la sussistenza di un trattamento illecito dei dati personali. Per l'integrazione degli elementi ulteriori della fattispecie penale, il giudice ha questionato se tale illiceità del trattamento fosse imputabile ai dirigenti di Google e se tale trattamento fosse operato al fine di conseguirne un profitto. A questo proposito si osserva come per raggiungere una risposta affermativa, il giudice abbia forzato il suo ragionamento, giustificandosi con il "buon senso" e affermando che "*Non può esserci dubbio (…) che non esiste in materia una zona franca (da un punto di vista oggettivo) che consenta a un qualsiasi soggetto (persona fisica o meno che sia) di ritenersi esente dall'obbligo di legge, nel momento in cui venga, in qualsiasi modo, in possesso di dati sensibili*"[4]. Come evidenziato da gran parte della dottrina, questo ragionamento presenta preliminarmente evidenti lacune per quanto concerne il principio di stretta legalità penale a causa del divieto di analogia in malam partem. Ulteriormente, il giudicante, al fine di rendere concreta la sua lotta alle "zone franche" di Internet, di fatto ha imposto ciò che non è previsto dalle norme regolatrici, ovvero il

2 G. Camera, O. Pollicino, La legge è uguale anche sul web, cit., p. 124.

3 G. Camera, O. Pollicino, cit., p. 129.

4 Trib. Milano, 12 aprile 2010, cit.

controllo preventivo dei materiali uploadati attraverso l'utilizzo di sistemi di filtraggio. Per rendere più plausibile il suo ragionamento, il giudice ha rilevato che gli ISP hanno ormai perduto la loro caratteristica neutralità per trasformarsi in "hoster attivi" nella gestione dei materiali pubblicati online, soprattutto per quel che riguarda le strategie di marketing utili a ottenere profitti e pubblicità attraverso i materiali pubblicati. Tuttavia l'obbligo di filtraggio, per quanto oggetto di ampio dibattito, anche a livello internazionale, è inesigibile. Inoltre il giudicante parrebbe confondere l'obbligo di informativa da parte del titolare del servizio (Google) sul trattamento dei dati dell''interessato (chi effettua l'upload del video) con l'obblighi, non previsti, di quest'ultimo nei confronti dei dati personali di terzi (cioè dei soggetti ripresi nel servizio)[5].

Per quanto concerne il terzo aspetto, in primo grado il giudice unico del Tribunale di Milano aveva assolto i tre manager di Google dall'accusa di concorso omissivo degli imputati nel reato di diffamazione commessa ai danni del ragazzo oggetto dello scherno mostrato dal video e dell'Associazione Vivi Down[6]. La linea accusatoria affermava che il video conteneva immagini raffiguranti atti e parole lesive e umilianti la dignità del ragazzo, nonché di dileggio e offesa della reputazione della succitata Associazione. Secondo le accuse, Google Video avrebbe trascurato ogni cautela per impedire la permanenza del video online per ben due mesi. Tali cautele sarebbero state obbligatorie proprio in virtù della normativa privacy, a parere dell'accusa; mentre la difesa sosteneva affermava che la pretesa di tal obbligo avrebbe significato prevedere in capo all'ISP (Internet service provider) un inaccettabile obbligo giuridico di controllo preventivo. Sul punto, il giudice rigetta le argomentazioni accusatorie, non rintracciando nei confronti degli imputati alcuna responsabilità in punto diffamazione[7]. Le argomentazioni del rigetto si possono riassumere come segue: da un lato non è stata provata l'attivazione di un obbligo di garanzia ex art. 40 c.p., poiché non è possibile ricostruire ai sensi dello stretto diritto penale positivo una correlazione tra la violazione degli obblighi di privacy e la diffamazione; dall'altro lato l'impostazione accusatoria non è ammissibile né ai sensi del diritto penale, né a rigor di logica poiché anche se fossero stati correttamente utilizzati i meccanismi di tutela previsti dalla legge sulla privacy, questi non sarebbero stati sufficienti a impedire l'evento sanzionato[8].

La condanna in primo grado dei tre manager aveva scosso l'opinione pubblica internazionale specializzata nei temi relativi alla governance di Internet perchè, attraverso la comminazione di sanzioni penali, si vedeva minacciare da un lato la neutralità della Rete e delle piattaforme che la compongono, dall'altro

---

5 A. Longo, «Regole globali per disciplinare privacy e internet» (Intervista a F. Pizzetti), Sole24Ore, 16 aprile 2010, consultata su tp://www.ius-web.it/PUB/allegati_prodotti/608/Intervista_a_Francesco_Pizzetti.pdf.

6 G. Camera, O. Pollicino, La legge è uguale anche sul web, cit., p. 150.

7 G. Camera, O. Pollicino, op. cit., 152.

8 G. Camera, O. Pollicino, ult. op. loc. cit.; G. Sartor, M. V. de Azevedo Cunha, The Italian Google-Case, cit., p. 4.

una grave limitazione della libertà di Internet, se non addirittura alla censura e all'autocensura. Con la decisione in commento la Corte d'Appello di Milano ha condivisibilmente riformato la sentenza di prime cure cancellando la condanna penale dei tre responsabili d'area di Google.

3. La decisione della Corte d'Appello di Milano

Innanzitutto i giudici d'appello hanno confermato la sussistenza della giurisdizione italiana e la competenza del Foro milanese per quel che concerne il radicamento della causa poiché da un lato Google possiede una propria sede italiana, mentre dall'altro gli effetti pregiudizievoli del reato si sono manifestati in Italia.

Secondariamente, per quanto concerne il capo di imputazione relativo alla violazione degli artt. 110, 40, 595, 1 e 3 co., c.p. i giudici d'appello ambrosiani osservano che ai sensi del diritto vigente non esiste un obbligo di impedire eventi offensivi a carico d'altri, né Google rivestiva alcuna posizione di garanzia poiché nel periodo dell'avvenuto contestato reato (ovvero il tempo in cui il video è rimasto visibile su Google Video dall'8 settembre 2006 al 7 novembre 2006) non era previsto un obbligo giuridico di impedire l'evento, né l'utilizzazione di c.d. programmi di filtraggio e di controllo sui contenuti generati dagli utenti e immessi in Rete; come del resto non sussiste ora. Ulteriormente, a carico degli imputati mancava l'elemento soggettivo necessario ai fini dell'integrazione del reato, ovvero il dolo.

I giudici d'appello milanesi altresì affermano che la categoria dell'hoster attivo", utilizzata dal giudicante di prime cure nelle sue argomentazioni motivazionali, non è prevista da alcuna norma di legge italiana ovvero comunitaria. Tuttavia, viene rilevato in sentenza che le attività poste in essere da Google e da altre analoghe piattaforme hanno assunto una natura differente rispetto a quella prevista dal legislatore comunitario nelle direttive in materia. Per quanto ora siano tecnicamente possibili le attività di filtraggio, rimozione, selezione, raccolta, indicizzazione del materiale, anche ai fini di raccolta pubblicitaria, va osservato che l'eventuale assunzione di tali incombenti non può essere imposta ai fini di obbedienza al mero "buon senso", poiché seppure il prestatore di servizi sia in grado di effettuare un servizio di "hosting attivo", va esclusa la possibilità di procedere ad una verifica preventiva efficace di tutto il materiale uploadato dagli utenti.

A carico del prestatore di servizi permane, invece, l'obbligo di informare l'interessato ai sensi dell'art. 13 del Codice della Privacy, mentre tale obbligo non si estende al dovere di informazione sulla violazione dei diritti di terzi, neppure previsto dall'art. 167 del medesimo codice, mentre l'art. 161 prevede in caso di trattamento illecito dei dati una sanzione amministrativa. In motivazione i giudici d'appello chiariscono altresì che il titolare del trattamento dei dati sensibili relativi alla salute del ragazzo ripreso nel video non è Google, ma il soggetto che ha caricato sulla piattaforma il video. Sul punto il giudice specifica che la valutazione della presenza di dati sensibili nel video non può essere fatta

attraverso un procedimento informatico, ma solo attraverso un giudizio semantico. A questo proposito, la lettura combinata delle disposizioni del Codice della Privacy insieme a quelle del D. Lgs. 70/2003[9] chiarisce da un lato che non esiste alcun obbligo di controllo preventivo da parte del fornitore di servizi; mentre dall'altro ribadisce che la valutazione dell'illeceità del contenuto diffuso attraverso la Rete è di competenza del titolare dei dati, cioè di chi effettua l'upload del video sulla piattaforma, non di Google. Infine, viene esclusa qualificazione della fattispecie a titolo di dolo, specifico ovvero eventuale, in quanto gli imputati non sono in grado di conoscere preventivamente la possibile illiceità del trattamento dei dati personali contenuti nei materiali caricati.

4. Il dibattito sul filtraggio della Rete nella giurisprudenza comparata.

Uno dei passaggi più interessanti della motivazione della sentenza d'appello concerne l'osservazione che la Rete avrebbe mutato la sua natura superando "nei fatti la figura di mero prestatore di servizio, che veniva elaborata all'epoca della citata Direttiva[10] e che delineava tale soggetto come del tutto estraneo rispetto alle informazioni memorizzate, sia a livello di gestione che di regolamentazione contrattuale con i destinatari del servizio". Il giudice d'appello riprende il concetto di "hosting attivo", già utilizzato da quello di prime cure, per analizzare in cosa consista siffatto mutamento. L'host attivo sarebbe configurato in un prestatore di servizi non neutro rispetto all'organizzazione e alla gestione dei contenuti degli utenti, caratterizzata anche dalla possibilità di un finanziamento economico attraverso l'inserimento di inserzioni pubblicitarie"[11]. Questa categoria emerge esclusivamente da constatazioni fattuali, legata all'elaborazione giurisprudenziale, anche comparata, mentre non è ancora inserita in alcuna fonte di diritto positivo. Pertanto parrebbe quantomeno di interesse verificare lo svilupparsi della giurisprudenza comparata sul punto.

Negli Stati Uniti il tema è strettamente connesso con il dibattito inerente la libertà di manifestazione del pensiero per quel che concerne la censura del c.d. hate speech, cioè l'incitamento all'odio razziale, etnico, sessuale ovvero nei confronti di certe minoranze[12]. In un caso analogo a quello in commento, svoltosi nell'ambito scolastico e inerente la diffusione di minacce ad un ragazzo

9 Si tratta del decreto legislativo n. 70 del 9 aprile 2003, emanato sulla base della delega contenuta nella legge comunitaria 2001 con cui l'Italia ha attuato la direttiva 2000/31/CE dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno.

10 Si tratta della direttiva 2001/31/CE di cui alla nota 9.

11 C. App. Milano, 27 febbraio 2013, p. 27.

12 M. Rosenfeld, Hate Speech in Constitutional Jurisprudence: A Comparative Analysis, 2001, http://ssrn.com/abstract=265939; D. K. Citron, H. Norton, Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age, 91 B.U.L. Rev. 1435 (2011);

apertamente omosessuale, la *Court of Appeal of the State of California*[13] ha statuito che la pubblicazione online di post minacciosi ovvero oltraggiosi verso una caratteristica personale della vittima configura la fattispecie di cyberbullismo. Pertanto, tale azione non può avvalersi delle garanzie di libertà di espressione fornite dal *First Amendment* della Costituzione americana in quanto integra l'*hate speech,* cioè l'incitamento all'odio, contrario alla protezione della dignità della vittima e della manifestazione della necessaria solidarietà con essa, doverosi elementi essenziali che non vengono meno neppure sul web.

