

CARLO ROSSELLO

RIFLESSIONI *DE JURE CONDENDO* IN MATERIA DI RESPONSABILITÀ DEL PROVIDER

SOMMARIO: 1. Il *digital divide* tra una sponda e l'altra dell'Atlantico. — 2. La storia delle idee. — 3. La sentenza *Google c. Vividown*. — 3.1. Mera intermediazione o fornitura di contenuti? — 3.2. Il rapporto tra controllo automatico (di carattere tecnico) e « controllo sociale » da parte degli utenti. — 3.3. È configurabile un obbligo per il proprietario o per il gestore del sito Web (sia esso *Host Provider*, *Access Provider*, *Service Provider* o *Content Provider*) di adeguarsi ai dettami del regime di tutela dei dati personali? — 3.4. Le conclusioni della pronuncia *Google c. Vividown*. — 4. Brevi riflessioni *de iure condendo*. — 4.1. Parallelo con la responsabilità da prodotto difettoso. — 4.2. Parallelo con la responsabilità da attività pericolose. — 5. Critiche e possibili soluzioni. — 6. Conclusioni.

1. IL *DIGITAL DIVIDE* TRA UNA SPONDA E L'ALTRA DELL'ATLANTICO.

Dalla lettura della sentenza (e non solo da quella, come si vedrà tra un attimo) si ricava l'impressione dell'esistenza di un ulteriore *digital divide* oltre a quello che corre tra Paesi a economia matura e Paesi in via di sviluppo.

Detta faglia corre al di sotto dell'oceano Atlantico e separa gli Stati Uniti dai Paesi dell'Unione Europea.

A dimostrazione di questo assunto, si può assumere come premessa maggiore la storia delle idee (se vogliamo, la dottrina statunitense in materia di *Governance* della Rete) con i riscontri puntuali che dette teorizzazioni trovano nel comportamento degli operatori economici, e specificamente i *Providers* statunitensi, e ancora più specificamente nei comportamenti e nella « filosofia » del colosso di *Mountain View* come identificati nella corporata sentenza oggetto di questo convegno.

* Relazione introduttiva al convegno « *Il futuro della responsabilità sulla rete. Quali regole dopo la sentenza Google/Vividown* », organizzato dalla Università di

Roma Tre e dalla Fondazione Calamandrei e svoltosi il 21 maggio 2010. La sentenza Trib. Milano 12 aprile 2010 è pubblicata in questa *Rivista*, 2010, p. 474.

2. LA STORIA DELLE IDEE.

Il pubblico al quale mi rivolgo è troppo sofisticato per non conoscere l'esistenza di una teorizzazione in base alla quale si è trascorsi da una originaria tesi (ormai superata) di insofferenza di Internet rispetto a qualsiasi forma di regolamentazione (i primi lavori di Lawrence Lessig e soprattutto il suo epocale *Code and Other Law of Cyberspace*¹ a una impostazione secondo la quale la Rete andrebbe soggetta ad una «*lex informatica*» frutto di una sorta di autopoiesi, una *enclave* dotata di regole sue proprie di fonte non statuale e tantomeno autoritativa².

Secondo detta teorizzazione, Internet andrebbe considerato come una sorta di universo parallelo nel quale operano e si auto-producono regole sociali di comportamento sue proprie³.

In particolare Johnson e Post propongono come fonte primaria di *Governance* della Rete un processo decentralizzato di adozione volontaria di standard di comportamento da parte degli operatori e della comunità degli utenti. Le regole di comportamento risulterebbero in tal modo diverse per ciascuna sotto-comunità di utenti, ma gli inconvenienti di tale disomogeneità verrebbero superati — sempre nelle tesi di Johnson & Post — dal fatto che coloro che non concordano con un determinato corpo di regole potrebbero «*migra-*

¹ L. LESSIG, *Code and Other Laws in the Cyberspace*, New York, Basic Books, 1999. In una conferenza tenuta presso la New York Media Association nel giugno 1998, Lawrence Lessig pronunciò una frase divenuta emblematica dell'approccio deregolamentato: «*We have no problem of governance in cyberspace. We have problem with governance*». Lessig, a quell'epoca professore alla Harvard Law School, è attualmente professore a Stanford, dove ha fondato il CIS («*Center for Internet Society*»). È stato assistente di Richard Posner nella sua attività di giudice presso il 7th Circuit della Corte di Appello, e può definirsi un analista della «*Post Chicago School*», una scuola di pensiero che affonda le radici nell'analisi economica del diritto liberista della progenie posneriana, e la combina con l'analisi dell'architettura della Rete. La tesi e l'impostazione generale sono riprese dall'A. in *The Future of Ideas*, New York-Toronto, Random House, 2001, tradotto in italiano col titolo *Il futuro delle idee*, Milano, 2006, specie pp. 30-88; 149-207.

