GIURISPRUDENZA

CASSAZIONE
SEZIONE III PENALE
3 FEBBRAIO 2014
N. 5107

PRESIDENTE: MANNINO
RELATORE: ANDRONIO

Diffamazione tramite Internet
• Trattamento dei dati personali. Responsabilità del provider
• Condizioni
• Fattispecie
• Esclusione. Obbligo normativamente previsto di controllo preventivo sui contenuti dei siti web
• Obbligo di informare il terzo che immette dati delle prescrizioni normative a tutela della privacy
• Esclusione

Il gestore o il proprietario di un sito web qualificabile come content provider non può essere ritenuto corresponsabile del reato di illecito trattamento dei dati personali 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.

RITENUTO IN FATTO. — 1. Con sentenza del 24 febbraio 2010, il Tribunale di Milano ha — per quanto qui rileva — ritenuto gli imputati D.D.C., F.P.A., D.L.R.G. responsabili del reato loro contestato al capo B dell'imputazione, relativo alla violazione dell'art. 110 cod. pen. e del D.Lgs. n. 196 del 2003, art. 167, commi 1 e 2, perché, in concorso tra loro e nelle loro rispettive qualità (D., di amministratore delegato di Google Italy s.r.l.; F., di responsabile della policy sulla privacy di Google Inc.; D.L.R., di amministratore delegato di Google Italy s.r.l.) procedevano al trattamento dei dati personali in violazione dello stesso D.Lgs. n. 196 del 2003, artt. 23, 17 e 26, con riferimento a un video immesso per la successiva diffusione a mezzo Internet sul sito www.video.google.it, raffigurante un soggetto affetto da sindrome di Down che viene preso in giro con frasi offensive e azioni vessatorie riferite alla sua sindrome da parte di altri soggetti minorenni.

La condotta contestata consiste, in particolare, nell'avere omesso un'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 di files, in ordine a quanto prescritto dal comma 1 del richiamato art. 13 e, per esso, del valido consenso di cui all'art. 23, comma 3. La violazione ipotizzata investe anche l'art. 26 richiamato, riguardando dati idonei a rivelare lo stato di salute della persona inquadrata nel video, e l'art. 17 anch'esso richiamato, per i rischi specifici insiti nel tipo di trattamento omesso, anche in relazione alle concrete misure organizzative da prestare.

2. Con sentenza del 21 dicembre 2012, la Corte d'appello di Milano ha

riformato, per la parte che qui rileva, la sentenza impugnata, evidenziando che il D.Lgs. n. 196 del 2003, art. 167 non richiama il precedente art. 13 e, dunque, non impone all'Internet provider di rendere edotto l'utente circa l'esistenza e i contenuti della legislazione sulla privacy. Infatti, l'eventuale violazione del citato art. 13, consistente nell'omessa o inidonea informativa all'interessato, viene punita non dall'art. 167, bensì dal precedente art. 161, che prevede una sanzione amministrativa. Nella stessa sentenza si esclude, inoltre, la configurabilità di un concorso omissivo nel reato contestato. Si esclude, altresì, la sussistenza del dolo specifico richiesto dalla disposizione incriminatrice, sul rilievo che gli imputati non erano preventivamente a conoscenza del filmato e dell'immissione del dato personale illecitamente trattato e sull'ulteriore rilievo della incompatibilità giuridica di detto dolo specifico col dolo eventuale individuato dal Tribunale in capo agli imputati.

3. Quest'ultima sentenza è stata impugnata, con ricorso per cassazione, dal Procuratore generale della Repubblica presso la Corte d'appello di Milano.

3.1. Si rileva, in primo luogo, l'erronea applicazione del D.Lgs. n. 196 del 2003, art. 26, perché la Corte distrettuale non avrebbe fatto conseguire, al dato pacifico delle pesanti allusioni allo stato di salute del soggetto rappresentato nel video in questione, la superfluità di ogni successiva valutazione in ordine alle caratteristiche del consenso prestato dai ragazzi che avevano fornito il video. Non si sarebbe, in particolare, considerato che, per i dati idonei a rivelare lo stato di salute, vige un divieto assoluto di loro diffusione anche in presenza del consenso dell'interessato, ai sensi del D.Lgs. n. 196 del 2003, art. 26, comma 5. Non si sarebbe considerato, inoltre, che lo status di soggetto affetto da sindrome di Down del ragazzo ripreso era ben percepibile dalla visione del video e risultava dal titolo del video stesso.

3.2. Con un secondo motivo di ricorso, si lamentano l'erronea applicazione della normativa sul commercio elettronico alla fattispecie nonché la mancanza della motivazione sul punto. Non si sarebbe tenuto in considerazione, in particolare, che il D.Lgs. n. 70 del 2003, art. 1, comma 2, lett. *b*), prevede espressamente che non rientrano nel campo di applicazione della normativa sul commercio elettronico le questioni relative al diritto alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle telecomunicazioni.

Si deduce, inoltre, l'erronea applicazione della normativa sul commercio elettronico al caso in esame, vista la previsione del D.Lgs. n. 70 del 2003, art. 16, comma 2. Non si sarebbe considerato, infatti, che il riconoscimento della natura di host attivo a Google video non può che comportare a livello giuridico l'esclusione della clausola di limitazione di responsabilità di cui al D.Lgs. n. 70 del 2003, art. 16, comma 1, perché il comma 2 di detta disposizione, in linea con l'art. 14 della direttiva dell'Unione europea sul commercio elettronico, dovrebbe essere interpretato nel senso che la limitazione di responsabilità si applica al prestatore del servizio di posizionamento su Internet qualora detto prestatore non abbia svolto un ruolo attivo quanto alla conoscenza e al controllo dei dati memorizzati.