Permanendo in materia di tutela delle minoranze, in particolare di quella omosessuale, la Corte distrettuale del *Western District of Missouri*[14] condannato, perchè discriminatoria, la pratica di filtraggio messa a punto da un locale distretto scolastico relativamente alla pubblicazione di contenuti inerenti alla promozione dei diritti delle persone LGBT *(Lesbian, Gay, Bisexual, Transgender)*. L'aspetto interessante di questa decisione è che inerisce non alla violazione della neutralità della Rete posta in essere con l'applicazione di un software di filtraggio preventivo, quanto piuttosto all'integrazione di una pratica discriminatoria contro una determinata categoria di soggetti nonché alla violazione dei diritti di libertà di manifestazione del pensiero protetti dal *First Amendment.*

Anche ordinamenti appartenenti ad altre tradizioni giuridiche si sono pronunciate sul medesimo tema: ad esempio, in Sudafrica, dove la Corte costituzionale[15] ha deciso una questione riguardante l'impugnazione di alcune disposizioni del Films and Publications Act (n. 65 del 1996) introdotto dal Films and Publications Amendment Act (n. 3 del 2009) che introduceva una sorta di controllo sui materiali pubblicati sui mezzi di comunicazione, Internet compresa per via della possibile diffusione di materiali pedopornografici online. La Corte costituzionale sudafricana ha stabilito che siffatto sistema è incostituzionale perchè viola la libertà di espressione, elemento vitale della democrazia. Al contrario, la giustizia brasiliana ha condannato Google a oscurare su YouTube il discusso film "Innocence of Muslims". L'istanza di oscuramento è stata presentata da una associazione di fedeli mussulmani e il giudice l'ha accolta perchè il film viola il sentimento religioso dei credenti. Google aveva l'obbligo di rimuo-

13 Court of Appeal of the State of California, B 207869, 15 marzo 2010, D. C. v. R. R. http://www.casp.net/california-anti-slapp-first-amendment-law-resources/caselaw/california-courts-of-appeal-cases/d-c-v-r-r/ La sentenza contiene una opinione dissenziente del giudice Frances Rothschild il quale ha affermato che l'opinione di maggioranza "alters the legal landscape to the severe detriment of First Amendment rights."

14 United States District Court for the, Central Division, PFLAG v. Camdenton R–III School Dist., 16.2.12, consultabile su http://www.aclu.org/lgbt-rights/pflag-v-camdenton-r-iii-school-district

15 Constitutional Court of South Africa, Print Media of South Africa v. Minister of Home Affairs, [2012] ZACC 28.9.1

vere il materiale entro dieci giorni, in caso contrario è condannata a una sanzione pecuniaria di 10.000 reais per ciascun giorno di inadempimento[16].

In Germania, invece, il dibattito sul filtraggio di contenuti ha riguardato tanto la tutela della privacy quanto quella dei diritti patrimoniali d'autore di opere digitali. Sotto il primo aspetto si ricordano le vicissitudini subite da un noto personaggio pubblico, Max Mosley, l'ex presidente della *Fédération Internationale de l'Automobile* che anni fa si ritrovò al centro di uno scandalo mondiale per la pubblicazione di un video girato a sua insaputa mentre lo ritraeva protagonista di un'orgia a sfondo nazista. Ottenuto un risarcimento in denaro con una importante sentenza emanata dalla High Court of Justice di Londra, Max Mosley non si ritenne comunque soddisfatto, poiché pretendeva la cancellazione totale del video[17]. Pertanto, egli adì la Corte europea dei diritti umani per far condannare il Regno Unito di Gran Bretagna proprio per non aver predisposto uno strumento di controllo preventivo sui materiali pubblicati online che ledano la privacy, tuttavia la Corte ha rigettato questa istanza perchè censoria[18]. Ciò nonostante l'importante personaggio sta proseguendo nella sua lotta citando Google presso le giurisdizioni nazionali affinchè venga obbligato rimuovere le immagini lesive della sua privacy[19].

Per quel che concerne la protezione del diritto patrimoniale d'autore, il Landgericht Hamburg,[20] giudice di primo grado della città anseatica, ha affermato che YouTube è responsabile per il caricamento di contenuti illeciti, cioè senza autorizzazione dei detentori dei diritti d'autore, effettuato dagli utenti. La questione vede contrapposti la *Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte* (GEMA) a YouTube, società controllata da Google. Accogliendo le istanze della GEMA, il giudice tedesco ha asserito che YouTube è tenuto a predisporre un software di filtraggio dei video i cui titoli contengano i nomi delle opere protette dal diritto patrimoniale d'autore e degli autori aderenti alla GEMA. Il *Landgericht Hamburg* ha osservato che il diritto dell'Unione Europea non preclude l'utilizzo di filtri software sull'uso delle parole, infatti la Corte di Giustizia dell'Unione Europea,[21] seppure abbia paventato il rischio che detto filtro possa portare a trattamenti indebiti di dati personali,

16 Sul punto si contano nel numero di e richieste di cancellazione provenienti dalle autorità governative brasiliane a Google proprio in merito a questo film. Fonte:

17 Mosley v. News Group Newspapers Ltd., [2008] EWHC (QB) 1777. In dottrina, J. E. Stanley, Max Mosley and the English Right to Privacy, 2012, http://ssrn.com/abstract=2009403

18 Corte europea dei diritti umani, 15 settembre 2001, Max Mosley v. Regno Unito di Gran Bretagna, App. n. 48009/08.

19 I. Hülsen, Max Mosley Sues Google in Landmark Battle over Digital Rights, Spiegel On Line, 31.8.12.

20 LG Hamburg, 310 O 461/10, 20.4.12.

21 L'esplicito riferimento effettuato nella motivazione del Landgericht Hamburg è il caso SABAM, la sentenza C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) del 16 febbraio 2012.

tale elemento non inerirebbe a questo caso, almeno a parere dei giudici di Amburgo. Ciò significa che la Corte tedesca non ammetterebbe il bilanciamento degli interessi in gioco, cioè quelli alla riservatezza e alla libertà di informazione degli utenti di Internet con quelli dei detentori dei diritti patrimoniali d'autore. Tuttavia essa afferma però che il rischio di blocco di contenuti leciti può essere eliminato attraverso una applicazione procedurale appropriata. A seguito di questa decisione, salutata dalla GEMA come una grande vittoria dei detentori dei diritti patrimoniali d'autore,[22] va registrato il fallimento di un tentativo di accordo di accesso a pagamento ai video musicali oggetto della disputa[23]. Inoltre, si osserva che in realtà il filtraggio dei materiali leciti ovvero illeciti pare essere indiscriminato, poiché sul sito tedesco di YouTube non viene interdetto l'accesso ai soli contenuti protetti, ma anche a video del tutto amatoriali che rappresentano elementi di cultura popolare[24] ovvero eclatanti eventi di cronaca, come quelli raffiguranti lo sciame di meteoriti caduto sui Monti Urali, in Russia nel febbraio scorso[25].

5. Conclusioni

Sono diversi i diritti fondamentali coinvolti nell'utilizzo di massa di Internet, quali la protezione della dignità (art. 1 della Carta dei diritti fondamentali dell'Unione Europea), della riservatezza (art. 7), dei dati personali (art. 8), della libertà di opinione e di critica (art. 10), e finanche della proprietà intellettuale (art. 17.2). Tuttavia, la partecipazione di massa sulla Rete dimostra come siano gli Internet Service Providers ad avere un rapporto di vicinanza e prossimità con i loro utenti. Seppure in questo contesto risulti essere difficile mantenere valida la distinzione tra controllori, provider e chi fruisce dei dati, l'applicazione di software di filtraggio non sembrerebbe essere uno strumento valido ed efficace nella protezione degli interessi in gioco. A questo proposito, parrebbe essere più appropriato lo strumento contrattuale. Infatti, esso offre un possibile rimedio preventivo sulla disciplina della responsabilità dei provider prevedendo al momento della sottoscrizione dell'abbonamento clausole contrattuali specifiche in materia di tutela di diritti fondamentali, della riservatezza, uploading e downloading a carico dell'utente che ponga in essere comportamenti illeciti.

---

22 GEMA Pressmitteilung, Urteil am Landgericht Hamburg: YouTube haftet für Nutzerinhalte, 20.4.2012, https://www.gema.de/presse/pressemitteilungen/presse-details/article/urteil-am-landgericht-hamburg-youtube-haftet-fuer-nutzerinhalte.html

23 K. J. O' Brien, Royalty Dispute Stops Music Videos in Germany, New York Times, 2.4.2009, http://www.nytimes.com/2009/04/03/technology/internet/03youtube.html?_r=0

24 P. Paukner, Diese Kultur ist in Deutschland leider nicht verfügbar, 28.1.13, Süddeutschen Zeitung, http://www.sueddeutsche.de/digital/streit-zwischen-youtube-und-gema-diese-kultur-ist-in-deutschland-leider-nicht-verfuegbar-1.1584813

25 C. Farivar, Germans can't see meteorite YouTube videos due to copyright dispute, 20.2.2013, http://arstechnica.com/tech-policy/2013/02/germans-cant-see-meteorite-youtube-videos-due-to-copyright-dispute/

Google/Vividown: leading case o abbaglio giurisprudenziale?

di Giovanni Maria Riccio (*)

Il caso

Con la pubblicazione delle motivazioni della Corte d'Appello di Milano, si chiude (finalmente) il caso Vividown c. Google, probabilmente il precedente più noto del diritto di internet in Italia[1].

Un caso che ha avuto un'ampia eco mediatica, anche al di fuori dei confini nazionali, ma che non può essere considerato un *leading case*. Tutte le accuse, ampiamente criticate dalla dottrina che si era occupata della vicenda, sono cadute, seppur dopo due gradi di giudizio.

Restano, però, alcuni dubbi, soprattutto in merito alle ricadute relative alla disciplina sulla protezione dei dati personali. La presente nota, pur nella sua brevità, si ripropone di affrontare tale profilo, volutamente tralasciando gli aspetti penalistici e processualisti del caso[2].

I fatti da cui trae origine la controversia sono noti. Alcuni ragazzini picchiano e maltrattano un loro compagno di classe disabile, riprendono la scena con un telefonino e pubblicano il video su Google Video. La bravata determina la condannata sia dei ragazzini (affidamento ai servizi sociali) che dell'insegnante presente in aula durante la ripresa del video.

In seguito, però, vengono citati in giudizio da Vividown, associazione a tutela delle persone disabili cui è iscritto il ragazzo malmenato, anche quattro dipendenti di Google (il Presidente del CdA di Google Italy; il responsabile delle policy sulla privacy per l'Europa; il responsabile del progetto Google Video per l'Europa; un altro membro del CdA di Google Italy).

L'accusa, per loro, è di diffamazione e violazione della privacy. La prima accusa discende dal fatto che i ragazzi, nel video, offendono il ragazzo disabile e menzionano anche l'associazione querelante, fingendo di appartenere a detta associazione.

La violazione della disciplina sulla tutela dei dati personali, invece, discenderebbe dalla mancata fornitura agli utenti dell'informativa privacy. L'art. 13 del D. Lgs. 196/2003, com'è noto, prevede una serie di informazioni che devo-

---

(*) In *Vita Notarile*.

[1] Basti ricordare, al riguardo, il convegno *Il futuro sulla responsabilità nella Rete. Quali regole dopo la sentenza sul caso Google/Vividown?*, organizzato dai proff. V. Zeno-Zencovich e S. Sica, e tenutosi il 21 maggio 2010 presso l'Università di Roma Tre. Gli interventi dei relatori sono pubblicati su *Dir. inf.*, 2010, volumi 2, 3, 4/5.