² È la tesi propugnata da V. GAUTRAIS-G. LEFEBVRE-K. BENYKHLEF, *Droit du commerce électronique et norme applicables: l'émergence de la lex electronica*, in *Revue*

de droit des affaires internationales (International Business Law Journal), 1997, p. 547 ss., i quali assegnano notevole importanza nella regolamentazione del *cyber-spazio* (e del commercio elettronico in particolare) alla *lex mercatoria*, e segnatamente alle pratiche contrattuali e agli usi che verranno a consolidarsi nel settore; T. DELACOURT, *The International Impact of Internet Regulation*, in *Harvard Internat. Law Journal*, 1997, p. 207 ss.; D.R. JOHNSON-D.G. POST, *Law and Borders - The Rise of Law in Cyberspace*, in *Stanford Law Review*, 1996, p. 1367 ss.; Id., *And How Shall the Net Be Governed? A Meditation on the Relative Virtues of Decentralised, Emergent Law*, in M.A. LEMLY-P.S. MENELL-R.P. MERGES-P. SAMUELSON (a cura di), *Software and Internet Law*, 2nd ed., Aspen Law & Business, New York, 2003, p. 1019 ss., secondo i quali Internet andrebbe considerato come un mondo parallelo nel quale operano e si sviluppano regole sociali autoprodotte.

³ Per una più ampia ricognizione mi permetto di fare rinvio a C. ROSSELLO, *Commercio elettronico. La Governance di Internet tra diritto statale, autodisciplina, soft law e lex mercatoria*, Milano, 2006, specie pp. 1-22.

vedersi precluso l'accesso (attraverso sistemi di filtraggio tecnico) alle aree con le quali i loro comportamenti sono incompatibili.

Si creerebbe così una sorta di federalismo elettronico, nel quale ciascuna sotto-comunità si dota di regole sue proprie.

Quanto alla coercibilità delle regole volontariamente assunte, essa sarebbe garantita dalla forza vincolante del contratto (tra *System operator* e utente), che è legge tra le parti, e come tale trova sanzione e protezione da parte dell'ordinamento⁴.

Su posizioni sostanzialmente non dissimili si attesta Joel Reidenberg⁵. Tale A. teorizza che « *The characteristics of lex informatica*

⁴ Cfr. D.R. JOHNSON and D.G. POST, *And How Shall the Net Be Governed? A Meditation on the Relative Virtues of Decentralized, Emergent Law*, disponibile on-line su www.cli.org.emdraft.html, ivi, p. 7 della versione elettronica. Cfr. Anche IDD., *Law and Borders. The Rise of Law in Cyberspace*, in 48 (1996) *Stanford Law Review*, p. 1367 ss., pubblicato con leggere modifiche anche con il titolo *The Rise of Law on the Global Network*, in B. KAHN and C. NESSON (a cura di), *Borders in Cyberspace*, cit., p. 3 ss., (e disponibile in linea all'indirizzo www.cli.org/X0025_LBFIN.html). Quanto al primo aspetto, gli AA. osservano come, considerata l'architettura « logica » e non « geografica » di Internet, qualsiasi tentativo di sormontare il problema dell'indipendenza dei messaggi da locazioni geografiche è « *as futile as an effort to tie an atom to a bit together* ». Per quanto concerne gli effetti dei comportamenti *on-line*, il fatto che le informazioni disponibili sul Web siano accessibili simultaneamente da parte di chiunque sia in connessione fa sì che un sito localizzato — ad esempio — in Brasile non abbia maggiori effetti sui cittadini Brasiliani di un sito localizzato in Belize accessibile dal Brasile. Ne derivano analoghe conseguenze quanto alla legittimità ed efficacia di regole che pretendano di governare tali comportamenti su base geografico-territoriale: « *no physical jurisdiction has a more compelling claim than any other to subject these events exclusively to its laws* ». Infine, mentre nel mondo reale l'individuo è avvertito del cambiamento delle regole applicabili ai suoi comportamenti dal fatto di attraversare frontiere fisiche, ciò non avviene nel *cyberspazio*.