3.3. Con un terzo motivo di doglianza, si deducono l'inosservanza del D.Lgs. n. 196 del 2003, artt. 167, 13, 23 e 4, nonché la mancanza e la manifesta illogicità della motivazione. Si contesta, in particolare, l'affermazione della Corte d'appello secondo cui trattare un video non significherebbe trattare il singolo dato contenuto in esso. Secondo il ricorrente, invece, la distinzione tra contenitore (ripresa video) e contenuto (dato personale oggetto della ripresa video) si risolverebbe in un puro artificio retorico che non consentirebbe di escludere dalla disciplina sulla privacy il trattamento del video. Inoltre l'aver riconosciuto a Google Italia, in relazione all'erogazione del servizio Google video, la natura di host attivo avrebbe imposto il riconoscimento della sussistenza della qualifica di titolare del trattamento anche in capo agli imputati. A ciò dovrebbe aggiungersi che, secondo l'art. 13, comma 4, richiamato, se i dati personali non sono raccolti presso l'interessato — come avvenuto nel caso in esame, dal momento che il video è stato caricato non già dal soggetto affetto da sindrome di Down ivi rappresentato ma da altri soggetti — l'informativa di cui al comma 1, comprensiva delle categorie dei dati trattati, deve essere data all'interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.

Il ricorrente richiama la sentenza Cass. sez. 3, 24 maggio 2012, n. 23798, con la quale era stata affermata la responsabilità penale del legale rappresentante e del responsabile della privacy di una società, per illecito trattamento di dati personali, in relazione al caso di passaggio di mano di un database formato da centinaia di migliaia di indirizzi e-mail, per la mancanza dell'informativa volta ad acquisire il consenso dell'interessato.

3.4. Si deducono, in quarto luogo, l'erronea applicazione della legge penale e l'illogicità manifesta della motivazione quanto all'esclusione dell'elemento soggettivo. Non si sarebbe considerato in particolare che, se è pacifico che la fattispecie incriminatrice richiede il dolo specifico, non è necessario che la finalità di profitto sia effettivamente conseguita, essendo sufficiente che essa sia perseguita. Sarebbe, in particolare, possibile per l'agente rappresentarsi, sia pure sotto forma di dolo eventuale, l'illiceità di un trattamento del dato personale e perseguire allo stesso tempo la finalità di profitto.

4. Con memoria depositata in prossimità dell'udienza, gli imputati, tramite i difensori, hanno eccepito, in primo luogo, di non essere titolari, in base al D.Lgs. n. 196 del 2003 (di seguito "Codice Privacy"), del trattamento dei dati personali del soggetto rappresentato nel video caricato sulla piattaforma Google video.

Rilevano, in particolare, che il titolare del trattamento è individuato, dall'art. 4 del Codice Privacy, come il soggetto che abbia il potere di esprimere scelte in ordine allo scopo del trattamento e alle modalità dello stesso; soggetto che nel caso di specie deve identificarsi con la persona che abusivamente aveva caricato il video sulla piattaforma senza preventivamente acquisire il consenso dell'interessato al trattamento dei dati e senza, comunque, rispettare le altre prescrizioni imposte dallo stesso Codice. Le difese richiamano, a tale scopo un parere pro veritate fornito dall'ex Presidente dell'Autorità Garante per la Protezione dei Dati Personali, oltre ai pareri del Gruppo di Lavoro Art. 29 per la protezione dei

dati, organo consultivo dell'Unione europea, composto dai rappresentanti delle Autorità garanti dei singoli Stati membri. Né potrebbe sussistere in capo agli imputati l'obbligo di fornire l'informativa agli interessati prima di acquisire il consenso di questi al trattamento dei dati; obbligo che, anche se configurabile, non determinerebbe del resto il sorgere di alcuna responsabilità penale.

Si evidenzia, in secondo luogo, che, al momento in cui si sono svolti i fatti (settembre-novembre 2006) non esisteva una tecnologia di filtraggio preventivo idonea ad identificare automaticamente i contenuti eventualmente illeciti di un video; con la conseguenza che una vigilanza da parte degli imputati non avrebbe potuto essere ritenuta esigibile.

Si sostiene, in terzo luogo, che al caso in esame è sostanzialmente applicabile la normativa sul commercio elettronico di cui al D.Lgs. n. 70 del 2003, con particolare riferimento alla prestazione dei servizi di hosting. E ciò, anche se l'art. 1 di detto decreto prevede che esso non si applica alle questioni di diritto relative alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle telecomunicazioni. La difesa sottolinea, sul punto, che sia la normativa sulla protezione dei dati personali sia quella sul commercio elettronico devono essere interpretate nel senso che lo hosting provider non acquisisce la qualifica di titolare del trattamento e, dunque, non può essere chiamato a rispondere del contenuto dei file inseriti da altri sulla piattaforma da lui gestita. A sostegno di tale interpretazione, si richiamano l'art. 1, comma 5, lett. *b*), della direttiva sul commercio elettronico e la sua interpretazione ad opera della Prima relazione della Commissione del 21 novembre 2003; nonché il parere del 7 gennaio 2009 del Garante europeo della protezione dei dati personali e lo Working Document dello staff della Commissione europea dell'11 gennaio 2012.

Si contesta, infine, la prospettazione dell'accusa in relazione alla sussistenza dell'elemento soggettivo del delitto di illecito trattamento dei dati, sul rilievo che gli imputati non erano a conoscenza — né avrebbero potuto esserlo secondo la tecnologia disponibile all'epoca dei fatti — dell'esistenza di dati personali all'interno di uno fra i molteplici video caricati sulla piattaforma Google video; con la conseguenza che essi non si erano rappresentati in alcun modo il fatto di procedere ad un trattamento di dati personali.

CONSIDERATO IN DIRITTO. — 5. Il ricorso del Procuratore generale non è fondato.

6. La complessità e la novità delle questioni trattate impongono una sintetica ricostruzione del quadro normativo interno di riferimento.

6.1. Il comma 1 dell'art. 4 del Codice Privacy reca le seguenti definizioni: « *a*) "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati

in una banca di dati; *b*) "dato personale", qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale; ... *d*) "dati sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

... *f*) "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza; *g*) "responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali; ... *i*) "interessato", la persona fisica, cui si riferiscono i dati personali; *l*) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione; *m*) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione ».