[2] La sentenza di appello, del resto, risulta essere già commentata, tra gli altri, da Cassano, *Google – Vividown. Assoluzione in Appello e … "tanto rumore per nulla"*, in *Dir. e giustizia*; Macrillò, *Caso Google – Vivi Down : negato in appello il concorso omissivo nel delitto ex art. 167 d.lgs. 196/03*, in *Riv. Penale*; Catullo, *Responsabilità penale del service provider e trattamento illecito dei dati*, in *Dir. Giustizia*; F. Resta, *Libertà della rete e protezione dei dati personali: ancora sul caso Vivi Down*, in *Indice Pen.*; (tutti contributi, al momento in cui si scrive, in corso di pubblicazione).

no essere fornite, tra cui le finalità del trattamento, la natura obbligatoria o meno della prestazione dei dati, i soggetti a cui i dati possono essere comunicati.

È altresì risaputo che la legge italiana prevede delle forti sanzioni per il mancato rispetto degli adempimenti richiesti. Il titolare del trattamento, ai sensi dell'art. 161 del D. Lgs. 196/2003, è punito con sanzioni amministrative (consistenti in una somma da seimila euro a trentaseimila euro) in caso di omessa o incompleta prestazione dell'informativa al soggetto interessato[3]. La disciplina legislativa, nel corso degli anni, è stata rettificata o emendata, da innovazioni legislative o interventi dell'Autorità Garante. Si pensi, ad esempio, alla possibilità per alcune società, tra cui quelle che offrono servizi di telefonia, di fornire un'informativa breve, che rimandi all'informativa completa. Un approccio che si sta diffondendo anche tra le aziende che fanno uso di cookies e che devono informarne l'utente, oltre che raccoglierne il consenso, come previsto dalla Direttiva 136/2009. Allo stesso modo, il Codice privacy contiene una serie di eccezioni all'obbligo dell'informativa, come nel caso di pediatri e medici di base.

Nel caso di specie, peraltro, veniva in rilievo l'art. 167 del Codice privacy che punisce "chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno" procede ad un trattamento di dati personali illecito. Pertanto, per determinare una condanna sul piano penale degli imputati, sarebbe stato necessario provare un fine di lucro in capo ai dipendenti di Google.

La sentenza di primo grado aveva assolto gli imputati dall'accusa di diffamazione, ma ne aveva condannati tre per violazione della legge sulla privacy.

In secondo grado le tesi accusatorie erano però ripetute nella requisitoria del Procuratore Generale, sostenendo che Google sarebbe stato "in grado di impedire l'immissione del video" e avrebbe avuto "i sistemi di controllo adatti da anni", senza esercitare tale controllo.

Le questioni

Le questioni, in estrema sintesi, sono tre.

È possibile ipotizzare una diffamazione in capo a Google e, quindi, un obbligo di controllo sui contenuti immessi in Rete?

È possibile coinvolgere nel processo anche Google Italy Srl, società controllata di Google Inc che, però, non ha accesso alla piattaforma Google Video, i cui server sono localizzati negli Stati Uniti e gestiti esclusivamente da Google Inc?

Infine: è ipotizzabile una violazione della privacy, dal momento che non sarebbe stata fornita alcuna informativa sulla tutela dei dati personali ai soggetti che caricavano il video?

---

[3] L'originaria disposizione normativa è stata così modificata dall'art. 44, comma 2, del decreto legge 30 dicembre 2008, n. 207 convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14. L'analisi dei provvedimenti del Garante per la protezione dei dati personali evidenzia, però, che le sanzioni per omessa o incompleta informativa sono non particolarmente frequenti e sono spesso associate ad altre violazioni della disciplina in materia di trattamento dei dati personali

Il primo punto, quello che, per usare le parole della sentenza, "attiene alla questione del governo di Internet", è risolto agevolmente dalla Corte, che afferma che "per sostenere la responsabilità a titolo di omissione in capo ad un *host* o *content provider*, occorre affermare a suo carico un obbligo giuridico di impedire l'evento e quindi da un lato, l'esistenza di una posizione di garanzia, dall'altro la concreta possibilità di effettuare un controllo preventivo".

Una posizione di garanzia che non è dato rinvenire nella legislazione vigente e, in particolare, nel D.Lgs. 70/2003 che anzi, all'art. 17, stabilisce un ISP non possa essere "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"[4]. Né sarebbe sostenibile l'estensione della normativa sulla diffamazione a mezzo stampa (artt. 57 e 57-bis c.p.), dal momento che si tratterebbe di un'analogia in *malam partem*, espressamente vietata nel nostro ordinamento.

Importante, sebbene incidentale, è invece il punto nel quale i giudici sostengono che l'imposizione di un sistema di filtraggio, l'unico in grado di operare un controllo preventivo sui contenuti immessi in Rete, avrebbe l'effetto di sovvertire l'architettura di Internet e l'attività degli intermediari della Rete, alterandone le sue funzionalità.

Un'affermazione rilevante, poiché riafferma il principio – troppe volte messo in discussione – della neutralità degli intermediari di Internet.

La possibilità di imporre l'adozione di sistemi di filtraggio è stata ampiamente discussa, in chiava critica dalla Corte di Giustizia, nel caso Scarlet[5]. In tale fattispecie, i giudici comunitari hanno affermato che le possibili ingiunzioni da ordinare agli ISP, ai sensi della direttiva n. 31 del 2000 sul commercio elettronico, non possono imporre ad un intermediario di internet di procedere ad "una sorveglianza generalizzata sulle informazioni che esso trasmette sulla propria rete" e tale "divieto abbraccia in particolare le misure nazionali che obbligherebbero un prestatore intermedio, come un FAI, a realizzare una vigilanza attiva su tutti i dati di ciascuno dei suoi clienti per prevenire qualsiasi futura violazione di diritti di proprietà intellettuale"[6].

---

[4] Sul punto, da ultimo, Petruso, *La responsabilità civile degli e-providers nella prospettiva comparatistica*, in Europa e dir. priv. 2011, 1138, il quale critica, in relazione alla decisione in esame, che non sia stata fatta distinzione tra *hosting* attivo e passivo.

[5] Corte di Giustizia, 24 novembre 2011 – Parti: Scarlet Extended SA c. Société Belge des auteurs, compositeurs et éditeurs SCRL (SABAM)

[6] Nelle parole della Corte di Giustizia, il sistema di filtraggio richiesto dalla SABAM, parte attrice nella controversia, determinerebbe, in capo alla Scarlet, l'insorgenza dell'"obbligo di procedere ad una sorveglianza attiva su tutti i dati di ciascuno dei suoi clienti per prevenire qualsiasi futura violazione di diritti di proprietà intellettuale" e che "includerebbe tutte le informazioni da trasmettere e ciascun cliente che si avvale di tale rete". Peraltro, gli effetti di tali ingiunzioni "non si limiterebbero al FAI coinvolto, poiché il sistema di filtraggio controverso è idoneo a ledere anche i diritti fondamentali dei clienti di tale FAI, ossia i loro diritti alla tutela dei dati personali e alla libertà di ricevere

L'applicabilità della normativa nazionale in materia di tutela dei dati personali

Il secondo punto, quello relativo all'assimilazione di Google Italy S.r.l. a Google Inc., rileva in relazione all'applicabilità della normativa sulla privacy al caso di specie.

Preliminarmente, deve ricordarsi che i video erano caricati su server localizzati negli Stati Uniti e che tali server non erano (e non sono) nella materiale disponibilità di Google Italy. L'art. 5, comma 2, del Codice della privacy prevede che la normativa italiana si applichi "anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici". Secondo la Corte d'Appello di Milano, Google Italy, società partecipata da Google Inc. e stabilita in Italia, sarebbe "una struttura organizzativa ben rientrante nella nozione di strumento anche non elettronico".

Di conseguenza, la legge sulla privacy italiana sarebbe applicabile al caso in questione.

Una soluzione che non convince, giacché gli strumenti non elettronici di cui discorre la legge sono, ad esempio, gli archivi cartacei[7]. Difficile immaginare che possa esserlo una società, per quanto controllata dalla società madre statunitense e da essa interamente partecipata[8].

Peraltro, i giudici non considerano che Google Italy, non potendo accedere ai server di Google Inc. (così come dimostrato nel corso dell'istruttoria), non effettuerebbe alcun trattamento dei dati personali. Difficile immaginare che tale collegamento sia determinato dalla presenza di pubblicità personalizzata per gli utenti italiani[9].

L'impressione, in tutta franchezza, è che i giudici italiani – al pari dei loro colleghi transalpini – abbiano esercitato una non meglio specificata *vis attactiva*, considerando Google, e tutte le società riconducibili a quel *brand*, quale

---

o di comunicare informazioni, diritti, questi ultimi, tutelati dagli artt. 8 e 11 della Carta".

[7] In relazione alla decisione di primo grado, ulteriori critiche erano state avanzate da Viola De Avezedo Cunha – Sartor, *Il caso Google-Vividown tra protezione dei dati e libertà di espressione online*, in *Dir. inf.*, 2010, 645.

[8] Parte della dottrina ha messo in discussione l'applicabilità della legge italiana sulla privacy, giacché l'immagine di una persona non rientrerebbe nella nozione di dato personale di cui all'art. 4 del D. Lgs. 196/2003; cfr. BEDUSCHI, *Caso Google: libertà d'espressione in Internet e tutela penale dell'onore e della riservatezza*, in *Corriere merito*, 2010, 960 ss.

[9] Così anche Maggio, *Il diritto di impresa non può prevalere sulla privacy e sulla tutela dei diritti della persona*, in *Riv. dir. ind.*, 2011, 47.

un'unica entità, a prescindere dall'esistenza di una rete piramidale, rappresentata da una serie di società dotate di una loro autonoma personalità giuridica[10].

Al di là di tale profilo, ad ogni modo, la sentenza conclude che la violazione dei dati personali, che era a fondamento della decisione di primo grado, non sarebbe stata compiuta. Il Tribunale, in primo grado, avrebbe applicato una norma errata: la mancata fornitura dell'informativa (la c.d. privacy policy) sarebbe sanzionata dall'art. 161 del Codice privacy e non dall'art. 167 Codice privacy. Una differenza non da poco, se si considera che, come accennato, nel primo caso l'illecito è punito con il pagamento di una sanzione amministrativa, mentre nell'altro si incorre in una responsabilità penale.

Mancherebbe inoltre – e trattasi di un aspetto che la dottrina aveva già segnalato in sede di commento della decisione di primo grado – un dolo specifico, non essendo richiesto, ai fini dell'applicabilità della norma, il mero dolo eventuale[11]. Allo stesso modo, si era fatto correttamente fatto notare che l'illecito di cui all'art. 167 Codice privacy può essere commesso solo mediante un atto commissivo e non mediante una mera omissione: pertanto, la mancata fornitura dell'informativa (così come un'informativa incompleta) avrebbe dovuto essere punita con una sanzione amministrativa e mai ai sensi della norma da ultimo citata[12].

In secondo luogo, e il profilo appare molto interessante, trattandosi di dati personali del ragazzo disabile, la sentenza chiarisce che l'informativa avrebbe dovuto essere fornita non da Google, ma dalla compagna di classe che aveva caricato il video sulla piattaforma[13]. Cade anche la previsione, pure criticata dai

---

[10] I giudici milanesi sembrano non tenere nella giusta considerazione né la teoria della sede reale (*Sitztheorie*), secondo cui il diritto societario applicabile è quello del luogo in cui, effettivamente, si svolge in via prevalente l'attività sociale, né la teoria della incorporazione (*Gründungstheorie*), secondo cui andrebbe osservato il dato formale del luogo di costituzione della società. L'ordinamento italiano, a differenza di altri (es. Germania e Francia), non propende per nessuna delle due teorie ma adotta un criterio, per dir così, misto Sul punto v. F.M. MUCCIARELLI, *Libertà di stabilimento comunitaria e concorrenza tra ordinamenti societari*, in *Giur. comm*., 2000, 6, 557 ss.; E. WYMEERSCH, *Il trasferimento della sede della società nel diritto societario europeo*, in *Riv. soc*., 2003, 4, p. 729 ss.; A. RIGHINI, *Il trasferimento transnazionale della sede sociale*, in *Contr. impresa*, 2011, p. 755 ss. La questione è stata ampiamente affrontata dalla Corte di Giustizia nel caso Cartesio, su cui v. S. LOMBARDO, *Le (a)simmetrie di Cartesio e la «nuova» libertà di stabilimento delle societa` nella prospettiva del Trattato di Lisbona*, in *Le Società*, 2010, p. 1084 ss.