La soluzione proposta da Johnson e Post è quella di considerare il *cyberspazio* come un luogo distinto dal mondo reale, i cui confini vengono varcati nel momento in cui, attraverso uno schermo ed una *password*, si oltrepassano le frontiere elettroniche che separano un mondo dall'altro. Un universo parallelo, le cui regole — autonome ed auto-

ctone — sarebbero più facilmente conoscibili e coercibili di quelle del mondo fisico. L'analogia proposta è quella con la *lex mercatoria*, quale corpo di regole autoprodotte dal ceto mercantile sviluppatosi dopo il medioevo. La risposta al problema della *governance* è quindi trovata — nella impostazione di Johnson e Post — tutta ed esclusivamente sul piano della autoregolamentazione: lo Stato dovrebbe ritirare la propria sovranità per allocare la funzione regolamentatrice a coloro che meglio comprendono il fenomeno tecnico, e che hanno interesse ad assicurare la crescita e la prosperità delle loro imprese.

⁵ J.R. REIDENBERG, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, in *Texas Law Review*, 1998, p. 553 ss. (contributo disponibile in formato elettronico — così come numerosi altri lavori di Joel R. Reidenberg, attualmente professore presso la *Fordham University School of Law* — all'indirizzo: <http://reidenberg.home.sprynet.com>), ivi, p. 555). Cfr. anche ID., *Governing Networks and Rulemaking in Cyberspace*, cit., p. 88 ss., ove l'affermazione in base alla quale « *policy makers must begin to recognize network sovereignty and begin to shift the regulatory role of states toward indirect means that develop networks rules* » (ivi, p. 98), e la conclusione che il settore privato — in particolare la determinazione degli standard tecnici — debbano avere un ruolo preminente nella *governance* delle reti globali, considerate come entità semi-sovrane (« *semi-sovereign entities* »), mentre allo Stato debba essere riservato un ruolo sussidiario di intervento nei soli casi in cui vengano in rilievo interessi pubblici o quando lo Stato stesso sia meglio in grado di intervenire di quanto lo sia le Rete, per il resto limitandosi alla funzione di incentivazione dell'autoregolamentazione (ivi, pp. 99-101). Sulla stessa linea si cfr. anche ID., *Privacy and the Interdependence of Law, Technology and Self-Regulation*, in AA.VV., *Variations sur le droit de la société de l'information*,

provide ways to accommodate different national public policies for controversial problems, such as content restrictions, the treatment of personal information, and the protection of intellectual property circulating in the transnational networks».

La conclusione dell'A. è che il settore privato, e in particolare la determinazione degli standard tecnici, debbano giocare un ruolo preminente nella regolamentazione delle Reti globali, considerate come entità semi-sovrane (*Semi-sovereign Entities*), mentre allo Stato dovrebbe essere riservato un ruolo sussidiario di intervento nei soli casi in cui vengano in rilievo interessi pubblici o quando lo Stato stesso sia meglio in grado di intervenire di quanto lo sia la Rete, per il resto limitandosi alla funzione di incentivazione dell'autoregolamentazione.

La soluzione di carattere tecnologico presenterebbe il vantaggio di non essere collegata ad alcun sistema giuridico (leggi: ordinamento) nazionale, e di fornire di per sé risposta ai principali problemi di coordinamento delle legislazioni nazionali, e ciò in particolare con riguardo: (i) ai controlli sui contenuti; (ii) alla protezione dei dati personali; (iii) alla protezione dei diritti di proprietà intellettuale sui contenuti diffusi in Rete.

Il vantaggio primario della soluzione tecnica (anziché normativa) sarebbe quello di: (i) non basarsi su confini territoriali; (ii) di consentire un'elasticità delle regole rapportata alla varietà degli strumenti tecnici, e infine (iii) di fondarsi su meccanismi di *self-enforcement* e di automonitoraggio.

L'obiezione mossa da questa sponda dell'Atlantico a tale pur pregevole impianto teorico è quella che, affidando la soluzione del problema di regolamentazione *unicamente* allo strumento tecnico e all'autodisciplina, si bypassa il processo democratico e si affida il governo della Rete esclusivamente agli attori forti: i fornitori di servizi, i *Providers* e comunque le imprese che prescelgono e governano lo strumento tecnico⁶.

Si prescinde — in definitiva — dal problema di uno sviluppo etico e socialmente responsabile della Rete⁷.

Chaiers du C.R.I.D., Bruxelles, Bruylant, 2001 (che ho consultato nella versione elettronica); ID., *L'instabilité et la concurrence des régimes réglementaires dans le cyberspace*, in E. MACKAAY, *Les incertitudes du droit*, Montreal, Editions Thémis, 2000, p. 134 ss.; C. KESSEDIAN, *Rapport de synthèse*, in K. BOELE-WOELKI and C. KESSEDIAN (a cura di), *Internet. Which Court Decides? Which Law Applies?*, The Hague-London-Boston, Kluwer Law International, 2001, p. 143 ss., specie p. 154; ID., *Technology and Internet Jurisdiction*, in *University of Pennsylvania Law Review*, 2005, p. 153 ss. (disponibile on-line presso il sito web di

Reidenberg); ID., *States and Internet Enforcement*, in *University of Ottawa Technology Law Journ.*, 2004, p. 213 ss. (*idem*).