6.2. L'art. 13 del Codice Privacy prevede, al comma 1, che:

"L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:

a) le finalità e le modalità del trattamento cui sono destinati i dati; *b*) la natura obbligatoria o facoltativa del conferimento dei dati; *c*) le conseguenze di un eventuale rifiuto di rispondere; *d*) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi; *e*) i diritti di cui all'art. 7; *f*) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'art. 5 e del responsabile.

Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'art. 7, è indicato tale responsabile".

Prevede inoltre, al comma 4, che, "Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione".

La violazione delle disposizioni dell'art. 13 è punita dal successivo art. 161 del Codice Privacy con la sanzione amministrativa del pagamento di una somma di denaro.

6.3. L'art. 17 dello stesso Codice prevede, poi, che il trattamento di dati che presentano rischi specifici "per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti". Tali misure e accorgimenti "sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare".

6.4. L'art. 23 dispone — per quanto qui rileva — che il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato e che tale consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.

6.5. Il successivo art 26, dopo avere affermato, al comma 1, che "i dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti", prevede, al comma 5, che "i dati idonei a rivelare lo stato di salute non possono essere diffusi".

6.6. La violazione di tali ultime disposizioni è sanzionata dall'art. 167, a norma del quale, "1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trame per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli artt. 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'art. 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

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

6.7. A tale disciplina si affianca quella contenuta nel D.Lgs. 9 aprile 2003, n. 70 (Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico), che all'art. 1, comma 2, alinea e lett. *b*), dispone che "Non rientrano nel campo di applicazione del presente decreto: ... *b*) le questioni relative al diritto alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle telecomunicazioni di cui alla L. 31 dicembre 1996, n. 675, e al D.Lgs. 13 maggio 1998, n. 171, e successive modificazioni.

6.8. Quanto alla responsabilità nell'attività di memorizzazione di informazioni (hosting), il successivo art. 16 del medesimo D.Lgs. n. 70 del 2003 prevede che, "1. Nella prestazione di un servizio della società dell'informazione, consistente nella memorizzazione di informazioni for-

nite da un destinatario del servizio, il prestatore non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore: *a*) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione; *b*) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

2. Le disposizioni di cui al comma 1 non si applicano se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore.

3. L'autorità giudiziaria o quella amministrativa competente può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse".

6.9. Infine, a norma del successivo art. 17 (Assenza dell'obbligo generale di sorveglianza), "1. Nella prestazione dei servizi di cui agli artt. 14, 15 e 16, il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.

2. Fatte salve le disposizioni di cui agli artt. 14, 15 e 16, il prestatore è comunque tenuto: *a*) ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione; *b*) a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite.

3. Il prestatore è civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non ha provveduto ad informarne l'autorità competente".

7. Dall'esame complessivo delle disposizioni riportate emerge che nessuna di esse prevede che vi sia in capo al provider, sia esso anche un hosting provider, un obbligo generale di sorveglianza dei dati immessi da terzi sul sito da lui gestito. Né sussiste in capo al provider alcun obbligo sanzionato penalmente di informare il soggetto che ha immesso i dati dell'esistenza e della necessità di fare applicazione della normativa relativa al trattamento dei dati stessi.

7.1. A tali conclusioni si giunge muovendo dall'analisi delle definizioni di "trattamento" e "titolare del trattamento" fornite dal richiamato art. 4 del Codice Privacy. Infatti, se non vi è dubbio che il concetto di "trattamento" sia assai ampio, perché comprensivo di ogni operazione che abbia

ad oggetto dati personali, indipendentemente dai mezzi e dalle tecniche utilizzati, il concetto di "titolare" è, invece, assai più specifico, perché si incentra sull'esistenza di un potere decisionale in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati. Dalla definizione legislativa si desume, in altri termini, che titolare del trattamento non è chiunque materialmente svolga il trattamento stesso, ma solo il soggetto che possa determinarne gli scopi, i modi, i mezzi.

Dal complesso dei precetti fissati dagli artt. 13, 17, 23, 26 del Codice Privacy, interpretati in combinato disposto con le norme sanzionatorie degli artt. 161 e 167 stesso Codice emerge, poi, che essi sono tutti diretti al titolare del trattamento, eventualmente nella persona del "responsabile", ovvero del soggetto preposto al trattamento stesso dal titolare, ai sensi dell'art. 4, comma 1, lett. *g*). Tali disposizioni presuppongono, infatti, l'esistenza di un effettivo potere decisionale circa: *a*) le finalità e le modalità del trattamento cui sono destinati i dati e la comunicazione eventuale dei dati stessi ad altri soggetti, anche attraverso la designazione dei responsabili (art. 13); *b*) la gestione dei rischi specifici "per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento" (art. 17); *c*) la ricezione del consenso degli interessati, nel rispetto dei divieti legge (artt. 23 e 26).

Ne deriva, più in particolare, che i reati di cui all'art. 167 del Codice Privacy — per i quali qui si procede — devono essere intesi come reati propri, trattandosi di condotte che si concretizzano in violazioni di obblighi dei quali è destinatario in modo specifico il solo titolare del trattamento e non ogni altro soggetto che si trovi ad avere a che fare con i dati oggetto di trattamento senza essere dotato dei relativi poteri decisionali.

7.2. Tali conclusioni trovano applicazione anche con riguardo alla figura dell'internet hosting provider, perché esso è definito dal D.Lgs. n. 70 del 2003, art. 16 come colui che si limita a prestare un "servizio consistente nella memorizzazione di informazioni fornite da un destinatario del servizio". Da tale definizione, interpretata nel contesto complessivo dello stesso art. 16, emerge, infatti, che il gestore del servizio di hosting non ha alcun controllo sui dati memorizzati, né contribuisce in alcun modo alla loro scelta, alla loro ricerca o alla formazione del file che li contiene, essendo tali dati interamente ascrivibili all'utente destinatario del servizio che li carica sulla piattaforma messa a sua disposizione. A tale proposito, risulta significativo che, secondo l'espressa previsione dello stesso art. 16, lo hosting provider non sia responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio.