[11] Cfr. Albamonte, *La responsabilità penale dell'internet provider tra libertà di comunicazione e tutela dei singoli (Nota a GIP Trib. Milano 24 febbraio 2010)*, in Questione Giustizia, 2010, 3, 184.

[12] Sul punto, per più ampie e approfondite argomentazioni, si rinvia a Manna, *La prima affermazione, a livello giurisprudenziale, della responsabilità penale dell'internet provider: spunti di riflessione tra diritto e tecnica,* in Giur. cost., 2010, 2, 1856.

[13] A tale conclusione era già giunta la dottrina in sede di commento della decisione di primo grado: cfr., *ex ceteris*, Beduschi, *Caso Google: libertà d'espressione in Inter-*

commentatori della sentenza e che non trova riscontro nel dato positivo della norma giuridica in rilievo, secondo cui il gestore della piattaforma sarebbe tenuto a invitare gli utenti a non utilizzare i servizi offerti per compiere attività illecite[14].

Se si accetta tale premessa – che, quindi, non vi fosse un obbligo specifico per la piattaforma informatica di fornire una *privacy policy* – allora deve convenirsi con quella parte della dottrina che, correttamente a parere di chi scrive, ritiene che non vi sia un rapporto di *genus ad speciem* tra disciplina sulla tutela dei dati personali e norme che regolano la responsabilità degli intermediari di internet, ricordando che la direttiva sul commercio elettronico ha previsto un approccio orizzontale, che prescinde dall'illecito concretamente realizzato[15].

Discorso diverso, pur affrontato da taluni commentatori, attiene all'efficacia deterrente dell'informativa. In altri termini, si afferma che, anche se la ragazzina che ha caricato il video avesse letto l'informativa sul trattamento dei dati personali, ciò non l'avrebbe distolta dal caricare il video sulla piattaforma.

La questione, posta in questi termini, appare mal posta e conduce ad una risposta retorica e, al tempo stesso, oziosa. È ovvio che l'informativa non scoraggia l'autore dell'illecito dal tenere una determinata condotta: tuttavia, bisogna anche convenire che tale non è la funzione richiesta dalla legge. L'art. 13 del D. Lgs. 196/2003 mira ad ingenerare una consapevolezza in capo al soggetto interessato, i cui dati saranno trattati. Quella consapevolezza che segna il passaggio da un modello ottocentesco di privacy, intesa come diritto ad evitare intromissioni nella propria sfera privata (o, per dirla altrimenti, come *right to be let alo-*

---

net e tutela penale dell'onore e della riservatezza, cit., 961; Lotierzo, *Il caso google - Vivi down quale emblema del difficile rapporto degli internet providers con il codice della privacy*, in Cass. Pen., 2010, 11, 3994; Melzi D'Eril – Vigevani, *Nelle motivazioni di condanna della sentenza violazione della privacy per mancato consenso (Nota a Trib. Milano sez. IV pen. 24 febbraio 2010, n. 1972)*, in *Guida al Diritto*, 2010, 25, 21, nonché, nella dottrina non italiana, Mendez, *Google Case in Italy*, *International Data Privacy Law*, Oxford Univ., 2011. Altra parte della dottrina ha invece sostenuto che Google non sarebbe stata tenuta a fornire un'informativa, dal momento che la sua condotta rientrerebbe nelle esenzioni previste per l'attività giornalistica, *ex* art. 136 D. Lgs. 196/2003, ovvero che dal momento che l'informativa all'interessato comporterebbe un impiego di mezzi manifestamente sproporzionati rispetto al diritto tutelato (sebbene, in questa seconda ipotesi, il Garante dovrebbe individuare delle modalità alternative); cfr. Mantelero, *La responsabilità on-line: il controllo nella prospettiva dell'impresa*, in *Dir. inf.*, 2010, 405 ss.

[14] Sul punto v. *amplius* Melzi D'Eril – Vigevani, *op. cit.*, 20.

[15] Bugiolacchi, *(Dis)orientamenti giurisprudenziali in tema di responsabilità degli internet provider*, in *Resp. civ. e prev.*, 2010, 1575 ss.

ne)[16], ma come controllo sulle informazioni che consentono di risalire alla mia persona o di ricostruire un mio immaginario profilo[17].

L'informativa, allora, altro non è se non un passaggio di un procedimento, segnato da tappe progressive nelle cui maglie si individua un ritorno al formalismo degli atti[18].

Al contrario, si potrebbe discutere su quanto l'obiettivo di tutelare il soggetto interessato, per mezzo di una maggiore consapevolezza sul trattamento dei dati, sia effettivamente raggiunto per mezzo dell'informativa.

Una recente indagine condotta dall'ICO (Information Commissioner's Office) dimostra che il 71% degli utenti non legge le informative pubblicate sui siti e che il 62% degli utenti stessi vorrebbe che queste informative fossero più chiare e/o semplificate[19].

Non sorprende, quindi, che un'altra ricerca indipendente abbia spiegato che occorrerebbero ben 244 ore lavorative all'anno per leggere tutte le nuove privacy policy che un utente incontra e che, anche a voler operare una scrematura di tali privacy policy, con il rischio quindi di "saltare" informazioni importanti, le ore necessarie sarebbero comunque non meno di 154[20].

Il rischio, quindi, è che le informative previste dall'art. 13 D. Lgs. 196/2003 si risolvano in documenti lunghi, di difficile comprensione per gli utenti[21]. Ciò determina, quindi, uno snaturamento della funzione stessa dell'informativa, che

---

[16] Secondo la ben nota ricostruzione risalente a Warren – Brandeis, *The Right to Privacy*, 4 *Harv. L. Rev.* 193, (1890).

[17] Rodotà, *Privacy e costruzione della sfera privata. Ipotesi e prospettive*, in *Pol. dir.*, 1981, 532.

[18] Il punto è ampiamente sviluppato da Sica, *Art. 1350. Degli atti che devono farsi per iscritto*, in *Comm. cod. civ.* diretto da F.D. Busnelli, Milano, 2003, *passim*. È noto il dibattito che, nel corso della fine del secolo scorso, ha investito la forma; in via di estrema sintesi, si rinvia ai due celebri saggi di Irti, *Idola libertatis. Tre esercizi sul formalismo giuridico*, Milano, 1985, e Perlingieri, *Forma dei negozi e formalismo degli interpreti*, Napoli, 1989.

[19] *Regulators demand clearer privacy policies*, in *Out-Law*, http://www.out-law.com/page-9795

[20] Mcdonald – Faith Cranor, *The Cost of Reading Privacy Policy*, 4:3 Journal of Law and Policy for the Information Society, 540 (2008).

[21] Aggregando i due dati, è facile concludere che gli utenti non leggono il contenuto delle informative privacy perché troppo complesse e lunghe. Del resto, la lunghezza delle policy privacy risponde sì alla necessità di essere *compliant* con le previsioni legislative, ma, al tempo stesso, è uno strumento per scoraggiare la lettura, così come avviene per le licenze dei software. Anche in questo settore, seppur con minore scientificità, è stato dimostrato che solo il 3,13% degli utenti leggerebbe attentamente i contratti di licenza, mentre il 25% ne leggebbe solo la parte relativa alle restrizioni legali e ben il 71,88% non li leggerebbe affatto[21]: una conclusione che potrebbe essere anche peggiore se il campione selezionato fosse italiano, considerando che, non di rado, gli accordi di licenza sono scritti esclusivamente in inglese.

si traduce in una tutela del soggetto che la predispone e non di colui che dovrebbe leggerla.

In definitiva, sebbene non possa chiedersi all'informativa di contribuire alla prevenzione di eventuali illeciti, non può non convenirsi che uno snellimento delle forme, nel settore della privacy, sarebbe onestamente auspicabile[22].

Uno snellimento che non deve essere letto come un'istanza di una privacy in tono minore, ma solo di una migliore privacy, le cui norme possano tutelare effettivamente, e non formalmente, i cittadini[23].

L'assenza di un fine di lucro (*rectius*: di un beneficio patrimoniale diretto)

Infine, un cenno merita il profilo del ritorno economico che Google avrebbe ottenuto, indirettamente, per mezzo della pubblicità presente sulla piattaforma. A giudizio della Corte d'Appello meneghina, il giudice di primo grado, sul punto, avrebbe commesso due errori: il primo di fatto, dal momento che non era vero che su Google Video fosse diffusa pubblicità[24]; il secondo, di diritto (in senso lato), giacché il contenuto della pubblicità non sarebbe stato comunque associato a quello del video e, quindi, non vi sarebbe stata una correlazione diretta tra l'illecito e l'eventuale fine di lucro[25]. Al riguardo, basti affermare che tutti gli operatori di Internet operano, al pari di ogni altro imprenditore, per un ritorno

---

[22] La questione potrebbe addirittura peggiorare a seguito della probabile approvazione della Proposta di Regolamento concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (Regolamento generale sulla protezione dei dati).

[23] Una migliore privacy che potrebbe anche comportare una minore spesa per le imprese. Si faccia attenzione: non vuole sostenersi che i costi per la privacy non siano necessari. Tali costi devono rientrare, nell'ottica di tutela della persona, tra i costi di impresa, costi assolutamente irrinunciabili, come potrebbero essere quelli per la sicurezza. Tuttavia, aumentare progressivamente adempimenti meramente formali – come accade anche nella nuova Proposta di Regolamento – non può essere la via da perseguire. Sugli aumenti di costi, in caso di approvazione del Regolamento, si rinvia a Christensen – Colciago – Etro – Rafert, *The Impact of the Data Protection Legislative Framework in the E.U.*, University of Venice, Ca' Foscari, Dept. of Economics, in corso di pubblicazione.

[24] A seguito della requisitoria del PG, L'Avv. Bongiorno, membro del collegio difensivo, aveva affermato: "Come è emerso chiaramente dalle indagini della polizia giudiziaria non vi era alcun messaggio pubblicitario connesso a Google Video e pertanto Google non ha tratto alcun profitto da questo o altri video".

[25] Sul punto, commentando la decisione di primo grado, Mendez, *Google Case in Italy*, cit., aveva giustamente affermato che "The Google case in Italy is not consistent with the law, and it imposes liability when it is not required. The crucial misinterpretation of the law arises from the Court's failure to recognize the role of an information society service provider. The provider of Information Society services catalogues, indexes, and arranges the data without modifying the content. If the service provider makes a profit from indexing and cataloguing the data, it does not necessarily mean the provider is intending to break the privacy laws".

economico e non per finalità filantropiche. Tuttavia, il vantaggio economico di questi soggetti non è necessariamente – come nel caso di Google – associato ai contenuti immessi dagli utenti. Ad analoghe considerazioni è arrivata da decenni la giurisprudenza statunitense in materia di copyright, che parla della necessità di un *direct financial benefit* (ossia di un vantaggio economico diretto)[26], così come, in epoca più recente, la Corte di Giustizia[27].