⁶ Cfr. in tal senso le riflessioni di J. BERLEUR et Y. POULLET, *Quelles régulation pour l'Internet?*, in J. BERLEUR-C. LAZAROR. QUECK (a cura di), *Gouvernance de la société de l'information. Loi, autoregulation, éthique*, Cahiers du CRID n. 22, Bruxelles, Bruylant, 2002, p. 133 ss., specie nelle conclusioni, pp. 149-151; Y. POULLET, *Les diverses techniques de réglementation d'Internet: l'autorégulation et le rôle du droit étatique*, in *Ubiquité*, 2000, p. 55 ss.

⁷ Significative in tal senso le parole di

3. LA SENTENZA *GOOGLE C. VIVIDOWN*.

Può essere di interesse, a questo punto, verificare in quale misura le teorizzazioni sopra sintetizzate si siano riverberate nella « filosofia » o nelle politiche aziendali di Google come ricostruibili dalla sentenza da cui prende spunto il presente convegno.

Nel corso della sua attività, la magistratura requirente è pervenuta, sulla base di corposo materiale probatorio, ai seguenti punti fermi fattuali.

Il primo aspetto riguarda la centralità della società madre (Google Inc., USA) rispetto alle società operanti in Europa. Tale assenza di un struttura societaria effettiva è stata accertata sia per l'Italia che per la Francia che per il Regno Unito e l'Irlanda, ove gli amministratori delle rispettive società (in Italia una s.r.l.!) erano gli stessi amministratori di Google Inc., e la delega si limitava alle sole operazioni bancarie. Insomma, tutto veniva gestito direttamente da Mountain View.

Il secondo aspetto attiene al completo disinteresse delle sede statunitense rispetto alle problematiche di tutela della privacy in Italia (o comunque in sede comunitaria) a seguito della entrata in vigore del « Codice della privacy » (D.Lgs. n. 196/2003) e al fatto che gli studi legali esterni non sono mai stati interpellati in proposito. Operando in 160 Paesi nel mondo, Google ritiene in sostanza impossibile conoscere le singole normative nazionali in tema di privacy, e ritiene di proporre un suo statuto di normativa globale⁸.

Ancora, nella motivazione della pronuncia si rimarca la totale e deliberata omissione di qualsiasi altra attività (anche di consulenza legale, attinenti alle questioni del diritto italiano o comunque comunitario) che potesse — in qualche modo — ostacolarne i profitti⁹. In buona sostanza, la pronuncia rileva l'assenza di qualsiasi interesse di Google al controllo e alla garanzia di conformità delle proprie politiche aziendali rispetto alla normativa di protezione delle privacy di matrice comunitaria.

Infine, un profilo marginale ma non trascurabile attiene al numero del tutto inadeguato degli addetti ai controlli manuali (in Italia, fra le 5 e le 10 persone) rispetto ad un colosso delle dimensioni di Google. Il controllo — si legge nella sentenza — si fonda essenzialmente sul sistema del « *flag in* » e sulle segnalazioni da parte degli utenti.

Philippe Quéau, Direttore della Divisione Informazione e Informatica dell'UNESCO: « - Les déséquilibres structurels de l'infrastructure mondiale d'Internet, les profondes inégalités de l'accès à l'information, les oligopoles transnationaux contrôlant l'infrastructure planétaire sont autant de sujets de préoccupation pour le régulateur. Une nouvelle

forme de régulation ou de "gouvernance" mondiale doit être conçue, dans une perspective éthique mondiale, au service de l'équité et du développement humain ».

⁸ Cfr. p. 58 della motivazione nella versione originale depositata (alla quale si riferiscono anche le citazioni successive).

⁹ Cfr. p. 52 della sentenza.

Ma lo snodo più significativo della pronuncia riguarda la qualificazione dell'attività dell'operatore professionale. Il discorso è stato sviluppato — dato il caso specifico — con riferimento a Google Video, ma potrebbe valere con riguardo a tutti quei soggetti (E-bay, Facebook ecc.) che aggregano dati la cui sommatoria rappresenta il valore aggiunto rispetto ai dati presi singolarmente di per sé.

3.1. *Mera intermediazione o fornitura di contenuti?*

Alle pp. 62 ss. la pronuncia spiega il funzionamento del sistema degli « Ad words » pubblicitari. Il sistema vale anche per Google Video.

