

## GIURISPRUDENZA

## APPELLO MILANO

27 FEBBRAIO 2013

PRESIDENTE: MALACARNE

ESTENSORE: MILANESI

**Diffamazione tramite Internet • Responsabilità del provider • Condizioni • Fattispecie • Esclusione • Obbligo normativamente previsto di controllo preventivo sui contenuti dei siti web • Esclusione**

*Il gestore o il proprietario di un sito web qualificabile come content provider non può essere ritenuto corresponsabile del rea-*

*to di diffamazione derivante dal contenuto di materiale caricato da terzi in mancanza di una previsione normativa che imponga il controllo preventivo di tutti i dati che transitano sui siti web. 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 la concreta possibilità di effettuare un controllo preventivo.*

**C**on la sentenza n. 1972/2010 emessa dal Tribunale di Milano in composizione monocratica, all'esito di giudizio abbreviato, in data 24 febbraio 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 cod. pen. nei termini di seguito indicati: perché in concorso tra loro D.D.C. - Presidente del Consiglio di Amministrazione di Google Italy s.r.l. dal 19 marzo 2004 e successivamente nominato amministratore delegato in data 2 aprile 2004 (fino al 21 maggio 2007), F.P.A. - Responsabile delle policy sulla privacy per l'Europa (Global Privacy Counse) di Google Inc., D.L.R.G. - membro del Consiglio di Amministrazione di Google Italy s.r.l. e successivamente nominato amministratore delegato in data 2 aprile 2004 (fino al 21 maggio 2007), D.A. - Responsabile del progetto Google 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, Google.it](http://video.google.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 addosso 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 7 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.Lgs. 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 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 omissso nell'ipotesi di cui al presente procedimento, non attivandosi Google Italy srl neppure in tal senso, tramite il prescritto interpellò, presso l'Autorità Garante. Trattamento omissso — anche in relazione alla concrete misure organizzative da apprestare, idonee alla sua successiva attuazione — fin dalla fase antecedente alla effettiva localizzazione del 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 un'attenta analisi del mercato italiano (confluita nel documento Google Video: «Preliminary analysis of italian market peculiarities» — redatto su indicazione di DESIKAN Arvind, dal personale di Google Italy s.r.l. assegnato al progetto Google 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.Lgs. 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 Google Video (in relazione al quale Google Italy s.r.l. beneficia degli indotti pubblicitari degli inserzionisti), procedevano al trattamento di dati personali in violazione agli artt. 23, 17 e 26 stesso D.Lgs. con relativo documento per la persona interessata (D.L.F.G.). E pertanto gli stessi venivano condannati, con le attenuanti generiche e la diminuzione 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.Lgs. 30 giugno 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 9 novembre 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.google.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 minchia 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 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.

Il padre del minore si doleva in particolare, della totale assenza di controllo da parte del Provider, nella specie Google 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 maggio 2006.

— Il medesimo video veniva caricato su Google Video tra T08/09/2006 ed il 10 settembre 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 5 novembre 2006 il blogger D.A. segnalava sul suo blog « Giornalettismo militante - Il Cannocchiale.it » la presenza del video sul sito.

— In data 6 novembre 2006 tale BARADINO Silvia chiedeva la rimozione del video tramite il centro di assistenza Google.

— In data 7 novembre 2006 la Polizia Postale di Roma richiedeva la rimozione del video.

— In data 7 novembre 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 Google 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 Google 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 Google Italy s.r.l. a proposito del servizio Google Video da lanciare sul territorio dello Stato.

In sintesi risultava che Google 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 Google 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 aprile 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 Google France, in Google UK, in Google Ireland, società tutte riferibili a Google Inc.

Per quanto riguarda il ruolo di A.D. lo stesso dalla documentazione reperita presso la sede di Google Italy e dalle dichiarazioni dei dipendenti italiani coinvolti nel progetto, emergeva essere il responsabile del progetto Google Video per l'Europa: proprio quest'ultimo imputato in una mail inviata a V.P. in data 13 novembre 2006, 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 Google 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 Google. Secondo la tesi accusatoria questo meccanismo era previsto anche in relazione al servizio Google 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 settembre 2009, escludeva però nel modo più assoluto che al tempo dei fatti fosse possibile inserire pubblicità su Google Video. Il medesimo teste inoltre dichiarava che inizialmente i controlli venivano svolti negli Stati Uniti, in seguito quando Google 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 Google, di cui Google Video può essere considerata una parte, può ritenersi espressione di una mera intermediazione, un mero User Guaranteed 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 Google 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 febbraio 2009 veniva depositata dichiarazione di remissione di querela da parte 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 cod. proc. pen., 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 costitutivi 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 febbraio 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 aprile 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.Lgs. 30 giugno 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 rispettiva 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 Google 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 Google Video comportavano necessariamente un trattamento degli stessi e quindi escludevano la possibilità di considerare Google Italy o comunque Google 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 Google 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 Google Inc.;