E ciò, alla duplice condizione: che il provider non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione;

che, non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso. Così disponendo, in conformità della direttiva 2000/31/CE, il legislatore ha inteso porre quali presupposti della

responsabilità del provider proprio la sua effettiva conoscenza dei dati immessi dall'utente e l'eventuale inerzia nella rimozione delle informazioni da lui conosciute come illecite. Se ne desume, ai fini della ricostruzione interpretativa della figura del titolare del trattamento dei dati, che il legislatore ha inteso far coincidere il potere decisionale sul trattamento con la capacità di concretamente incidere su tali dati, che non può prescindere dalla conoscenza dei dati stessi. In altri termini, finché il dato illecito è sconosciuto al service provider, questo non può essere considerato quale titolare del trattamento, perché privo di qualsivoglia potere decisionale sul dato stesso;

quando, invece, il provider sia a conoscenza del dato illecito e non si attivi per la sua immediata rimozione o per renderlo comunque inaccessibile esso assume a pieno titolo la qualifica di titolare del trattamento ed è, dunque, destinatario dei precetti e delle sanzioni penali del Codice Privacy. In via generale, sono, dunque gli utenti ad essere titolari del trattamento dei dati personali di terzi ospitati nei servizi di hosting e non i gestori che si limitano a fornire tali servizi.

7.3. L'interpretazione appena delineata risulta ulteriormente confermata dal tenore letterale del successivo art. 17 — applicabile a tutte le categorie di provider disciplinate dagli artt. precedenti, ivi compreso lo hosting service provider — che esclude la configurabilità di un obbligo generale di sorveglianza sulle informazioni trasmesse o memorizzate e di un obbligo generale di ricercare attivamente eventuali illeciti. La stessa disposizione individua il punto di equilibrio fra la libertà del provider e la tutela dei soggetti eventualmente danneggiati nella fissazione di obblighi di informazione alle autorità, a carico dello stesso provider, relativamente a presunte attività o informazioni illecite dei quali sia venuto a conoscenza, anche al fine di consentire l'individuazione dei responsabili.

Né a tale conclusione può obiettarsi — come fa il Procuratore generale con il secondo motivo di ricorso — che il D.Lgs. n. 70 del 2003, art. 1, comma 2, lett. *b*), prevede espressamente che non rientrano nel campo di applicazione della normativa sul commercio elettronico le questioni relative al diritto alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle telecomunicazioni.

La richiamata disciplina sul commercio elettronico viene infatti in rilievo — come visto — non in via diretta ma solo in via interpretativa, al fine di chiarire ulteriormente e confermare la portata che la disciplina in materia di privacy ha già di per sé.

In questo quadro, la definizione di Internet hosting provider contenuta nel richiamato D.Lgs. n. 70 del 2003, art. 16 deve essere intesa come meramente ripetitiva della nozione comune di Internet hosting provider già desumibile dal linguaggio utilizzato dagli operatori informatici. Si tratta, peraltro, di una nozione che si pone in linea con l'orientamento del Gruppo di lavoro istituito dall'art. 29 della direttiva 95/46/CE e composto dai rappresentanti delle autorità garanti in materia di privacy dei singoli Stati membri; organo consultivo indipendente avente il compito di esaminare le questioni attinenti all'applicazione delle norme nazionali di attuazione di detta direttiva. Nei suoi pareri (v., in particolare, il n. 5 del 2009 e il n. 1 del 2010, in ec.europa.eu/justice/policies/docs) si evidenzia, in

particolare, che i titolari del trattamento dei dati caricati in siti di hosting sono i singoli utenti che li hanno caricati e che l'essere titolare del trattamento deriva dal fatto concreto che un soggetto abbia scelto di trattare dati personali per propri fini; con la conseguenza che la persona che può essere chiamata a rispondere delle violazioni delle norme sulla protezione dei dati è sempre il titolare del trattamento e non il mero hosting provider. Analoghe considerazioni vengono svolte, a proposito del fornitore di servizi di motore di ricerca su Internet, ai punti 84 e seguenti delle conclusioni dell'Avvocato generale presentate il 25 giugno 2013 di fronte alla Corte di Giustizia nella causa C-131/12 (Google Spain SL e Google Inc. contro Agencia Espanda de Proteccion de Datos e Mario Costeja Gonzalez), laddove si precisa, in particolare, che tale fornitore è riconducibile alla categoria dei titolari del trattamento di dati solo laddove incida direttamente sulla struttura degli indici di ricerca, ad esempio favorendo o rendendo più difficile il reperimento di un determinato sito.

7.4. A tali considerazioni deve aggiungersi, infine, che la clausola di cui all'art. 1, comma 5, lettera *b*), della direttiva sul commercio elettronico, ripresa da quella contenuta nel D.Lgs. n. 70 del 2003, art. 1, comma 2, lett. *b*), non ha di per sé la funzione di rendere inoperanti comunque in ogni fattispecie che riguardi la materia della protezione dei dati personali le norme in materia di commercio elettronico. Più semplicemente, detta clausola ha la funzione di chiarire che la tutela dei dati personali è disciplinata da un *corpus* normativo diverso da quello sul commercio elettronico; *corpus* normativo che rimane applicabile in ambito telematico anche in seguito all'emanazione della normativa sul commercio elettronico. Da ciò discende l'ovvia conseguenza che l'applicazione delle norme in materia di commercio elettronico deve avvenire in armonia con le norme in materia di tutela dei dati personali; armonia perfettamente riscontrabile — come appena visto — nel caso della determinazione dell'ambito di responsabilità penale dell'Internet hosting provider relativamente ai dati sensibili caricati dagli utenti sulla sua piattaforma. Tale interpretazione trova piena conferma, inoltre, nella Prima relazione della Commissione in merito all'applicazione della direttiva 2000/31/CE, del 21 novembre 2003, in cui si legge, al paragrafo 4.6, che le limitazioni della responsabilità giuridica stabilite dalla direttiva sul commercio elettronico hanno carattere generale e coprono tanto la responsabilità civile quanto quella penale, per tutti i tipi di attività illegali intraprese da terzi.