In ogni caso, ritenere che l'ISP possa essere responsabile anche in caso di beneficio economico indiretto, sarebbe come condannare un gestore telefonico per le telefonate di stalking compiute da un suo cliente: anche l'operatore di telefonia ha un ritorno economico dalle telefonate compiute (e per di più Google non ha tratto alcun profitto dal video incriminato o, quanto meno, trattasi di un aspetto non adeguatamente provato dall'accusa). Prospettata così, però, sembrerebbe una soluzione peregrina. Per quale motivo le cose dovrebbero essere diverse per operatore di internet?

Conclusioni

Come si diceva in apertura, con la decisione della Corte d'appello dovrebbe chiudersi una vicenda che aveva destato un enorme scalpore, dovuto alle prime condanne penali per dirigenti di Google, ma che, sul piano meramente giuridico, poco aveva aggiunto al dibattito sulle responsabilità in internet. Un impianto accusatorio originario disarticolato da qualsivoglia impianto normativo, una decisione di primo grado in buona parte corretta, seppur scivolata su di un errore in-

---

[26] Cfr. caso *Religious Technology v. Netcom*, 907 F. Supp. 1361 (N.D. Cal. 1995),dove si afferma che il beneficio economico ottenuto dall'ISP deve essere direttamente connesso con la violazione perpetrata dal terzo. Giova riportare il passaggio della decisione Netcom: "Plaintiffs must further prove that Netcom receives a direct financial benefit from the infringing activities of its users. For example, a landlord who has the right and ability to supervise the tenant's activities is vicariously liable for the infringements of the tenant where the rental amount is proportional to the proceeds of the tenant's sales. *Shapiro, Bernstein*, 316 F.2d at 306. However, where a defendant rents space or services on a fixed rental fee that does not depend on the nature of the activity of the lessee, courts usually find no vicarious liability because there is no direct financial benefit from the infringement". Sul punto, per ulteriori precisazioni sul punto, con riferimento al contesto del *copyright* statunitense sia consentito rinviare a Riccio, *La responsabilità civile degli internet providers*, Torino, 2002, cap. 2 e 4. Analoghe considerazioni sono svolte, da ultimo, in *Viacom International, Inc. v. YouTube, Inc.*, No. 07 Civ. 2103.

[27] Testualmente, la Corte di Giustizia, punto 116: "*Occorre osservare che la semplice circostanza che il servizio di posizionamento sia a pagamento, che la Google stabilisca le modalità di pagamento, o ancora che essa dia informazioni di ordine generale ai suoi clienti, non può avere come effetto di privare la Google delle deroghe in materia di responsabilità previste dalla direttiva 2000/31*". Cfr. anche Alvanini, *La responsabilità dei services providers*, in *Dir. ind.*, 4, 2010, 332; in senso parzialmente contrario, sempre in merito all'orientamento della giurisprudenza comunitaria, Giove – Comelli, *Responsabilità del provider per mancata rimozione di link a materiale illecito*, in *Dir. ind.*, 2012, 75.

terpretativo, una decisione di secondo grado che rimette ordine: più che di un *leading case*, si tratta di un cambio di rotta rispetto ad uno svarione giurisprudenziale.

Non può tacersi, però, che il lungo tempo intercorso tra l'inizio delle indagini e la decisione in commento costituisce un ulteriore tassello al calo di immagine del nostro Paese di fronte a potenziali investitori stranieri.

Se, poi, cumuliamo il problema endemico delle lungaggini processuali con l'incertezza che regna spesso nelle decisioni giudiziarie che riguardano internet e con il sensazionalismo, anziché la volontà di risolvere i reali problemi, che muove talune indagini, il quadro che ne emerge risulta estremamente preoccupante per un sereno e stabile sviluppo economico di internet in Italia.

Libertà della rete e protezione dei dati personali:
ancora sul caso Vivi Down

di Federica Resta (*) [1]

1. Premessa

Con la sentenza in epigrafe[2], la Corte d'appello di Milano torna a occuparsi del rapporto tra libertà della rete e tutela dei dati personali, in relazione alla vicenda Vivi Down-Google esaminata, in primo grado e con esiti parzialmente diversi, dalla IV Sezione del Tribunale di Milano, con sentenza n. 1972 del 12.4.2010[3].

Il caso all'esame della Corte riguardava la diffusione in rete, attraverso il canale Google Video, e in assenza del consenso dell'interessato, di un filmato realizzato da alcuni studenti minorenni, ritraente atti vessatori commessi ai danni di un compagno (anch'egli minore) con ritardo mentale e frasi di scherno pronunciate nei confronti dell'associazione Vivi Down, per la ricerca scientifica e per la tutela della persona Down. Le immagini erano state rimosse da Google Video a circa due mesi di tempo dalla loro pubblicazione on-line e a ventiquattro ore dopo che Google era stata avvertita – da un privato e dalla polizia postale - della presenza del video sul canale in esame.

In primo grado, gli imputati (dirigenti di Google) erano stati assolti, per insussistenza del fatto, dall'imputazione di concorso (omissivo) nel reato di diffamazione (aggravata dal mezzo) commessa ai danni del minore e dell'Associazione Vivi Down, mentre erano stati condannati per trattamento illecito di dati personali, avendo in particolare omesso di effettuare gli adempi-

---

(*) In *Diritto dell'Informazione e dell'Informatica*.

[1] Avvocato, dottore di ricerca in diritto penale e funzionario del Garante per la protezione dei dati personali. Le opinioni contenute in questo contributo sono espresse a titolo personale e non impegnano in alcun modo l'Istituzione di appartenenza.

[2] Su cui vds. G. CASSANO, *Google – Vividown. Assoluzione in Appello e … "tanto rumore per nulla*", in corso di pubblicazione su *Diritto e giustizia*.

[3] Pubblicata, tra l'altro, in *Giur. Mer*., 2010, n. 9, 2232, con nota di V. PEZZELLA, *Google Italia, diffamazione e riservatezza: il difficile compito del provider (e del giudice)*; v. anche F.G. CATULLO, *Ai confini della responsabilità penale: che colpa attribuire a Google, ivi*., 2011, n. 1, 159. Su questi temi v. anche L. PICOTTI, *I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali*, in *Rivista giuridica di merito*, 2012,12; G. CORRIAS LUCENTE, *Ma i* network providers, *i* service providers *e gli* access providers *rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che gestiscono?*, in *Giur. Mer*.,, 2004, 2526; R. LOTIERZO, *Il caso* Google-Vivi Down *quale emblema del difficile rapporto degli* internet providers *con il codice della* privacy, in *Cass. Pen*., 2010, pp. 1288 e ss.; A. MANNA, *I soggetti in posizione di garanzia*, in *Dir. inf*., 2010, pp. 779 e ss. ; A. INGRASSIA, *Il ruolo dell'*internet service provider *nel ciberspazio: cittadino, controllore o tutore dell'ordine? Risposte attuali e scenari futuribili di una responsabilità penale dei* provider, in penalecontemporaneo.it e ID., *La Corte d'Appello assolve i manager di Google anche dall'accusa di illecito trattamento dei dati personali, ibid.*.

menti prescritti dalla disciplina in materia di protezione dei dati personali[4], con relativo nocumento per il minore e al fine di trarne profitto mediante il servizio Google video.

2. Giurisdizione e competenza: no *server, but law*

La sentenza di appello – nel confermare l'assoluzione per il concorso nella diffamazione – riforma invece la pronuncia di primo grado sul punto del trattamento illecito, sancendo anche in tal caso l'assoluzione per insussistenza del fatto, fornendo peraltro importanti indicazioni, in particolare, sulla configurabilità, in capo all'internet provider, della responsabilità penale per reati commessi in rete.

Anzitutto, la sentenza conferma la giurisdizione del giudice italiano e, quindi, la propria competenza, con riferimento al caso di specie, disattendendo le eccezioni avanzate dalla difesa. In particolare, la Corte rileva come la giurisdizione del giudice nazionale si radichi in ragione del verificarsi dell'evento del reato in Italia, nonostante il "caricamento del server" (e dunque una frazione della condotta) si verifichi all'estero[5]. In relazione al delitto di diffamazione, infatti, l'evento si è verificato nel territorio nazionale - nella forma della percezione dell'espressione ingiuriosa da parte di persone che si trovavano in Italia- come pure gli effetti pregiudizievoli del delitto di trattamento illecito di dati personali (art. 167 d.lgs. 196/2003). Quanto alla competenza territoriale, poi, essa è correttamente attribuita all'autorità giudiziaria milanese ai sensi degli artt. 8 e 9 c.p.p., trovandosi a Milano la sede di Google Italy, responsabile della condotta contestata. Tale localizzazione consente poi di ritenere applicabile alla società la disciplina in materia di protezione dei dati personali, ai sensi dell'art. 5, comma 1, del d.lgs. 196/2003. Del resto, anche qualora non si dovesse ritenere rilevante, nel caso di specie, il principio di stabilimento enunciato da tale disposizione, l'applicabilità della disciplina in materia di protezione dei dati personali deriverebbe dal disposto di cui al comma 2 del citato art. 5, secondo cui è sufficiente che nel territorio dello Stato si trovino strumenti anche non elettronici impiegati per il trattamento in questione.

E' del resto principio ormai consolidato che il fatto che il server del sito non si trovi fisicamente in Italia non esclude la giurisdizione italiana, laddove almeno una parte del comportamento contestato avvenga nel nostro Paese. Come ad esempio avviene quando chi carichi sul sito delle immagini o dei contenuti illeciti si trovi in Italia. Si è quindi affermata la regola "no server but law", contro

---

[4] Acquisizione del consenso informato dell'interessato, peraltro in forma scritta, trattandosi di dati sensibili in quanto idonei a rivelare lo stato di salute dell'interessato (artt. 23 e 26 d.lgs. 196/2003); interpello al Garante per la verifica preliminare del trattamento che presenta rischi specifici (art. 17 d.lgs. 196)

[5] Come affermato, in relazione alla diffamazione on-line, ad es,., da Cass., Sez. II, Sent. n. 36721 del 21-02-2008 (ud. del 21-02-2008), B.M.I. (rv. 242085); Cass., Sez. V, sent. n. 4741 del 27-12-2000 (cc. del 17-11-2000), (rv 217745).

l'altra: "no server no law", al fine di impedire che la legge possa essere aggirata sfruttando la stessa assenza di confini che caratterizza la rete.

3. Il concorso (omissivo) nel delitto di diffamazione

a)La sentenza di primo grado

La sentenza appellata assolveva il responsabile privacy per l'Europa di Google, il presidente del consiglio di amministrazione di Google Italy e il suo amministratore delegato, nonché il responsabile del progetto Google video per l'Europa, dall'accusa di concorso omissivo (ex art. 40 cpv CP) nel reato di diffamazione per avere, in sostanza, omesso di impedire la divulgazione in rete di simili immagini dal contenuto diffamatorio (definito di "bullismo mediatico" in sentenza).