— Google Italy esercitando unicamente una attività di marketing a favore di Google Inc. non aveva alcun potere né alcuna possibilità di trattare i dati riferibili a quest'ultima.

— Andava escluso che ci fosse un collegamento Google Video - ADwords.

— Google 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 Google Video fornito una completa informativa agli utenti in merito al trattamento dati.

— Non esisteva alcun fine di profitto da parte di Google Italy essendo Google 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.Lgs. 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.Lgs. 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.Lgs. 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 Google 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 oltretutto 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 Google 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 là di ogni ragionevole dubbio, i seguenti elementi probatori.

— Google Italy costituiva la mano operativa e commerciale di Google Inc. in Italia.

— Attraverso Adwords, Google Italy era in grado di collegare i clienti con i video immessi in rete da Google Video, e quindi in definitiva di trattare i dati contenuti in quest'ultimo sito.

— Google Italy di conseguenza era responsabile rispetto alla normativa sulla privacy dei dati contenuti nei video caricati sulla piattaforma di Google Video.

— In Google 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 differente, 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 Google 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 malam 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 cod. pen. 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 giugno 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 cod. pen. 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.Lgs. 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 Google 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 D.Lgs. 30 giugno 2003 numero 196 ed in particolare:

— dall'art. 13 difettando del tutto l'informativa sulla privacy, (visualizzabile dalla pagina iniziale di Google 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 omoesso nell'ipotesi di cui al presente procedimento.

La *ratio* dell'introduzione nei sistemi penali moderni di norme come quelle di cui all'articolo 40 cod. pen., atte ad incriminare ipotesi di reato commissivo mediante omissione deve ricercarsi nella necessità di soddisfare esigenze di 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 effettuati da persone.

Va ricordato che veniva accertato che il servizio Google 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 al 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 (D.Lgs. 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 riconoscimento testuale nell'art. 1 comma 2 lettera *a*) D.Lgs. 70/2003, disposizione in linea con l'art. 1 comma 4 lettera *b*) della Direttiva 200/31/CE.

In effetti il servizio Google 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 200/31/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 conseguenziale 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 cod. proc. pen. 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 cod. pen. 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 Google Video veniva effettuato anche da Google Italy.

— La sentenza riteneva erroneamente che Google Italy attraverso il sistema AdWords avesse la possibilità di gestire i dati contenuti in Google 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.Lgs. 196/2003.

La sentenza affermava la penale responsabilità dell'imputato sulla base di presupposti erronei.

La sentenza erroneamente riteneva applicabile il codice privacy a Google Video ravvisando la giurisdizione italiana D.D.C. doveva essere ritenuto non punibile per mancanza dei presupposti *ex art.* 10 cod. pen.

La sentenza deve essere dichiarata nulla *ex artt.* 521 comma 2, 522 e 604 comma 1 cod. proc. pen. 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 cod. pen. 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: insussistenza in fatto e irrilevanza penale in diritto.

— I due trattamenti (Google Inc. — utente; utente — interessato)

— Google Inc. ha correttamente informato l'utente.

— Era l'utente che doveva acquisire il consenso dall'interessato.

2) Google Italy non trattava e non poteva trattare i dati del servizio Google Video e non ha effettuato alcun trattamento dei dati del D.L..

— Distinzione tra Google Italy srl e Google Inc.

— Google Italy non ha contribuito alla predisposizione della piattaforma informatica di Google Video.

— Google Italy e l'impossibilità tecnica di qualsiasi operazione di trattamento dati relativa al servizio Google Video.

3) Google Video era un servizio gratuito e non comportava profitto per Google Italy.

— Non era possibile inserire annunci del servizio AdWords sul servizio Google Video.

— Non vi era interazione commerciale operativa tra Google Video e Google Italy tramite il servizio AdWords.

— Google Italy non traeva alcun profitto dal servizio Google Video.