La difesa di Google ha proposto la tesi dell'attività di mera intermediazione, per cui Google sarebbe solo il tramite tecnico attraverso il quale i creatori di contenuti diventano visibili (*User Generated Content Aggregator Service Provider*).

Detta tesi difensiva è stata scardinata dai P.M. e dalla pronuncia.

In particolare, è stata confutata la tesi difensiva della mera attività di intermediazione¹⁰. Ogni contenuto (anche video) immesso nel sistema va in realtà ad incrementare il patrimonio informativo della società. Ogni contenuto così immesso aumenta di conseguenza la possibilità di successo di un'inserzione e il correlativo profitto economico per il Provider.

Non si è quindi in presenza di un semplice *User Generated Content*.

I contenuti pubblicitari sono gestiti da Google e rappresentano il modo in cui questa produce enormi profitti.

Google è in realtà un *Content Provider*¹¹, il che taglia le gambe alle tesi difensiva della mera intermediazione (*Host provider*) sviluppata dalla difesa, con conseguente irresponsabilità in relazione ai contenuti (l'obbligo di acquisire il consenso avrebbe fatto capo a chi ha caricato il video incriminato).

3.2. *Il rapporto tra controllo automatico (di carattere tecnico) e « controllo sociale » da parte degli utenti.*

Le consulenze tecniche svolte nel corso del giudizio che ha condotto alla pronuncia che si commenta hanno evidenziato come non fosse presente neppure un'analisi testuale in base al titolo del video.

Strumenti più efficaci di controllo sono stati introdotti solo dopo che, con l'acquisizione di YouTube, Google ha eliminato il più temibile concorrente sul mercato.

¹⁰ Vedi p. 75 della motivazione.

¹¹ P. 76.

Secondo i magistrati requirenti, ciò che importa a Google è acquisire informazioni e proteggere le proprie, ma non proteggere la privacy altrui. La politica societaria è sintetizzata a p. 84 della sentenza: « *Prima copia/acquisisci, poi (eventualmente) cancella (sempre che lo imponga un Tribunale o che vi sia un business migliore a fare il contrario)* ».

3.3. *È configurabile un obbligo per il proprietario o per il gestore del sito Web (sia esso Host Provider, Access Provider, Service Provider o Content Provider) di adeguarsi ai dettami del regime di tutela dei dati personali?*

A mio avviso, a questo proposito poco vale la distinzione tra *Host Provider* e *Content Provider*.

Senza dubbio il *Content Provider* è in posizione più delicata, perché in qualche modo contribuisce a creare o comunque a far propri i dati dallo stesso gestiti. Ma anche l'*Host Provider* (e cioè il mero intermediario) non è esente dal comportamento di « trattamento », dal momento che egli diffonde i dati raccolti. Esso è responsabile nel momento in cui diventa un *Hoster attivo*¹².

Sul versante penalistico, la sentenza non è in grado di trarne le necessarie conseguenze a fronte del principio del divieto di analogia *in malam partem*. Si legge nella sentenza: « *Non esiste un obbligo di legge codificato che imponga ai Provider un controllo preventivo della innumerevole serie di dati che passano ogni secondo nelle maglie dei gestori o proprietari dei siti WEB, e non è possibile ricavarlo aliunde oltretutto superando il divieto di analogia in malam partem* ».

Al contempo, la pronuncia chiarisce come non costituisca condotta sufficiente ai fini che la legge impone quella di « nascondere » le informazioni sugli obblighi derivanti dal rispetto della normativa sulla privacy all'interno di « condizioni generali di servizio » il cui contenuto appare speso incomprensibile, sia per il tenore delle stesse che per le modalità con le quali vengono sottoposte all'accettazione dell'utente.

Tale comportamento, improntato all'esigenza di minimalismo contrattuale, e di scarsa volontà comunicativa, costituisce una specie di « precostituzione di alibi » da parte del soggetto/Web che non esclude una valutazione negativa della condotta tenuta nei confronti degli utenti¹³.

L'informativa sulla privacy, visualizzabile per l'utente dalla pagina iniziale del servizio « *Google video* » in sede di attivazione del-

¹² Cfr. p. 92 della sentenza.

¹³ Cfr. p. 96.

l'account al fine di porre in essere il caricamento di *files* da parte dell'utente medesimo, è stata valutata come del tutto carente, o comunque talmente « nascosta » da risultare assolutamente inefficace ai fini che la normativa si propone¹⁴. L'utente è infatti portato a pensare che si tratti dei suoi dati personali e non di quelli relativi a soggetti compaiono nel video.