L'assoluzione, sul punto, si fondava sulla ritenuta insussistenza, in capo agli imputati (nella loro qualità di content provider), di una posizione di garanzia da cui derivi un obbligo di attivazione volto a impedire altrui condotte illecite commesse in rete, mediante il controllo preventivo sul contenuto dei dati immessi nel relativo spazio web, non potendo tale posizione di garanzia rinvenirsi, ai fini in esame, negli adempimenti prescritti al titolare del trattamento dal codice in materia di protezione dei dati personali (d.lgs. 196/2003). La posizione contraria, sostenuta dai magistrati del pubblico ministero, si richiamava principalmente a quanto sostenuto dalla Cassazione sul caso "Pirate bay" (sez. terza penale, sent. n.49437/09 del 23.12.2009), in materia di responsabilità penale degli internet service provider per le violazioni della disciplina sul diritto d'autore commesse in rete[6]. In tale pronuncia, si ammette tra l'altro la possibili-

[6] Su tema analogo cfr. anche Corte di giustizia, Grande Sezione, sent. 29.1.2008, Promusicae (C-275/06), secondo cui "La direttiva del Parlamento europeo e del Consiglio 8 giugno 2000, 2000/31/CE, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («direttiva sul commercio elettronico»), la direttiva del Parlamento europeo e del Consiglio 22 maggio 2001, 2001/29/CE, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, la direttiva del Parlamento europeo e del Consiglio 29 aprile 2004, 2004/48/CE, sul rispetto dei diritti di proprietà intellettuale, e la direttiva del Parlamento europeo e del Consiglio 12 luglio 2002, 2002/58/CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), non impongono agli Stati membri, in una situazione come quella oggetto della causa principale, di istituire un obbligo di comunicare dati personali per garantire l'effettiva tutela del diritto d'autore nel contesto di un procedimento civile. Tuttavia, il diritto comunitario richiede che i detti Stati, in occasione della trasposizione di tali direttive, abbiano cura di fondarsi su un'interpretazione delle medesime tale da garantire un giusto equilibrio tra i diversi diritti fondamentali tutelati dall'ordinamento giuridico comunitario. Inoltre, in sede di attuazione delle misure di recepimento delle dette direttive, le autorità e i giudici degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme a tali direttive, ma anche evitare di fondarsi su un'interpretazione di

tà di un concorso del provider nel reato contestato agli uploaders, qualora il primo non si limiti alla mera " messa a disposizione del protocollo di comunicazione" ma compia, invece, attività - quali, in particolare, l'indicizzazione dei contenuti inseriti- ulteriori rispetto al mero file transfert e tali dunque da realizzare un apporto causale all'altrui condotta illecita, penalmente rilevante ex art. 110 c.p..

Sulla base di tale interpretazione dovrebbe quindi ritenersi corresponsabile del reato di cui all'art. 167 d.lgs. 196/2003 il provider che (come nel caso in esame) non si limiti a fornire un semplice rapporto di interconnessione, ma, ge-

---

esse che entri in conflitto con i detti diritti fondamentali o con gli altri principi generali del diritto comunitario, come, ad esempio, il principio di proporzionalità". Ancora, sul tema del rapporto tra diritto d'autore e protezione dati, cfr. Corte di giustizia, Terza Sezione, sent. 24.11.2011, Sabam c. Scarlet (C 70-2010), secondo cui l'ordine imposto, in sede giurisdizionale, a un internet service provider, di apprestare un sistema di filtraggio preventivo e generalizzato di tutte le comunicazioni elettroniche degli utenti (sistema di tipo *deep packet inspection*) non appare compatibile (oltre che con la libertà d'impresa, anche con) il principio stabilito dall'art. 15 della direttiva 2000/31/CE, che vieta alle autorità nazionali di adottare misure che impongano a un fornitore di accesso ad Internet di procedere ad una sorveglianza generalizzata sulle informazioni che esso trasmette sulla propria rete (come già statuito dalla Corte con la sentenza L'Oréal del 12.7.2011, causa C-324/09, secondo cui il divieto di cui al citato art. 15 comprenderebbe anche le misure nazionali che obbligherebbero un prestatore intermedio, quale il fornitore di accesso a internet, a realizzare una vigilanza attiva su tutti i dati di ciascuno dei suoi clienti per prevenire qualsiasi futura violazione di diritti di proprietà intellettuale. Peraltro, un obbligo siffatto di vigilanza generale sarebbe incompatibile con l'art. 3 della direttiva 2004/48, il quale enuncia che le misure contemplate da detta direttiva devono essere eque e proporzionate e non eccessivamente costose).. Tale sistema, inoltre, per le concrete modalità con cui dovrebbe essere predisposto, violerebbe, ad avviso della Corte, il principio di proporzionalità nella misura in cui imporrebbe – sia pure per la tutela del diritto d'autore – un sacrificio eccessivo a diritti fondamentali degli utenti quali quelli alla riservatezza delle comunicazioni e alla protezione dei dati personali. Da un lato, infatti, secondo la Corte, tale sistema di filtraggio implicherebbe un'analisi sistematica di tutti i contenuti, nonché la raccolta e l'identificazione degli indirizzi IP degli utenti all'origine dell'invio dei contenuti illeciti sulla rete, indirizzi che costituiscono dati personali protetti, in quanto consentono di identificare in modo preciso suddetti utenti. Dall'altro, tale sistema rischierebbe di ledere la libertà di informazione, poiché potrebbe non essere in grado di distinguere adeguatamente tra un contenuto lecito e un contenuto illecito, sicché il suo impiego potrebbe produrre il risultato di bloccare comunicazioni aventi un contenuto lecito (una sorta di "chilling effect"). Infatti – osserva la Corte – la liceità di una trasmissione dipende anche dall'applicazione di eccezioni di legge al diritto di autore che variano da uno Stato membro all'altro. Inoltre, in certi Stati membri talune opere possono rientrare nel pubblico dominio o possono essere state messe in linea gratuitamente da parte dei relativi autori. Pertanto, secondo la Corte, l'imposizione di un simile sistema di filtraggio non rispetterebbe l'obbligo di garantire un giusto equilibrio tra, da un lato, il diritto di proprietà intellettuale e, dall'altro, la libertà di impresa, il diritto alla tutela dei dati personali e la libertà di ricevere o di comunicare informazioni.

stendo i dati in suo possesso, “ne divenga in qualche modo “dominus” e quindi “titolare del trattamento” ai sensi di legge, con gli obblighi corrispondenti”.

Da tale posizione di garanzia – così ricostruita – deriverebbe inoltre, in capo al fornitore che realizzi le suddette attività (tale dunque da essere qualificato come hoster attivo, se non addirittura content provider), un obbligo “preventivo” di controllo sui video caricati sul sito, anche mediante la predisposizione di sistemi di filtraggio, di talché l’aver mantenuto sul sito Google Video il video in questione, per un periodo di quasi due mesi, integrerebbe gli estremi del concorso omissivo nel reato di diffamazione.

Sintetizzando la posizione dei pubblici ministeri, dunque, la responsabilità degli imputati deriverebbe dal mancato controllo (preventivo) sul contenuto del video, agli stessi addebitabile in virtù della posizione di garanzia rivestita dal “ content provider” nei confronti del trattamento dei dati personali dei soggetti contenuti negli uploading degli utenti. L’omesso controllo del corretto trattamento dei dati personali contenuti nel video avrebbe dunque causato l’evento del reato contestato, che altrimenti non sarebbe avvenuto (o sarebbe avvenuto con minor danno da diffusione per la persona offesa). Tale argomento si fonderebbe sul rilievo secondo cui, essendo il “content provider” un produttore o gestore di contenuti, l’illiceità del contenuto si propagherebbe al gestore medesimo in virtù del ricordato principio collegato alla posizione di garanzia (principio riaffermato, a loro dire, dalla sentenza “Pirate bay”).

Di contro, ad avviso del giudice di prime cure, benché il gestore o proprietario del sito web qualificabile come “ content provider” possa e debba essere ritenuto potenzialmente responsabile della violazione della disciplina di protezione dati, non si può tuttavia “renderlo per ciò solo corresponsabile di altro reato di diffamazione (ma non solo) derivabile dal contenuto del materiale caricato. Ed infatti, pur ammettendo per ipotesi che esista un potere giuridico derivante dalla normativa sulla privacy che costituisca l’obbligo giuridico fondante la posizione di garanzia, non vi è chi non veda che tale potere, anche se correttamente utilizzato, certamente non avrebbe potuto “ impedire l’evento” diffamatorio”. Del resto, dal momento che la posizione di garanzia impone al soggetto nei cui confronti viene sancita un obbligo “ preventivo” di impedire l’evento illecito - e non un mero obbligo di farne cessare gli effetti - nell’ipotesi in esame, dall’obbligo del gestore di impedire l’evento diffamatorio, deriverebbe il correlato dovere di effettuare “un controllo o un filtro preventivo su tutti i dati immessi ogni secondo sulla rete”. Condotta, questa, che il Tribunale qualifica come “inesigibile e quindi non perseguibile penalmente ai sensi dell’art. 40 Cpv. c.p.”

Sarà dunque possibile, ad avviso del Tribunale, ravvisare in capo ai provider (in particolare se “si tratti di hoster attivi o content provider”) la responsabilità per i contenuti divulgati nello spazio web dagli stessi gestito solo provandosene la consapevolezza. Nel caso in esame, ad avviso del Tribunale, il fatto, che il video fosse stato presente sul sito per due mesi, addirittura tra i video più “cliccati” dagli utenti, costituirebbe “un principio di prova della “consapevolezza”

da parte dei gestori del suo contenuto; principio che non ha raggiunto la pienezza della prova solo per l'estrema difficoltà dell' effettuazione delle indagini (e della ricostruzione del dolo del soggetto agente) in vicende di questo tipo". Qualora la consapevolezza, in capo ai gestori, dei contenuti trasmessi fosse stata pienamente provata, si sarebbe allora potuto ritenere esigibile un obbligo d'impedimento dell'evento, sulla scorta di quanto previsto dall'art. 16 del d.lgs. 70/2003 ma anche di quanto affermato dalla Cassazione nel citato caso "Pirate bay", secondo cui, appunto, il gestore concorre nel reato quando compie attività, quali quella dell'indicizzazione delle informazioni provenienti dagli utenti, che gli consentano di percepire il contenuto dei *file* immessi in rete.

b) La sentenza di appello

Su questa scia, la Corte d'appello di Milano conferma l'assoluzione degli imputati dal concorso nella diffamazione, rilevando come l'appello proposto dal pubblico ministero non fornisca elementi di ordine "logico o probatorio" suscettibili di fondare una diversa decisione, ma non senza fornire ulteriori indicazioni sul tema della responsabilità del provider per i reati commessi in rete. Rileva infatti la Corte come, anzitutto, ai fini dell'imputabilità, all'host o al content provider, a titolo di concorso omissivo, dei reati da altri commessi in rete, sia necessario individuare a suo carico un obbligo giuridico d'impedimento dell'evento e, dunque, da un lato la sussistenza di una posizione di garanzia e, dall'altro, la concreta possibilità di effettuare un controllo preventivo sulla rete[7].

Ebbene, riguardo alla posizione di garanzia, la Corte ribadisce l'assenza di una previsione normativa in tal senso, non essendo d'altro canto estensibile analogicamente il disposto di cui agli artt. 57 e 57-bis c.p.[8], a ciò ostando il divieto di analogia *in malam partem* in materia penale, quale corollario del principio di stretta legalità e tassatività di cui all'art. 25, cpv., Cost.

Né, d'altro canto, una posizione di garanzia correlata a un dovere di attivazione da parte del provider potrebbe fondarsi sugli adempimenti prescritti al titolare del trattamento dalla disciplina in materia di protezione dei dati personali, che non contempla specificamente le condotte in questione e persegue finalità

---

[7] Sulla linea, dunque, di quanto già affermato dal Tribunale di Milano con la sentenza del 18.3.2004, in Giur. Mer., 2004, 1719, con nota di F. RESTA, *La responsabilità penale del provider: tra lasseiz faire ed obblighi di controllo*, secondo cui "I proprietari delle infrastrutture di telecomunicazione (c.d. network providers), i fornitori di accessi (c.d. access providers) ed i fornitori di servizi (c.d. service providers), non possono ritenersi corresponsabili dei reati commessi da coloro che utilizzano i loro servizi (c.d. content providers) per mera omissione di controllo, in quanto, da una parte, non hanno un obbligo giuridico di evitare l'evento, e dall'altro, per la struttura stessa della rete, non hanno la possibilità concreta di esercitare un efficace controllo sui messaggi ospitati sul proprio sito".