Il difensore dell'imputato FLEISHER Peter Andrei 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.Lgs. 196/2003.

— Il D.Lgs. 70/2003

— Il D.Lgs. 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'inconfigurabilità del reato di illecito trattamento in capo a Google Italy.

— AdWords.

— Il gruppo Google.

— I link tra Google Italy e Google 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 Google.

— In diritto: concorso omissivo nell'omesso trattamento.

4) In subordine riconoscere le già concesse attenuanti 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 cod. pen. e con riconoscimento del beneficio della non menzione della condanna nel certificato del casellario giudiziale ex art. 175 cod. pen.

5. IL PROCESSO D'APPELLO. — A seguito di emissione di decreto di citazione per l'udienza del 4 dicembre 2012 avanti la Corte venivano depositate memorie difensive.

In data 16 novembre 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.Lgs. 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 dovevano i 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 novembre 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 audio-video 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 Google Video.

All'udienza del 4 dicembre 2012, formalizzata la costituzione delle Parti dopo la relazione introduttiva venivano fissate per la discussione le udienze dell'11 e del 21 dicembre 2012.

In data 13 dicembre 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.Lgs., 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 interpellato 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.Lgs. 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.Lgs. 171/98.

Gli appelli degli imputati sostengono che Google 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 Google come semplice internet provider sembrerebbe fatta propria dalla sentenza di primo grado ma, questa definizione è sbagliata perché Google non è un semplice host provider in ragione dei numerosi servizi aggiuntivi offerti, per esempio le miniature e i sistemi di raffinazione della ricerca. Google 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 Google Video era fonte di guadagno per Google quindi la finalità di lucro di cui all'art. 167 D.Lgs. cit. è sussistente ed è provata dai documenti sequestrati nella sede di Google 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 con-

ferma, in quanto dall'istruttoria svolta e dai documenti rinvenuti nella sede originaria, Google Italy è stata costituita il 22 agosto 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 Google Italy era un mera esecutrice delle decisioni prese dalla casa madre Google Inc., ed è assolutamente contrario al materiale probatorio acquisito sostenere un'autonomia di Google Italy o di Google Video.

Al termine il P.G. si riportava alle conclusioni già prese in sede di requisitoria finale in data 11 dicembre 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 dicembre 2012 i difensori degli appellanti sottoponevano all'attenzione della Corte memoria *ex art.* 121 cod. proc. pen.

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 Google e nel caso di Google 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 Google 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 Google 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 Google 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 Google 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, Google Italy Srl, e segnatamente i suoi amministratori che non svolgevano ruoli esecutivi e che non avevano relazioni con il servizio Google Video.

In nessun caso infatti Google Italy poteva dirsi coinvolta nell'attività dei trattamenti dei dati relativi al servizio Google 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 Google 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 dicembre 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 giugno 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 luglio 2010, la residua parte civile costituita dall'Associazione Vivi Down, provvedeva a rimettere la querela sporta in data 9 novembre 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 dicembre 2012, 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 57-bis cod. pen. 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 cod. pen.

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 cod. pen., 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 6 luglio 2006).

Occorre sottolineare però, che neppure sotto questo profilo la tesi accusatoria, secondo cui in sostanza la responsabilità degli imputati derive-

rebbe 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 7 luglio 2010, la residua Parte Civile, Associazione Vivi Down, abbia rimesso la querela sporta in data 9 novembre 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 dalle 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 cod. proc. pen., essendo stato il reato in questione commesso almeno in parte nel nostro Paese, a Milano, dove ha sede Google Italy responsabile del comporta-

mento incriminato e cioè del trattamento dei dati inteso come elaborazione ed organizzazione dei video caricati in Google 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 al luogo in cui si sono verificati gli effetti pregiudizievoli dell'illecito.

Vedi art. 5.3 della Convenzione di Bruxelles del 27 settembre 1968 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. 15-16 dicembre 2009 - Cass. Sez. III n. 49437/09 del 29 settembre 2009).

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 9 luglio 2008-20 ottobre 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 novembre 2000-27 dicembre 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 cod. proc. pen. del PM e riportate nella sentenza di primo grado.

Secondo le stesse, D. risultava essere Vicepresidente e Legale rappresentante di Google Inc., nonché Vicepresidente di Google International, ovvero il vertice proprio delle due società detentrici delle complessive quote sociali di Google Italy srl, società costituita a Milano il 27 agosto 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 Google Italy e Google Video, stabilito nel territorio dello Stato.