Se ne ricava, secondo i P.M., « una chiara accettazione consapevole del rischio concreto di inserimento e divulgazione di dati — anche e soprattutto sensibili — che avrebbero dovuto essere oggetto di particolare tutela. Non solo, ma anche dell'interesse economico a tale accettazione del rischio e della chiara consapevolezza di quest'ultimo »¹⁵.

In realtà, attraverso il sistema delle « *ad words* » e il riconoscimento di parole chiave (finalizzato a quegli scopi pubblicitari che determinano il lucro del Provider) esiste la possibilità di controllare (gestire, indicizzare, organizzare) anche i dati contenuti nel sito che ospita i video generati dagli utenti.

3.4. *Le conclusioni della pronuncia Google c. Vividown.*

La conseguenza finale della pronuncia in questione è quella di sentenza ritenere sussistente il capo di imputazione *b*), e cioè l'illecito trattamento di dati personali.

Quanto al capo di imputazione *a*), e cioè a dire il concorso (congiuntamente con i soggetti che hanno caricato il video) nel reato di diffamazione, i magistrati requirenti hanno ricostruito un *obbligo preventivo di controllo dei contenuti* attraverso « filtri » che lo stato attuale della tecnologia consente, mentre all'opposto è risultato che Google attuava semplicemente un *controllo successivo* attraverso il sistema del « flag in » da parte della comunità degli utenti.

La sentenza, per parte sua, configura non un obbligo di controllo preventivo dei dati immessi nel sistema, bensì di corretta e puntuale informazione, da parte di chi accetti e apprenda dati provenienti da terzi, ai terzi che questi dati consegnano¹⁶.

Applicando il principio di divieto di analogia *in malam partem*, la sentenza esclude nel caso di specie che l'esistenza di un'adeguata informativa (in fase di « login » e di « upload ») circa la normativa sulla privacy avrebbe in modo certo impedito l'evento (diffamazione). Si motiva in proposito che l'obbligo del Provider di impedire l'evento diffamatorio imporrebbe allo stesso una *posizione di garanzia* e un controllo o filtro preventivo su tutti i dati immessi ogni secondo sulla Rete, causandone l'immediata impossibilità di funzionamento quantomeno allo stato attuale della tecnica¹⁷.

¹⁴ Cfr. p. 97.

¹⁵ Così a p. 98 della sentenza.

¹⁶ Cfr. p. 93.

¹⁷ V. p. 104 della sentenza.

Secondo la sentenza, si è in presenza di un comportamento « inesigibile » e quindi non perseguibile penalmente¹⁸. Si segnala peraltro¹⁹ la necessità di riempire la lacuna con un intervento normativo che configuri un'ipotesi di responsabilità penale per omesso controllo. Non è neppure escluso che a breve lo stato della tecnica consenta un simile genere di controllo preventivo.

4. BREVI RIFLESSIONI *DE JURE CONDENDO*.

Sulla base dei significativi spunti ricavabili dalla pronuncia e poc'anzi richiamati, è possibile svolgere alcune considerazioni *de jure condendo*. È bene precisare che queste ultime (i) in primo luogo riguardano il solo *coté* civilistico della materia, e (ii) in secondo luogo prescindono dalla attuale concreta disciplina di diritto positivo della responsabilità delle diverse categorie di Provider rinvenibile nel D.Lgs. 70/2003 sui servizi della società dell'informazione, meglio conosciuto come disciplina del commercio elettronico²⁰.

È ricorrente l'affermazione secondo la quale attribuire al Provider [che non sia meramente fornitore di accesso o puro intermediatore nella circolazione dei servizi della società dell'informazione] una posizione di *garanzia* produrrebbe una paralisi degli operatori professionali, che si troverebbero nell'impossibilità di proseguire la propria attività se non esponendosi al rischio di continue condanne.

Può allora presentare qualche utilità il confronto — già operato da altri nel passato — con almeno due settori nei quali tale posizione di garanzia è stata — normativamente o attraverso l'interpretazione giurisprudenziale — riconosciuta.

4.1. *Parallelo con la responsabilità da prodotto difettoso.*

Può essere di qualche utilità il confronto con la normativa in materia di responsabilità da prodotto difettoso [D.P.R. 224/1988²¹].

¹⁸ Cfr. p. 105.

¹⁹ *Ibidem*.

²⁰ Per un esaustivo commento del quale cfr. C. ROSSELLO-G. FINOCCHIARO-E. TOSI, *Commercio elettronico, documento informatico e firma digitale. La nuova disciplina* (nella collana « Lex nova » curata per i tipi di Giappichelli da E. ROPPO), Torino, 2003, pp. XIII, 738.