[8] Per l'affermazione secondo cui, *de jure condito*, il dettato dell'art. 57 c.p. non si applica al direttore di un quotidiano *on line*, cfr., in particolare, Cass., sez. V, sent. n. 35511 del 16.7.2010.

diverse (dalla violazione degli obblighi privacy non deriverebbe, peraltro, l'evento verificatosi, con conseguente interruzione del nesso eziologico tra condotta ed evento).

Del resto, la posizione di garanzia in questione non potrebbe rinvenirsi – come pure ammesso dalla giurisprudenza[9]- dall'esistenza di un "potere giuridico o di fatto attraverso il corretto uso del quale il soggetto garante sia in grado, attivandosi, di impedire l'evento", in quanto anche la predisposizione dei vari sistemi di filtraggio dei contenuti all'epoca dei fatti disponibili non avrebbe consentito, ad avviso della Corte, l'impedimento dell'evento. In altri termini, anche ravvisando in capo al *provider* - come prospettato dal P.G. - quale fonte dell'obbligo di impedimento di illeciti altrui, il carattere pericoloso dell'attività compiuta da *Google Video*, «si finirebbe per richiedere un comportamento inesigibile e di conseguenza non perseguibile penalmente ai sensi dell'art. 40 cpv. c.p.», in ragione della carenza di poteri impeditivi in capo all'*host provider*.

Infatti, in ogni caso, un obbligo di impedimento dell'evento rispetto al fornitore di un servizio quale Google video rappresenterebbe, ad avviso della Corte, una condotta inesigibile (e dunque non penalmente rilevante ai sensi dell'art. 40 cpv. cp.), presupponendo l'esercizio di un controllo pieno ed efficace (una sorta di filtro preventivo) sulla "massa dei video caricati da terzi" in concreto impossibile e dalle conseguenze dirimenti (aggiungo) in punto di tutela del diritto alla libertà di espressione, risolvendosi in una forma di censura o quantomeno di sindacato del provider sulle opinioni diffuse in rete dagli utenti, di dubbia compatibilità con l'art. 21 Cost[10].

D'altro canto- pur ritenendo Google video un *hoster attivo*[11]- da tale qualifica non conseguirebbe comunque, in capo agli imputati, un obbligo di impedimento degli altrui reati, essendo tale obbligo im*possibile* sia *sotto il profilo quantitativo* - per la quantità di materiale caricata in rete- sia *qualitativo*, non potendo un mero dispositivo tecnico di filtraggio procedere a una verifica "se-

---

[9] Cfr., ad es., Cass., IV, sent. N. 32298 del 6.7.2006.

[10] Cfr., in tal senso, quanto dichiarato da Stefano Rodotà nell'intervista *Google, l'allarme di Rodotà: Sentenza non diventi censura*, in *www.repubblica.it* del 25 febbraio 2010: «L'Italia aveva assunto un ruolo di punta nel dibattito internazionale affermando che *internet* non richiede strumenti di tipo penalistico, ma una Costituzione, un "*Internet Bill of Rights*". Nell'ultimo periodo, il governo ha abbandonato questa linea, manifestando iniziative di tipo censorio. Ora questo clima potrebbe essere rafforzato da una lettura sbrigativa della sentenza e anche da un'eventuale motivazione del tribunale che non tenesse conto della natura della rete. Ogni giorno su YouTube o su Facebook vengono introdotti centinaia di migliaia di contenuti, e questo esclude possibilità di controlli preventivi come quelli previsti su stampa, radio e tv».

[11] Ovvero "un *provider* che non si limita a memorizzare le informazioni degli utenti ma svolge invece un'attività «non neutra rispetto all'organizzazione ed alla gestione dei contenuti degli utenti». Si tratta tuttavia, precisa la Corte, di una categoria soggettiva non prevista da alcuna norma di legge, ma fondata "su una constatazione fattuale del ruolo svolto dall'Ip".

mantica e contenutistica" del tipo di dati personali divulgati[12]. Ciò, fermo restando che, come espressamente afferma la Corte, Google Video, in quanto capace di organizzare e selezionare il materiale trasmesso dagli utenti, non può "continuare ad insistere nella sua pretesa neutralità".

In capo agli imputati difetterebbe poi comunque, ad avviso della Corte, il dolo che deve caratterizzare il concorso, nella forma della "coscienza e volontà di concorrere con altri nella realizzazione del reato".

4. Il trattamento illecito di dati personali

a) La sentenza di primo grado

In primo grado, il Tribunale di Milano aveva condannato gli imputati per trattamento illecito di dati personali (art. 167 d.lgs. 196/2003), avendo essi, in concorso, omesso di effettuare gli adempimenti prescritti dalla disciplina in materia di protezione dei dati personali, "consentendo il caricamento del file video incriminato in data 8 settembre 2006 ed il suo mantenimento sul sito Google video.it", con relativo nocumento per il minore e l'Associazione e al fine di trarne profitto mediante il servizio Google video (attraverso gli introiti derivanti dalle inserzioni pubblicitarie ad esso correlate).

In particolare, secondo il giudice di prime cure, la disciplina in materia di protezione dei dati personali "sancirebbe un obbligo non di controllo preventivo dei dati immessi nel sistema, ma di corretta e puntuale informazione, da parte di chi accetti ed apprenda dati provenienti da terzi, ai terzi che questi dati consegnano". Nel caso in esame infatti- afferma il Tribunale - se è ben vero che un hoster attivo (come nel caso Google Italy) ha sicuramente più elementi per poter riconoscere l'esistenza di un reato commesso da un singolo uploader, ed ha, inoltre, sicuramente degli obblighi che la legge gli impone per il trattamento dei dati sensibili dei soggetti che vengono " caricati" sul suo sito web, "è altrettanto vero che non può essere imposto (perché irrealizzabile) allo stesso un obbligo generale e specifico di controllo su tutti i dati " sensibili" caricati (obbligo impossibile, se non altro, perché si imporrebbe ad un terzo la preventiva conoscenza di tutti i dati personali e particolari di tutte le persone che ogni momento "transitano" sul web); quello che è imponibile allo stesso è un obbligo di corretta informazione agli utenti dei conseguenti obblighi agli stessi imposti dalla legge, del necessario rispetto degli stessi, dei rischi che si corrono non ottemperandoli (oltre che, naturalmente, l'obbligo di immediata cancellazione di quei dati e di quelle comunicazioni che risultassero correttamente segnalate come criminose)".

Pertanto, gli imputati avrebbero omesso di ottemperare, tra gli altri, all'obbligo di informativa di cui all'art. 13 d,lgs. 196/2003, non potendo ritenersi a tal fine sufficiente," nascondere le informazioni sugli obblighi derivanti dal

[12] La Corte precisa sul punto che «la valutazione dei fini di un immagine all'interno di un video in grado di qualificare un dato come sensibile o meno, implica un giudizio semantico e variabile che certamente non può essere delegato ad un procedimento informatico».

rispetto della legge sulla privacy all'interno di " condizioni generali di servizio" il cui contenuto appare spesso incomprensibile, sia per il tenore delle stesse che per le modalità con le quali vengono sottoposte all'accettazione dell'utente". Tale inadempimento avrebbe quindi determinato l'integrazione degli estremi del delitto di cui all'art. 167 d.lgs. 196/2003, sebbene la sentenza non si soffermi sull'efficacia causale di tale omissione rispetto alla condotta illecita tenuta dall'inserzionista.

b) La sentenza di appello

In relazione alla contestazione del trattamento illecito di dati personali, la sentenza d'appello rileva una parziale asimmetria tra il capo d'imputazione e le considerazioni del Tribunale, in quanto mentre il primo sottende una "partecipazione attiva" nel reato da parte degli imputati, le seconde "finiscono per ravvisare un concorso costituito da una condotta omissiva", non immaginabile rispetto a un illecito di pura condotta quale quello di cui all'art. 167 d.lgs. 196 cui, come tale, non è applicabile la clausola di equivalenza di cui all'art. 40 cpv. c.p..

Sembrerebbe, in effetti, che il tribunale abbia costruito l'imputazione per trattamento illecito nella forma del concorso omissivo, implicitamente ravvisando una posizione di garanzia nella precedente condotta illegittima (Cass. Sez. IV, n. 32298 del 6.7.2006), per non avere gli imputati adempiuto agli obblighi d'informativa, secondo una ricostruzione che sarebbe stata poi in parte ripresa dal Procuratore generale in sede di appello.

Inoltre, la Corte contesta l'insussistenza, in capo agli imputati, del dolo specifico richiesto dalla norma (nella forma alternativa del profitto per sé o altri o dell'altrui danno), ritenendo che il giudice di prime cure lo abbia in sostanza "confuso" con il mero fine di profitto "costituito dalla palese vocazione economica di Google", non potendosi invece, nel caso di specie, riscontrare alcun vantaggio direttamente conseguito, quale oggetto del dolo sotteso alla condotta in esame. Né potrebbe ritenersi compatibile con il previsto dolo specifico la forma eventuale del dolo, ravvisata in capo agli imputati per aver serbato una "voluta disattenzione" nelle privacy policies aziendali, per fini di massimizzazione del profitto. Infatti, rileva la Corte, la struttura del delitto di cui all'art. 167 d.lgs. 196 presuppone la necessaria "partecipazione psichica intenzionale e diretta del soggetto al raggiungimento di un profitto", non integrata dalla mera accettazione del rischio "concreto di inserimento e divulgazione di dati, anche e soprattutto sensibili, che avrebbero dovuto essere oggetto di particolare tutela; non solo, ma anche dell'interesse economico ricollegabile a tale accettazione del rischio".

In linea generale, tuttavia, la Corte (oltre a sottolineare correttamente l'irrilevanza della violazione dell'obbligo d'informativa ai fini dell'integrazione del delitto di cui all'art. 167 d.lgs. 196, che tale norma non richiama, tra i requisiti di illiceità speciale previsti) contesta che gli imputati fossero tenuti – quali fornitori del servizio Google video – ad adempiere agli obblighi richiamati dal capo d'imputazione e previsti dall'art. 167 d.lgs. 196 quali, in particolare,

l'acquisizione del consenso dell'interessato e l'interpello al Garante per la verifica preliminare. Infatti, "nel caso, toccava all'uploader che, caricando il video, si assumeva la responsabilità del trattamento dei dati personali dell'interessato, chiedere e ottenere il consenso prescritto".

E' questo, effettivamente, il punto dirimente della sentenza, che consente di escludere già sul piano oggettivo la sussistenza del delitto di cui all'art. 167 d.lgs. 196, per la cui integrazione è necessario procedere al trattamento di dati in violazione di taluni adempimenti prescritti dallo stesso codice in materia di protezione dei dati personali. Ebbene, tra le norme richiamate dall'art. 167 quali parametri normativi dei previsti requisiti di illiceità speciale, quelle contestate agli imputati nel capo d'imputazione non prevedono adempimenti cui nella specie poteva ritenersi tenuta Google video, spettando invece agli inserzionisti i quali, sotto la propria diretta responsabilità (anche penale), hanno caricato il video in questione in rete. Erano dunque, nella specie, gli uploaders i soggetti tenuti a richiedere il consenso dell'interessato (da prestarsi in forma scritta perché inerente dati sensibili) ed, eventualmente, a effettuare l'interpello al Garante ai sensi dell'art. 17.