Un'ulteriore conferma è data, poi, dalla sentenza della Corte di giustizia dell'Unione Europea 23 marzo 2010, nei procedimenti da C-236/08 a C-238/08 (punto 120), nella quale si afferma che l'art. 14 della Direttiva sul commercio elettronico (corrispondente al D.Lgs. n. 70 del 2003, art. 16) deve essere interpretato nel senso che si applica al prestatore di un servizio di posizionamento su Internet qualora detto prestatore non abbia svolto un ruolo attivo a conferire la conoscenza o il controllo dei dati memorizzati. Se non ha svolto un tale ruolo, il provider non può essere ritenuto responsabile per i dati che ha memorizzato, salvo che, essendo venuto a conoscenza della natura illecita di tali dati, abbia omesso di prontamente rimuoverli o di disabilitare l'accesso agli stessi.

8. I principi appena enunciati trovano applicazione anche nel caso in esame, nel quale, in estrema sintesi: *a*) il video raffigurante un soggetto affetto da sindrome di Down ingiuriato e preso in giro dai suoi compagni proprio in relazione alla sua particolare sindrome era stato caricato su Google video, servizio di Internet hosting, all'insaputa di tale soggetto; *b*) nei giorni 5 e 6 novembre 2006 alcuni utenti avevano segnalato la presenza del video sul sito e ne avevano chiesto la rimozione; *c*) la rimozione era stata chiesta dalla Polizia postale il 7 novembre 2006; *d*) in quello stesso giorno il video era stato rimosso dal provider.

La posizione di Google Italia S.r.l. e dei suoi responsabili, imputati nel presente procedimento, è infatti quella di mero Internet host provider, soggetto che si limita a fornire una piattaforma sulla quale gli utenti possono liberamente caricare i loro video; video del cui contenuto restano gli esclusivi responsabili. Ne consegue che gli imputati non sono titolari di alcun trattamento e che gli unici titolari del trattamento dei dati sensibili eventualmente contenuti nei video caricati sul sito sono gli stessi utenti che li hanno caricati, ai quali soli possono essere applicate le sanzioni, amministrative e penali, previste per il titolare del trattamento dal Codice Privacy.

8.1. Tale essendo l'ambito nel quale va inquadrata la fattispecie concreta, deve rilevarsi che il primo motivo di ricorso è infondato.

Il ricorrente lamenta, in particolare, che la Corte d'appello non avrebbe considerato che, per i dati idonei a rivelare lo stato di salute, vige un divieto assoluto di loro diffusione anche in presenza del consenso dell'interessato, ai sensi del D.Lgs. n. 196 del 2003, art. 26, comma 5. Non si sarebbe considerato, inoltre, che lo status di soggetto affetto da sindrome di Down del ragazzo ripreso era ben percepibile dalla visione del video e risultava dal titolo del video stesso.

Quanto al primo di tali rilievi — ulteriormente sviluppato nell'ambito del terzo motivo di ricorso — deve premettersi che, secondo quanto affermato dalla giurisprudenza di questa Corte, pur nel diverso ambito del bilanciamento fra diritto di cronaca e protezione dei dati personali (sez. 3, 4 maggio 2011, n. 17215), la pubblicazione di un'immagine che rappresenti le condizioni di salute di un soggetto — si trattava in quel caso della foto di una persona ricoverata in fin di vita con il volto devastato da un colpo di arma da fuoco — configura un trattamento di dati personali. E ciò, perché — come già osservato — il concetto di "trattamento" è assai ampio e prescinde dall'inserimento dei dati in una vera e propria banca-dati, potendosi concretizzare in qualunque operazione di utilizzazione e diffusione di tali dati, anche per mezzo della rappresentazione fotografica o della ripresa video.

Ne consegue — con riferimento al caso di specie — che la realizzazione e il caricamento sul sito del video da parte degli utenti del servizio Google video configura un "trattamento" ai sensi dell'art. 4, comma 1, lett. *a*), del Codice Privacy, effettuato in violazione del divieto di diffusione dei dati idonei a rilevare lo stato di salute fissato dal successivo art. 26, comma 5.

Circa i responsabili della violazione, deve però ribadirsi che — contrariamente a quanto sostenuto dal ricorrente — questi sono da identifi-

carsi con gli utenti che hanno caricato il video sulla piattaforma Google video e non con i soggetti responsabili per la gestione di tale piattaforma, trattandosi, come già ampiamente visto, di un mero servizio di hosting. Ed è proprio la natura del servizio reso ad escludere anche la fondatezza del secondo dei rilievi svolti dal Procuratore generale nell'ambito del primo motivo di ricorso, non essendo configurabile alcun obbligo generale di controllo in capo ai rappresentanti di Google Italy s.r.l., gestore del servizio stesso.

8.2. Sull'infondatezza del secondo motivo di ricorso, relativamente alla pretesa inapplicabilità della normativa sul commercio elettronico alle questioni relative al diritto alla riservatezza, è sufficiente qui richiamare le considerazioni già ampiamente svolte sub 7.3.

Quanto alla pretesa non riconducibilità dell'attività svolta da Google Italy s.r.l. alla categoria dell'hosting, devono essere invece richiamati i rilievi *sub* 8., dovendosi ribadire che nel caso di specie il provider si è limitato a fornire ospitalità ai video inseriti dagli utenti, senza fornire alcun contributo nella determinazione del contenuto dei video stessi.