A partire dal 2006 il servizio Google Video veniva localizzato in Europa e poi in Italia a partire dal 12 luglio 2006.

Essendo A. il responsabile del progetto Google Video per tutta l'Europa con gestione rispetto all'Italia a cura di Google Italy srl.

Occorre a questo punto solo sottolineare che essendo Google Italy srl soggetto giuridico stabilito nel territorio dello 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, ri-

mane comunque applicabile l'articolo 5 comma 2 D.Lgs. 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 Google Italy in relazione ai dati immessi nel sistema di Google Video, la nozione di trattamento prevista dall'art. 4 del medesimo D.Lgs.

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 Google si trovi negli Stati Uniti, Google ha l'obbligo legale di attenersi alle leggi europee, ed in particolare alle normative sulla privacy, dato che i servizi di Google 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 Google 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.Lgs. 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 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 constatazione fattuale del ruolo svolto dall'Ip, è 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 Google Video non possa che essere qualificata quantomeno come un hosting attivo.

In effetti va escluso che Google 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.Lgs., 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 cod. proc. pen.

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.Lgs. 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 pri-

vacy, 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 nocimento 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 Google.

Cfr. in senso conforme Cass. Pen. Sez. 3 17 novembre 2004-15 febbraio 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 Google 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'8 giugno 2000, addirittura vieta, tenendo a mente l'art. 15 del D.Lgs. 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 ».

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 cod. pen. 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 cod. pen. 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 Google (Cfr. in senso conforme Cas. III Sez. n. 1464/12 del 24 maggio 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 Google 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 marzo 2008 in Cass. Pen. 2008 n. 12. e Cass. Sez. IV 18 settembre 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 ottobre 1994 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 cod. proc. pen. in parziale.

Riforma della sentenza emessa dal Tribunale di Milano del 24 febbraio 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.

## LIBERTÀ DELLA RETE E PROTEZIONE DEI DATI PERSONALI: ANCORA SUL CASO GOOGLE-VIVI DOWN<sup>1</sup>

Tribunale di Milano, con sentenza n. 1972 del 12 aprile 2010<sup>3</sup>.

### 1. PREMessa.

**C**on la sentenza in epigrafe<sup>2</sup> 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

<sup>1</sup> Le opinioni contenute in questo contributo sono espresse a titolo personale e non impegnano in alcun modo l'Istituzione di appartenenza.

<sup>2</sup> Su cui vds. G. CASSANO, *Google - Vividown. Assoluzione in Appello e ... « tanto rumore per nulla »*, in corso di pubblicazione su *Diritto e giustizia*.

<sup>3</sup> 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 inter-*



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 adempimenti prescritti dalla disciplina in materia di protezione dei dati personali<sup>4</sup>, con relativo nocumento per il minore e al fine di trarne profitto mediante il servizio Google video.

## 2. GIURISDIZIONE E COMPETENZA.

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<sup>5</sup>. 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 pre-

net 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 cyberspazio: cittadino, controllore o tutore dell'ordine? Risposte attuali e scenari futuri 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.*, ma per una prospettiva più ampia, v., in particolare, S. RONDÀ, *Il diritto di avere diritti*, Roma-Bari, 2013, 378 ss.

<sup>4</sup> 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); interpellò al Garante per la verifica preliminare del trattamento che presenta rischi specifici (art. 17 D.Lgs. 196).

<sup>5</sup> Come affermato, in relazione alla diffamazione on-line, ad es., da *Cass.*, Sez. II, Sent. n. 36721 del 21 febbraio 2008 (ud. del 21 febbraio 2008), B.M.I. (rv. 242085); *Cass.*, Sez. V, sent. n. 4741 del 27 dicembre 2000 (cc. del 17 novembre 2000), (rv. 217745).

giudizievoli 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 cod. proc. pen., 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.