In particolare, sulla responsabilità del Provider e sulle diverse categorie individuate dal D.Lgs. in questione cfr. G. FACCI,

La responsabilità del provider, ivi, pp. 131 ss. (nonché ID., *La responsabilità dei Providers*, in C. ROSSELLO-G. FINOCCHIARO-E. TOSI (a cura di), *Commercio elettronico*, in *Trattato di Diritto Privato* diretto da M. Bessone, Torino, 2007, p. 233 ss., ove riferimenti bibliografici.

²¹ Per un sintetico commento v. C. ROSSELLO, *Responsabilità del produttore*, in ALPA e ZATTI (a cura di), *Commentario al codice civile, Leggi complementari*, Padova, 2003.

La responsabilità in capo al produttore è di tipo oggettivo, fondata sul principio del rischio, o in ogni caso una responsabilità professionale per colpa presunta, con inversione dell'onere della prova.

È nota la derivazione di stampo giuseconomico di tale responsabilità oggettiva, risalente alle prime storiche pronunce statunitensi degli anni '40 del secolo scorso. Il produttore è: (1) il *best risk avoider*, e cioè il soggetto meglio in grado di adottare le misure preventive di sicurezza (2) il *best risk insurer*, e cioè il soggetto meglio in grado di assicurare il rischio; (3) il *best risk (or loss) spreader*, colui che cioè è in grado di distribuire (spalmare) sulla collettività il costo degli incidenti.

D'altra parte, il carattere strettamente oggettivo (*strict liability*) della responsabilità del produttore è attenuato dall'esimente di cui all'art. 6, lett. e), del D.P.R. 224/1988, in base al quale il prodotto non può essere considerato difettoso « *se lo stato delle conoscenze scientifiche e tecniche, al momento in cui il produttore ha messo in circolazione il prodotto, non permetteva ancora di considerare il prodotto come difettoso* ». Anche in questo caso, la valutazione è quella relativa alla *praticabilità economica* delle misure tali da evitare il rischio.

Si effettua in altri termini un bilanciamento tra l'esigenza di non congelare e bloccare l'attività e la prescrizione deontologica di metter in atto tutte le misure di sicurezza non solo imposte normativamente, ma comunque consentite dallo stato della tecnica.

4.2. *Parallelo con la responsabilità da attività pericolose.*

Il trattamento di dati personali è assimilato dal Codice della Privacy all'attività pericolosa di cui all'art. 2050 cod. civ.

Anche in questo caso, può essere utile un sintetico parallelo.

Dapprima la norma è stata considerata in chiave di *colpa presunta*, laddove la prova liberatoria era integrata dalla dimostrazione di aver adottato tutte le misure idonee ad evitare il danno.

Tuttavia, la giurisprudenza applicativa ha sempre più mostrato la tendenza ad applicare in materia una valutazione *a posteriori*, tale da rendere la prova liberatoria una sorta di *probatio diabolica*, e da rendere l'art. 2050 cod. civ. una delle norme più rigorose in materia di responsabilità oggettiva o per *rischio di impresa*, in base al principio (risalente al diritto romano) del « *cuius commoda, eius et incommoda* ». La circostanza di non aver adottato tutte le misure di sicurezza idonee ad evitare il danno viene infatti sovente ricavata dalla giurisprudenza applicativa dal fatto stesso che il danno si sia verificato. La prova liberatoria viene fatta in sostanza fatta coincidere con il *caso fortuito*.

Ma anche in questa impostazione, la responsabilità è ulteriormente aggravata dalla distinzione tra « *fortuito interno* » (quello

connesso ai rischi in virtù dei quali l'attività è da considerarsi pericolosa) e c.d. «*fortuito esterno*» (quello cioè estraneo ai rischi connaturati all'attività pericolosa). Ad esempio, nel caso di esplosione di una nave cisterna in conseguenza di un fulmine, ciò che verrebbe da considerare quale «*Act of good*» in senso naturalistico viene invece ricondotto in termini giuridici fra quei rischi che vanno comunque addossati all'esercente l'attività pericolosa²².

Fortuito esterno sarebbe solo quello non governabile in termini di razionalità economica e neppure gestibile efficientemente sotto il profilo assicurativo (ad es. l'attacco terroristico o il fatto di guerra).

5. CRITICHE E POSSIBILI SOLUZIONI.

La dottrina che si è occupata dell'argomento ha escluso l'applicazione tanto del primo quanto del secondo paradigma di responsabilità quantomeno al Provider che non ha effettivo controllo sui contenuti immessi, pena la paralisi dell'attività o un eccessivo aumento dei costi per la Internet community.

Ma allora, è probabile che lo snodo cruciale stia proprio lì.