8.3. Analoghe considerazioni valgono con riferimento al terzo motivo di doglianza, con cui si deduce l'inosservanza del D.Lgs. n. 196 del 2003, artt. 167, 13, 23 e 4, e si afferma che, secondo l'art. 13, comma 4, richiamato, se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie dei dati trattati, deve essere data dal provider all'interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.

Va infatti rilevato che nessuno obbligo sussiste in capo al provider, non essendo questo, ma il singolo utente il responsabile del trattamento dei dati personali contenuti nel video caricato dall'utente stesso. E ciò, a prescindere dall'ulteriore analisi del quadro normativo, dalla quale emerge con chiarezza che l'eventuale violazione dell'art. 13 del Codice Privacy è sanzionata in via meramente amministrativa dal successivo art. 161 e non rientra, invece, fra quelle sanzionate penalmente dall'art. 167.

Il ricorrente afferma, poi, che vi sarebbe una qualche analogia tra la fattispecie per la quale qui si procede e quella esaminata dalla sentenza Cass., sez. 3, 24 maggio 2012, n. 23798, con la quale era stata affermata la responsabilità penale del legale rappresentante e del responsabile della privacy di una società, per illecito trattamento di dati personali, in relazione al caso di passaggio di mano di un database formato da centinaia di migliaia di indirizzi e- mail, per la mancanza dell'informativa volta ad acquisire il consenso degli interessati.

Tale affermazione non merita, all'evidenza, di essere condivisa perché non tiene conto delle peculiarità della posizione dell'Internet host provider più volte evidenziate rispetto alla posizione di un soggetto che, detenendo una vera e propria banca dati contenente gli indirizzi di una serie di soggetti, che lui stesso ha formato e gestito e della quale conosce fin dall'inizio il contenuto e le finalità, la cede ad un altro soggetto senza preoccuparsi di acquisire il consenso degli interessati.

8.4. I rilievi finora svolti conducono ad escludere in radice la configurabilità, sotto il profilo oggettivo, di una responsabilità penale dell'Internet host provider e rendono, dunque, superfluo l'esame del quarto motivo di ricorso e dei correlati rilievi contenuti nella memoria difensiva relativamente alla configurabilità dell'elemento soggettivo del reato. E ciò, a prescindere dall'ulteriore considerazione che la mancanza di una conoscenza, in capo al provider, del dato sensibile contenuto nel video caricato dagli utenti sul suo sito e la mancanza di un obbligo generale di sorveglianza inducono ad escludere comunque — come ben evidenziato dalla Corte d'appello — la rappresentazione e la conseguente volizione da parte degli imputati del fatto tipico, costituito dall'abusivo trattamento di tale dato.

9. Ne consegue il rigetto del ricorso del Procuratore generale.

P.Q.M. — Rigetta il ricorso del Procuratore generale.

La rete e le utopie regressive (sulla conclusione del caso Google/Vividown)

1. Premessa

La sentenza in commento definisce il ricorso del Procuratore generale avverso la sentenza d'appello sul caso Google-Vivi Down, relativo alla diffusione, attraverso il canale Google Video e, in assenza del consenso dell'interessato, di un filmato realizzato da alcuni studenti minorenni, ritraente vessazioni ai danni di un compagno con ritardo mentale e ingiurie nei confronti dell'associazione Vivi Down. Le immagini erano state rimosse da Google Video a circa due mesi di tempo dalla loro pubblicazione on-line e 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. Erano però stati condannati per trattamento illecito di dati personali, avendo in particolare omesso di effettuare gli adempimenti prescritti dalla disciplina in materia di protezione dati [1], con relativo nocumento per il minore e al fine di trarne profitto mediante il servizio Google video. La sentenza di appello — nel confermare l'asso-

* Le opinioni contenute in questo contributo sono espresse dall'Autore, funzionario presso l'Autorità Garante per la protezione dei dati personali, a titolo personale e non impegnano in alcun modo l'Autorità medesima.

[1] Acquisizione del consenso informato dell'interessato, peraltro in forma scritta, trattandosi di dati sensibili in quanto idonei a rivelare lo stato di salute dell'interessato (artt. 23 e 26 d.lgs. 196/2003); interpello al Garante per la verifica preliminare del trattamento che presenta rischi specifici (art. 17 d.lgs. 196).

luzione per il concorso nella diffamazione — aveva invece riformato la pronuncia di primo grado sul punto del trattamento illecito, sancendo anche in tal caso l'assoluzione per insussistenza del fatto.

Nel rigettare il ricorso avverso la sentenza d'appello, la Corte di Cassazione ha, in particolare, fornito importanti precisazioni sulla particolare posizione di un internet hosting provider quale, appunto, quella in esame e sul regime di responsabilità che ne consegue, nonché sul rapporto tra disciplina del commercio elettronico e normativa di protezione dati.

2. Titolarità del trattamento e responsabilità penale.

Centrale e assorbente, nell'argomentazione della Corte, è la considerazione secondo cui Google Video non possa ritenersi titolare del trattamento realizzato con la diffusione in internet del filmato, non disponendo di quel potere decisionale in ordine al trattamento necessario ai fini dell'assunzione della qualità di titolare, secondo l'art. 4 del d.lgs. 196/2003 (codice in materia di protezione dei dati personali; *infra*: Codice). L'internet hosting provider quale Google Video si limita infatti a prestare, ai sensi dell'art. 16 d.lgs. 70/2003 (codice del commercio elettronico), un servizio "consistente nella memorizzazione di informazioni fornite da un destinatario del servizio" quale l'utente. Il provider — osserva la Corte — non ha, dunque, alcun controllo né potere decisionale o possibilità di scelta relativamente ai dati memorizzati, al punto che l'art. 16 esclude espressamente la responsabilità dello stesso rispetto alle informazioni memorizzate a richiesta di un destinatario del servizio.

Titolare del trattamento dovrà invece ritenersi, in casi del genere — osserva la Corte — il singolo utente che abbia caricato in internet quei contenuti, avendone deciso modi, tempi, finalità.