È 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 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 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 cod. pen.) nel reato di diffamazione per avere, in sostanza, omissso 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 dicembre 2009), in materia di responsabilità penale degli internet service provider per le violazioni della disciplina sul diritto d'autore commesse in rete<sup>6</sup>. In tale pronuncia, si ammette tra l'altro la

<sup>6</sup> Su tema analogo cfr. anche Corte di giustizia, Grande Sezione, sent. 29 gennaio

2008, Promusicae (C-275/06), secondo cui « La direttiva del Parlamento europeo e

possibilità 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

del Consiglio 8 giugno 2000, 2000/31/CE, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("direttiva sul commercio elettronico"), la direttiva del Parlamento europeo e del Consiglio 22 maggio 2001, 2001/29/CE, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, la direttiva del Parlamento europeo e del Consiglio 29 aprile 2004, 2004/48/CE, sul rispetto dei diritti di proprietà intellettuale, e la direttiva del Parlamento europeo e del Consiglio 12 luglio 2002, 2002/58/CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), non impongono agli Stati membri, in una situazione come quella oggetto della causa principale, di istituire un obbligo di comunicare dati personali per garantire l'effettiva tutela del diritto d'autore nel contesto di un procedimento civile. Tuttavia, il diritto comunitario richiede che i detti Stati, in occasione della trasposizione di tali direttive, abbiano cura di fondarsi su un'interpretazione delle medesime tale da garantire un giusto equilibrio tra i diversi diritti fondamentali tutelati dall'ordinamento giuridico comunitario. Inoltre, in sede di attuazione delle misure di recepimento delle dette direttive, le autorità e i giudici degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme a tali direttive, ma anche evitare di fondarsi su un'interpretazione di esse che entri in conflitto con i detti diritti fondamentali o con gli altri principi generali del diritto comunitario, come, ad esempio, il principio di proporzionalità». Ancora, sul tema del rapporto tra diritto d'autore e protezione dati, cfr. Corte di giustizia, Terza Sezione, sent. 24 novembre 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 luglio 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, se-

transfert e tali dunque da realizzare un apporto causale all'altrui condotta illecita, penalmente rilevante ex art. 110 cod. pen.

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, gestendo 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, integrebbene 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. cod. pen. »

condo 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 intel-

lettuale e, dall'altro, la libertà di impresa, il diritto alla tutela dei dati personali e la libertà di ricevere o di comunicare informazioni.

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.

a) *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 omisivo, 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<sup>7</sup>.

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 cod. pen.<sup>8</sup>, 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.

<sup>7</sup> Sulla linea, dunque, di quanto già affermato dal Tribunale di Milano con la sentenza del 18 marzo 2004, in *Giur. mer.*, 2004, 1719, con nota di F. RESTA, *La responsabilità penale del provider: tra laissez 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 connessi da coloro che utilizzano i lo-

ro 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 ».

<sup>8</sup> Per l'affermazione secondo cui, *de jure condito*, il dettato dell'art. 57 cod. pen. non si applica al direttore di un quotidiano *on line*, cfr., in particolare, Cass., sez. V, sent. n. 35511 del 16 luglio 2010.

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 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<sup>9</sup> — 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. cod. pen. », 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. cod. pen.), 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.<sup>10</sup>.

D'altro canto — pur ritenendo *Google video* un *hoster attivo*<sup>11</sup> — da tale qualifica non conseguirebbe comunque, in capo agli imputati, un obbligo di impedimento degli altrui reati, essendo tale obbligo *impossibile* 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 « semantica e contenutistica » del tipo di dati per-

<sup>9</sup> Cfr., ad es., Cass., IV, sent. n. 32298 del 6 luglio 2006.

<sup>10</sup> 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 mo-

tivazione 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 ».

<sup>11</sup> 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".

sonali divulgati<sup>12</sup>. 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 documento 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 po-

<sup>12</sup> 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 ».

tendo ritenersi a tal fine sufficiente, « nascondere le informazioni sugli obblighi derivanti dal rispetto della legge sulla privacy all'interno di "condizioni generali di servizio" il cui contenuto appare spesso incomprendibile, 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 sostiene 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. cod. pen.

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 luglio 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'irrelevanza 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'interes-



sato 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 ».

È 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. 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<sup>13</sup> — 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 informazioni 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 procedurali 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

<sup>13</sup> 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.

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 luglio 2011 della Grande Sezione, causa C-324/09, L'Oréal c. E-bay). Ancora, la Corte, con sentenza del 23 marzo 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<sup>14</sup>, 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 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

<sup>14</sup> F. RESTA, *La responsabilità, etc.*, cit.

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 on-line » (cons. 54) sancisce appunto, in capo al « responsabile del trattamento »<sup>15</sup> — 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; motivi 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.

FEDERICA RESTA

<sup>15</sup> 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 tratta-

mento 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.