Il provider professionale che lucra ingenti profitti tramite la raccolta pubblicitaria è in grado di farlo proprio perché è tecnicamente in grado di offrire agli utenti una pubblicità profilata sulle loro preferenze — preferenze ricavate a loro volta dalle *queries* rivolte al motore di ricerca — e di abbinare determinati contenuti pubblicitari ai contenuti di quanto «ospitato» sul sito.

È difficile, in questa ipotesi, esprimersi in termini di attività di *mera intermediazione*, e si scolora sensibilmente nella figura del fornitore di contenuti.

I cicli storici della responsabilità civile stanno a dimostrare che quando certe categorie di attività si sono evolute (in un sistema di capitalismo maturo) tanto da poter sopportare le esternalità negative generate, il sistema giuridico si è evoluto di conseguenza. Si è in altri termini trascorsi da una responsabilità fondata esclusivamente sulla colpa, a modelli di colpa professionale presunta — con conseguente inversione dell'onere probatorio — quando non a responsabilità rigorosamente oggettiva. Ciò è avvenuto dapprima in relazione al rischio di impresa, poi con riguardo ai danni circolazione stradale, poi ancora per il danno da prodotto difettoso.

²² Cfr. C. ROSSELLO, *Stato attuale (ed effettive conseguenze) dell'evoluzione giurisprudenziale in materia di danno da attività pericolose*, in *Dir. mar.*, 1985, pp. 853-889 a commento del lodo

arbitrale 16 agosto 1984 reso nel caso «*M/V Hakuyoh Maru*». Nel caso specifico si trattava dello scoppio di una nave cisterna avvenuto in conseguenza di un fulmine.

Viene allora da domandarsi se i larghi margini di profitto in oggi lucrati dagli operatori dei servizi della società dell'informazione non consentano di applicare modelli di responsabilità che « spalmino » sulla collettività — anche attraverso lo strumento assicurativo — i costi sociali che inevitabilmente si riconnettono alle esternalità negative ingenerate da tali servizi, anziché addossare l'intero pregiudizio al singolo danneggiato.

In fondo si tratta di applicare il vecchio principio « *cuius commoda, eius et incommoda* », o se si preferisce la formulazione più recente risalente alla codificazione napoleonica, « *ubi emolumentum, ibi onus* ».

La responsabilità in termini di *responsabilità professionale qualificata per colpa presunta* potrebbe in questo caso essere imputata al *Content Provider* (nel senso appena esplicato) quanto meno nelle ipotesi in cui risulti dimostrato che — attraverso mezzi di controllo consentiti dallo stato attuale della tecnica — esso avrebbe potuto evitare il danno.

La responsabilità sarebbe poi ovviamente imputata a titolo di colpa quando — nonostante le segnalazioni di illiceità provenienti dall'utenza — il Provider non sia immediatamente intervenuto a rimuovere i contenuti denunciati.

6. CONCLUSIONI.

Un regime di questo genere non pare — a mio avviso — così assurdo e scardinante in linea di principio.

Intanto, la responsabilità (civile o penale) dell'autore materiale dell'illecito dovrebbe rappresentare un deterrente abbastanza efficace rispetto al proliferare di illeciti commessi via Internet.

L'utente andrebbe a tal fine adeguatamente identificato (al di là dell'uso di *nick names* o *avatar*), in modo da poterlo rintracciare in caso di illeciti.

Inoltre, l'utente va adeguatamente avvisato che, con il caricare determinati contenuti sul server, rischia di incorrere in responsabilità.

Una volta che il Provider sia tenuto corresponsabile degli illeciti perpetrati dagli utenti (*ex art. 2055 cod. civ.*), è certo che si attiverà (nel suo proprio interesse) sia per l'identificazione che per fornire un simile avviso nella maniera più adeguata e « *smart* » a farne un efficace deterrente.

In secondo luogo, la responsabilità dovrebbe scattare solo quando: (1) sia accertata la materiale (e tecnica) possibilità di un controllo, in base allo « stato dell'arte », oppure (2) in caso di omesso tempestivo intervento nonostante la segnalazione dell'illecito.

Per finire, occorre prestare attenzione a non mettersi fuori gioco da soli rispetto alla globalità della Rete. È infatti persino

troppo evidente come un regime di responsabilità alternativo a quello attuale può essere messo in opera solo a condizione che esso sia concertato e uniforme per una nutrita serie di Paesi (quanto meno a livello di Unione Europea). Diversamente, il rischio è quello di rimanere « tagliati fuori » dalla Rete e dai suoi innegabili benefici.

Per concludere, vi è materia per lavorare — a livello comunitario e non certo nazionale — per un nuovo statuto della responsabilità del Provider.