L'assenza, in capo al provider, della qualifica di titolare del trattamento, ne esclude anche la soggezione agli obblighi (di informativa, acquisizione del consenso, ecc.) che il Codice assegna, infatti, al solo titolare (o eventualmente al responsabile del trattamento, ove designato dal primo) quale "dominus" del trattamento.

Di qui l'impossibilità di ritenere il provider soggetto attivo del reato (per cui in primo grado gli imputati avevano riportato condanna) di trattamento illecito di dati personali, che presuppone la violazione di obblighi imputabili, appunto, al solo titolare. Si tratta, insomma, di un reato proprio, integrato — osserva la Corte — da "condotte che si concretizzano in violazioni di obblighi dei quali è destinatario in modo specifico il solo titolare del trattamento e non ogni altro soggetto che si trovi ad avere a che fare con i dati oggetto di trattamento senza essere dotato dei relativi poteri decisionali". Ciò, in quanto il legislatore ha inteso far coincidere "il potere decisionale sul trattamento con la capacità di concretamente incidere su tali dati, che non può prescindere dalla conoscenza dei dati stessi".

Infatti, come si evince dalla disciplina del commercio elettronico, il limite all'assenza di responsabilità del provider consiste nell'effettiva conoscenza dei dati immessi e, quindi, nell'eventuale inerzia nel rimuovere contenuti illeciti della cui presenza in rete il gestore abbia, appunto, avuto notizia a seguito di comunicazione della autorità competenti. Ai sensi dell'art. 16 del codice del commercio elettronico, infatti, e in

conformità alla direttiva 2000/31/CE, l'hosting provider non risponde dei dati memorizzati a condizione che non sia effettivamente a conoscenza dell'illiceità delle informazioni stesse (o, relativamente ad azioni risarcitorie, di fatti e circostanze che ne rendono manifesta l'illiceità) e che, non appena a conoscenza di tali elementi, su comunicazione delle autorità competenti, provveda immediatamente alla rimozione del dato o alla disabilitazione dell'accesso. Ciò, fermo restando il potere dell'autorità giudiziaria o amministrativa competente, di esigere — anche in via d'urgenza — che il provider impedisca o ponga fine alle violazioni commesse.

Con riferimento alla medesima disciplina sancita dalla direttiva sul commercio elettronico (e che del resto il d.lgs. 70/2003 ha trasposto), la Corte di giustizia ha precisato che un intermediario deve essere considerato responsabile degli illeciti commessi in rete qualora abbia contezza di attività o informazioni illecite sia a seguito di esami effettuati di propria iniziativa, sia a seguito di notificazione (sentenza 12.7.2011 della Grande Sezione, causa C-324/09, L'Oréal c. E-bay). Ancora, la Corte, con sentenza del 23.3.2010, ha precisato che l'art. 14 della direttiva 2000/31/Ce si applica al prestatore "di un servizio di posizionamento su internet qualora detto prestatore non abbia svolto un ruolo attivo atto a conferirgli la conoscenza o il controllo dei dati memorizzati. Se non ha svolto un siffatto ruolo, detto prestatore non può essere ritenuto responsabile per i dati che egli ha memorizzato su richiesta di un inserzionista, salvo che, essendo venuto a conoscenza della natura illecita di tali dati o attività di tale inserzionista, egli abbia omesso di prontamente rimuovere tali dati o disabilitare l'accesso agli stessi".

La stessa giurisprudenza europea dimostra dunque come il provider (e in particolare l'hosting provider) non abbia alcun obbligo generale di sorveglianza sui dati immessi da terzi sul sito da lui gestito e non possa dunque rispondere degli illeciti commessi in rete dagli utenti, essendogli eventualmente imputabile solo l'inerzia nella rimozione di contenuti della cui illiceità sia venuto a conoscenza. A fortiori, l'hosting provider non può qualificarsi titolare del trattamento in quanto, non avendo alcun potere decisionale in ordine al trattamento stesso, non è destinatario degli obblighi (informativa, acquisizione del consenso, ecc.) che tale potere presuppongono. In tal senso è significativo un passaggio delle conclusioni presentate dall'Avvocato Generale alla Corte di giustizia in relazione alla causa C-131/12 (Google Spain e Google inc. c. Agencia española de protecciòn de datos), secondo cui il fornitore del servizio di motore di ricerca può qualificarsi come titolare del trattamento solo ove incida direttamente sulla struttura degli indici di ricerca, ad esempio favorendo od ostacolando il reperimento di un determinato sito.

Né questa ricostruzione potrebbe essere revocata in dubbio — osserva la Corte, in antitesi all'eccezione del Procuratore generale — dalla clausola di salvaguardia della normativa in materia di protezione dati, contenuta nell'art. 1, comma 2, lettera *b*), d.lgs. 70/2003 (che a sua volta recepisce l'art. 1, par. 5, lett. *b*) della direttiva citata), in quanto tale norma di coordinamento si limita a confermare "la portata che la disciplina in materia di privacy ha già di per sé" e non osta dunque all'applicazione — non già in via diretta ma meramente interpretativa — di norme, quali quelle di cui all'art. 16 d.lgs. 70/2003, che definiscono non istituti o aspetti specifici della protezione dati, ma concetti generali della

fornitura di servizi in rete [2]. Il riferimento al codice del commercio elettronico è dunque, nel caso in esame, necessario per comprendere se, alla luce della posizione attribuita al provider dalla disciplina del commercio elettronico, essa possa ritenersi compatibile con il potere decisionale e la "signoria" sul trattamento presupposti dalla qualità di titolare.

Confermata, dunque, l'impossibilità di considerare Google Video, internet hosting provider [3], come titolare rispetto al trattamento dei dati personali caricati dagli utenti, va esclusa anche l'imputabilità del delitto di trattamento illecito di dati personali che, appunto, tale qualità soggettiva presuppone.