Adempimenti di questo tipo – che presuppongono oltretutto la consapevolezza della natura sensibile dei dati trattati - non potrebbero imputarsi al fornitore di un servizio quale Google video che, per quanto configurabile – come afferma la Corte - quale *hoster attivo* non può comunque ritenersi, secondo la Corte, autonomo titolare dei dati personali dei soggetti protagonisti del video e come tale tenuto agli obblighi di cui agli artt. 17, 23 e 26 d.lgs. 196. Soprattutto perché, a prescindere dalla configurabilità del provider (sia pure nella forma dell'hosting attivo) come titolare autonomo o meno del trattamento dei dati dei protagonisti del video, egli è comunque estraneo al contenuto del video stesso, la conoscenza del quale è invece necessaria anche per poter configurare in capo al fornitore un obbligo di intervento e specifici adempimenti -quali quelli di cui agli artt. 26 e 17 d.lgs. 196 – diversamente modulati in ragione del tipo di dato trattato.

Secondo la Corte, infatti, «la responsabilità per il trattamento dei dati è legata al mancato adempimento di specifiche condizioni che rendono lecito l'uso di tali dati, ma tali condizioni non possono che essere messe in capo al titolare, al "*controller*" dei dati medesimi. In effetti trattare un video, acquisirlo, memorizzarlo, cancellarlo, non può significare di per sé trattamento di dati sensibili. Esistono due distinte modalità di trattare dei dati che non possono essere, a parere di questa Corte, considerati in modo unitario». In particolare, osserva ancora la Corte, «trattare un video non può significare trattare il singolo dato contenuto, conferendo ad esso finalità autonome con quelle perseguite da chi quel video realizzava. Sarà il titolare del trattamento ad avere l'obbligo di acquisire il consenso al trattamento dei dati personali» e dunque l'uploader e non già Google video, la cui estraneità rispetto ai contenuti del video ospitato emerge anche, secondo la Corte, dalla disciplina di cui agli articoli 16 e 17 del d.lgs. 70/2003, alla cui stregua il prestatore non è responsabile delle informazioni memorizzate a

condizione che non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e che, non appena a conoscenza di ciò, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

5. Né censura né anomia. Prospettive di riforma (per una rete libera, ma attenta ai diritti)

Sono probabilmente quegli obblighi di attivazione analoghi a quelli di cui all'art. 17 d.lgs. 70/2003 gli elementi su cui è necessario fondare, anche in prospettiva di riforma, una disciplina a tutela dei diritti fondamentali in rete, che contemperi i vari interessi in gioco e in particolare i diritti alla dignità e alla protezione dei dati personali da un lato e, dall'altro, la libertà di espressione e la segretezza delle comunicazioni. Il bilanciamento tra questi diritti fondamentali dev'essere, ovviamente, tracciato dal legislatore e non può certamente essere rimesso non solo alla discrezionalità di soggetti privati, quali i provider, non tenuti a conoscere e sindacare il contenuto dei dati divulgati. Come ben rileva la sentenza in commento, infatti, "demandare ad un *internet provider* un dovere/potere di verifica preventiva, appare una scelta da valutare con particolare attenzione in quanto non scevra da rischi, poiché potrebbe finire per collidere contro forme di libera manifestazione del pensiero».

Ma un così delicato bilanciamento tra diritti fondamentali non può essere delegato neppure, integralmente, alla tecnica, attribuendo a sistemi di filtraggio automatico dei dati trasmessi il potere di inibirne la divulgazione. Infatti, se simili sistemi possono - come ad esempio previsto in materia di pedopornografia[13] - inibire l'accesso a *siti* previamente segnalati dall'autorità competente e, per l'effetto, bloccare la divulgazione di dati che, per la loro stessa struttura estrinseca, si presentano illeciti, essi non possono invece compiere un'autonoma valutazione in ordine alla legittimità o meno *del contenuto* delle informazioni in questione.

Tuttavia, per evitare che la rete divenga appunto – come osservava il giudice di prime cure – la «"sconfinata prateria " dove tutto è permesso e niente può essere vietato», uno spazio anomico in cui gli stessi diritti fondamentali siano impunemente violati (anziché promossi), è necessario prevedere – adeguatamente bilanciando i vari interessi in gioco- specifici obblighi di attivazione del provider. Il quale, informato dell'illiceità dei contenuti trasmessi e su richiesta dell'interessato o dell'autorità giudiziaria, sia tenuto a rimuovere le informazio-

[13] Cfr., in particolare, art. 14-quater l. 1998, n. 269 e successive modificazioni e il d.M. 8 gennaio 2007 (c.d. decreto Gentiloni) recante "Requisiti tecnici degli strumenti di filtraggio che i fornitori di connettività alla rete Internet devono utilizzare, al fine di impedire, con le modalità previste dalle leggi vigenti, l'accesso ai siti segnalati dal Centro nazionale per il contrasto alla pedopornografia", emanato in attuazione di tale disposizione. L'inadempimento, da parte dei fornitori di "servizi resi attraverso la rete", agli obblighi previsti dagli artt. 14-ter e quater della legge integra, di per sé, gli estremi di specifici illeciti amministrativi, salvo, ovviamente, che il fatto costituisca reato.

ni contestate, pena un suo concorso nel reato sottostante, indubbi essendo, a questo punto, non solo il contributo agevolativo fornito sul piano soggettivo, ma anche la consapevolezza del carattere illecito dell'altrui condotta favorita. Si tratterebbe, in linea generale, di immaginare un sistema di notice and take down con adeguate garanzie procedimentali per assicurare agli interessati il necessario contraddittorio e il rispetto del diritto di difesa, prevedendo un intervento (anche solo in funzione consultiva) del Garante per la protezione dei dati personali, così da evitare azioni di tipo meramente censorio da parte dei provider. Si consideri del resto che simile modello si conformerebbe a quanto affermato, già de jure condito, dalla Corte di giustizia, secondo cui un intermediario deve essere considerato responsabile degli illeciti commessi in rete qualora abbia contezza di attività o informazioni illecite sia a seguito di esami effettuati di propria iniziativa, sia a seguito di notificazione (sentenza 12.7.2011 della Grande Sezione, causa C-324/09, L'Oréal c. E-bay). Ancora, la Corte, con sentenza del 23.3.2010, ha precisato che l'art. 14 della direttiva 2000/31/Ce si applica al prestatore "di un servizio di posizionamento su internet qualora detto prestatore non abbia svolto un ruolo attivo atto a conferirgli la conoscenza o il controllo dei dati memorizzati. Se non ha svolto un siffatto ruolo, detto prestatore non può essere ritenuto responsabile per i dati che egli ha memorizzato su richiesta di un inserzionista, salvo che, essendo venuto a conoscenza della natura illecita di tali dati o attività di tale inserzionista, egli abbia omesso di prontamente rimuovere tali dati o disabilitare l'accesso agli stessi".

Come già rilevato in altra sede[14], sarebbe auspicabile prevedere allora una fattispecie contravvenzionale, punita con sanzioni interdittive congiuntamente a pene pecuniarie, sostenuta dal dolo diretto, per le ipotesi di omesso impedimento, da parte del provider (che non si limiti, tuttavia, alla mera fornitura di accesso alla rete), della trasmissione di dati del cui carattere illecito abbia consapevolezza, e in presenza del requisito della tecnica possibilità ed esigibilità della misura impeditiva. Sarebbe poi opportuno introdurre una clausola di non punibilità per i providers i quali abbiano adottato sistemi di controllo - da prevedersi in via legislativa - od, al più, regolamentare, sulla base, tuttavia, di principi e criteri direttivi sufficientemente precisi, stabiliti dalla fonte primaria - idonei ad impedire la diffusione di informazioni illecite. Tale soluzione, che in parte si modella sulla disciplina dei *compliance programs*, di cui al d.lgs. n. 231 del 2001, ben si attaglierebbe, peraltro, alle ipotesi di responsabilità delle imprese- providers, i cui amministratori, ad esempio, commettano reati per avvantaggiare la società ed essa non si sia premunita con l'adozione dei suddetti modelli «anticrimine».

Interessante, in tale senso, è in particolare quanto previsto dalla p.d.l. AC 3818 (XVI legislatura), che, nel novellare il d.lgs. 196/2003, sancisce, in capo a chiunque vanti un interesse alla rimozione o al blocco di dati divulgati illecitamente, il diritto a presentare un'apposita istanza di oscuramento, rimozione, rettificazione, aggiornamento, integrazione o blocco degli stessi dati pubblicati, da

[14] F. RESTA, *La responsabilità, etc., cit.*

rivolgersi direttamente all'utente che abbia divulgato i dati in questione. Qualora egli non sia identificabile o comunque non intenda adempiere, l'interessato potrà rivolgere analoga istanza al Garante per la protezione dei dati personali, il quale – nell'esercizio di un ruolo quasi da ombudsman – si pronuncerà in ordine alla fondatezza o meno della richiesta, trasmettendo il relativo parere ai fornitori di servizi di comunicazione e di informazione offerti mediante reti di comunicazione elettronica, responsabili per il trattamento dei dati video, audio, fotografici e testuali diffusi. Essi saranno quindi tenuti, secondo la p.d.l, a valutare- assumendosene le relative responsabilità - se aderire all'istanza. In caso di rigetto dell'istanza e qualora dalla (persistente) divulgazione dei dati illegittimamente trattati derivi nocumento, i fornitori, così informati, risponderanno penalmente, in base a quanto previsto dall'art. 167-bis (*Diffusione di dati illeciti)*, che la proposta inserisce nel d.lgs. 196/2003. Ad analoga responsabilità penale si esporrà il fornitore, per non aver oscurato o rimosso – dietro apposita istanza dei genitori - i dati del minore il quale abbia registrato mediante falsa dichiarazione di maggiore età i propri dati personali su un sito *web*, sempre che dal fatto derivi nocumento.

Si tratta, in sintesi, di un sistema che – pur ovviamente perfettibile e anche, in alcuni aspetti, diversamente immaginabile – mira a responsabilizzare i provider non imponendo loro un obbligo di preventivo e generale controllo dei contenuti divulgati in rete, ma un onere di attivazione di dati illecitamente raccolti o illecitamente diffusi, in presenza di apposita istanza.

Si consideri del resto che quello della previsione di obblighi di rimozione, su segnalazione, di contenuti illegittimi, è modello in linea generale non dissimile da quanto previsto dall'art. 17 del draft di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (COM(2012)11), attualmente all'esame del Parlamento europeo e destinato a sostituire la direttiva 95/46/CE. Tale norma, al fine di "rafforzare il diritto all'oblio nell'ambiente online" (cons. 54) sancisce appunto, in capo al "responsabile del trattamento"[15] - il quale, avendo pubblicato dati personali altrui, abbia ricevuto dall'interessato espressa richiesta di cancellazione- un duplice dovere di attivazione. Dovere consistente da un lato nella rimozione, senza ritardo, delle informazioni in questione (salvo vi ostino ragioni di tutela del diritto alla libertà di espressione; mo-

[15] Nozione, questa, definita come corrispondente al "la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, singolarmente o insieme ad altri, determina le finalità, le condizioni e i mezzi del trattamento di dati personali; quando le finalità, le condizioni e i mezzi del trattamento sono determinati dal diritto dell'Unione o dal diritto di uno Stato membro, il responsabile del trattamento o i criteri specifici applicabili alla sua nomina possono essere designati dal diritto dell'Unione o dal diritto dello Stato membro". Si tratta dunque – come già nel contesto della direttiva 95/46- di un soggetto corrispondente più alla figura del "titolare" del trattamento di cui all'art. 4, comma 1, lett.f) del d.lgs. 196/2003 che non a quella del responsabile di cui all'art. 29 dello stesso d.lgs. 196.

tivi di interesse pubblico nel settore della sanità pubblica; finalità storiche, statistiche e di ricerca scientifica; esigenze di adempimento a specifici obblighi legali di conservazione dei dati) e, dall'altro, nell'informazione dei terzi che stiano trattando tali dati della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei propri dati personali. Fermo restando che, qualora abbia autorizzato un terzo a pubblicare dati personali, il responsabile del trattamento sarà ritenuto responsabile di tale pubblicazione.