L'assenza di tale qualifica in capo agli imputati esclude quindi anche la possibilità di ritenere integrato il delitto di trattamento illecito per violazione del divieto di diffusione di dati idonei a rivelare lo stato di salute (quali, nella specie, la condizione di handicap del ragazzo ingiuriato nel video) sancito in via assoluta dall'art. 26, c. 5, del Codice ovvero dell'obbligo di informativa ai sensi dell'art. 13, c. 4 [4]. Di tali illeciti possono infatti rispondere solo, nella fattispecie, gli utenti che quel video hanno caricato. Non essendo dunque configurabile, neppure sotto il profilo oggettivo, il delitto di trattamento illecito di dati personali da parte di Google video, la Corte non procede all'esame del quarto motivo di ricorso, attinente all'elemento soggettivo, rilevando tuttavia, sia pur incidentalmente, l'impossibilità di ravvisare il dolo rispetto a una fattispecie caratterizzata dall'assenza, in capo al provider, di obblighi di generale controllo sui contenuti veicolati.

Del resto, nel caso in esame non ricorrono neppure le circostanze previste dall'art. 16 D.Lgs. 70/2003 per radicare la responsabilità dell'hosting provider, non avendo Google avuto contezza dell'illiceità del video caricato ed avendo provveduto alla sua rimozione lo stesso giorno della richiesta avanzata in tal senso dalla Polizia postale.

3. Prospettive.

Nel negare all'hosting provider la qualifica di titolare del trattamento, gli obblighi correlati a tale status e, di conseguenza, la responsabilità da trattamento illecito di dati personali, la Cassazione tocca il punto nevralgico di questa disciplina, fondata sull'assenza di un generale obbligo di sorveglianza del fornitore sui dati immessi in rete dagli utenti e sotto la loro responsabilità. Il provider dovrà invece attivarsi senza ritardo per rimuovere i contenuti qualora abbia consapevolezza della loro illiceità, concorrendo altrimenti nel reato commesso da chi quelle informazioni abbia immesso in rete.

È, infatti, proprio questo sistema di "notice and take down". — centrale nella direttiva sul commercio elettronico — a garantire al punto

[2] In tal senso depone anche la prima Relazione della Commissione Ue sull'applicazioue della direttiva sul commercio elettronico, le cui limitazioni — si afferma — hanno carattere generale e coprono "tanto la responsabilità civile quanto quella penale", per tutti i tipi di attività illegali intraprese da terzi.

[3] imitandosi il provider, nell'ambito di tale servizio, a fornire ospitalità ai filmati caricati dagli utenti, in assenza di alcun contributo alla determinazione del loro contenuto.

[4] Norma la cui violazione, peraltro, non integra gli estremi del trattamento illecito di dati personali ma il mero illecito amministrativo di cui all'art. 161 del Codice.

più alto l'equilibrio tra libertà e responsabilità in rete; tra libertà di espressione e difesa dei diritti delle vittime dei reati commessi on-line; tra assenza di censure e doveroso accertamento delle responsabilità di chiunque abbia usato la rete per offendere, ingiuriare, ledere gli altrui diritti e libertà. Proprio per questo, andrebbero rafforzati gli strumenti (soprattutto procedurali) idonei a garantire alla vittima di illeciti commessi in rete la possibilità di ottenere quanto prima dal provider la rimozione dei contenuti lesivi, senza alterare il bilanciamento garantito dalla direttiva sul commercio elettronico né il sistema di anonimato "tracciabile" oggi vigente che consente di coniugare la massima libertà di espressione con le esigenze di accertamento e repressione dei reati.

In tal senso si muove, ad esempio, la proposta di legge Moretti-Sanna AC 2049 recante "Modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, alla legge 8 febbraio 1948, n. 47, e al codice penale, in materia di tutela della dignità personale nella rete internet" che introduce alcune importanti innovazioni nel sistema di tutela della vittima degli illeciti commessi in rete e, soprattutto, dell'*hate speech*, ormai sempre più frequente e sempre più violento [5].

In particolare, la proposta di legge — lungi dal prevedere alcun filtro preventivo né alcun obbligo di controllo, da parte dei gestori, dei contenuti diffusi in rete — codifica soltanto un onere di attivazione per rimuovere espressioni violente, ingiuriose o diffamatorie, mediante una specifica procedura d'urgenza, modulata sui tempi — contratti e veloci — che caratterizzano la vita della rete. Essa presuppone in prima istanza una richiesta di adesione spontanea al titolare del trattamento e, solo nel caso di un suo rifiuto di adempiere o di impossibilità di identificare il titolare, la pronuncia (anch'essa in tempi brevissimi: dalle 48 alle 72 ore nei casi più complessi) del Garante per la protezione dei dati personali, secondo una procedura tale da garantire pienamente il contraddittorio delle parti. All'esito di tale pronuncia, il Garante potrà prescrivere, se del caso allo stesso fornitore, le misure necessarie per conformare il trattamento alla disciplina di protezione dati, la cui omessa adozione integrerà gli estremi dell'illecito amministrativo — o, nei casi più gravi, del delitto — di inosservanza dei provvedimenti del Garante.

Si tratta di misure che, muovendosi nel sistema già tracciato dalla direttiva sul commercio elettronico, consentirebbero di offrire alle vittime dell'hate speech — o comunque dei reati commessi in rete — delle procedure agili, facilmente accessibili e sufficientemente celeri per ottenere tutela, impedendo soprattutto il protrarsi dell'offesa.

Misure come queste consentirebbero di impedire le due opposte "utopie regressive" [6], che finirebbero con il rendere la rete uno spazio di censura o, all'opposto, di anomia.

FEDERICA RESTA

[5] Oltre a rivedere la disciplina della diffamazione nel segno della centralità della rettifica quale causa di non luogo a procedere e a codificare specifici istituti a tutela del diritto all'oblio, all'aggiornamento e alla rettificazione dei dati personali.

[6] Mutuo la definizione utilizzata, sia pur con riferimento a diverse realtà, da Luigi Manconi, Difendo la Cancellieri dalla cultura del sospetto, in Huffingtonpost.it.