IAIC MiBACT DGBIC CREDA

DIRITTO MERCATO TECNOLOGIA

FONDATA E DIRETTA DA
Alberto M. Gambino

COMITATO DI DIREZIONE
Valeria Falce, Giusella Finocchiaro, Oreste Pollicino,
Giorgio Resta, Salvatore Sica

10 settembre 2019

Anonimato in rete e responsabilità civile dell'*hosting provider* nella prospettiva *de jure condendo*

Giovanna D'Alfonso

Nuova Editrice Universitaria

La rivista è stata fondata nel 2009 da Alberto M. Gambino ed è oggi pubblicata dall'Accademia Italiana del Codice di Internet (IAIC) sotto gli auspici del Ministero dei beni e delle attività culturali e del turismo - Direzione generale biblioteche e istituti culturali (DGBIC) e dell'Università Europea di Roma con il Centro di Ricerca di Eccellenza del Diritto d'Autore (CREDA).

Norme di autodisciplina

1. La pubblicazione dei contributi sulla rivista "Diritto Mercato Tecnologia" è subordinata alla presentazione da parte di almeno un membro del Comitato di Direzione o del Comitato Scientifico e al giudizio positivo di almeno un membro del Comitato per la Valutazione Scientifica, scelto per rotazione all'interno del medesimo, tenuto conto dell'area tematica del contributo. I contributi in lingua diversa dall'italiano potranno essere affidati per il referaggio ai componenti del Comitato Scientifico Internazionale. In caso di pareri contrastanti il Comitato di Direzione assume la responsabilità circa la pubblicazione.
2. Il singolo contributo è inviato al valutatore senza notizia dell'identità dell'autore.
3. L'identità del valutatore è coperta da anonimato.
4. Nel caso che il valutatore esprima un giudizio positivo condizionato a revisione o modifica del contributo, il Comitato di Direzione autorizza la pubblicazione solo a seguito dell'adeguamento del saggio.

La Rivista adotta un Codice etico e di buone prassi della pubblicazione scientifica conforme agli standard elaborati dal Committee on Publication Ethics (COPE): Best Practice Guidelines for Journal Editors.

Sede della Redazione

Accademia Italiana del Codice di Internet, Via dei Tre Orologi 14/a, 00197 Roma, tel. 06.8088855, fax 06.8070483, www.iaic.it, info@iaic.it

Anonimato in rete e responsabilità civile dell'*hosting provider* nella prospettiva *de jure condendo*

Giovanna D'Alfonso
Università degli Studi della Campania "Luigi Vanvitelli"

Sommario: 1. Inquadramento della problematica – 2. Il riconoscimento del diritto all'anonimato in rete nel sistema statunitense – 3. L'anonimato in rete in ambito europeo. Il riconoscimento del diritto all'anonimato in rete in Germania – 4. Le limitazioni alla tutela dell'anonimato in rete nell'ordinamento italiano – 5. La figura "atipica" dell'*hosting provider* «attivo» – 6. La responsabilità civile dell'*hosting provider* «attivo» per i contenuti illeciti pubblicati sulla piattaforma digitale da utenti del servizio anonimi o che si esprimano con pseudonimo – 7. Prospettive *de jure condendo*

1. Inquadramento della problematica

Difficile è la configurabilità della responsabilità civile dell'*hosting provider* per i danni arrecati a terzi da contenuti illeciti pubblicati, sul portale da costui gestito, da utenti del servizio in modo anonimo o con pseudonimo.

Si osservi, in via preliminare, che diverse sono le prassi degli *hosting providers*[1], relative alla gestione dell'identità dei fruitori del servizio. Mentre

[1] La direttiva del Parlamento e del Consiglio europeo dell'8 giugno 2000, n. 31, «relativa a taluni aspetti giuridici della società dell'informazione, in particolare il commercio elettronico, nel mercato interno», c.d. «direttiva sul commercio elettronico», nel regolamentare, agli artt. 12-16, la responsabilità civile degli *internet service providers* - ossia i prestatori che, operando nella società dell'informazione, offrono liberamente servizi di connessione, trasmissione e memorizzazione di dati-, li ha classificati in tre categorie, prevedendo distinti regimi di responsabilità. Più precisamente la direttiva ha qualificato la posizione giuridica del *mere conduite provider* (art. 12) che svolge l'attività di («semplice trasporto») fornire l'accesso alla rete o di trasmettere su una rete di comunicazione informazioni, date dal destinatario del servizio; la figura del *caching provider* (*ex* art. 13) che, nell'eseguire la funzione di trasmissione su una rete di

talune piattaforme digitali (quali *Airbnb*) prevedono, ai fini della pubblicazione di contenuti, la previa autenticazione del loro autore, richiedendo un documento d'identità e verificandone la veridicità; diversamente, altri portali – quali *TripAdvisor*, sito che ospita recensioni su strutture recettive, ed il più famoso *social network*, *Facebook*- consentono ad ogni utente di registrare anche più di un *account*, essendo, a tal fine, sufficiente la disponibilità di più indirizzi *e mail* e la modifica delle credenziali, senza controllare la veridicità delle generalità fornite per iscriversi al sito.

Il problema si pone allorchè il soggetto offeso non sia in grado di identificare l'autore del contenuto illecito, in quanto anonimo o che abbia agito con pseudonimo, neanche con la collaborazione dell'*hosting provider* che gli fornisca i dati che abbia raccolto ed abbia a sua disposizione. Pertanto l'unica via percorribile, ai fini del ristoro della situazione soggettiva lesa, sarebbe l'esperimento dell'azione legale contro quest'ultimo.

Cio' detto, si intende qui esaminare se il nostro sistema giuridico avvalori la pretesa del terzo danneggiato nei confronti di codesto legittimato passivo.

Al fine di rispondere alla domanda occorre dapprima analizzare la questione del riconoscimento, all'interno del nostro ordinamento giuridico,

---

comunicazione di informazioni fornite dall'utente del servizio, svolge una memorizzazione automatica, intermedia e temporanea, al solo fine di rendere i dati immediatamente disponibili per il recupero che l'utente ne voglia effettuare; infine la figura dell'*hosting provider* (*ex* art. 14) che si obbliga a locare uno spazio di memoria sul proprio *server* e fornisce, su tale spazio, la specifica attività di memorizzazione duratura delle informazioni provenienti dai destinatari del servizio. Per un commento all'articolata disciplina della responsabilità civile delle tre distinte figure di *Internet service providers* si v., *ex multis*, tra i primi approfonditi commenti, G.M. Riccio, *La responsabilità civile degli* internet service providers, Torino, 2002, p. 57 ss.; G. Ponzanelli, *Verso un diritto uniforme per la responsabilità degli* internet service providers, in *Danno e resp*., 2002, p. 5 ss.; V. Zeno Zencovich, *Profili attivi e passivi della responsabilità dell'utente in* Internet, in A. Palazzo-U. Ruffolo (a cura di), *La tutela del navigatore,* Milano, 2002, p. 195 ss.; F. Di Ciommo, *Evoluzione tecnologica e regole di responsabilità civile,* Napoli, 2003, *passim*; R. Bocchini, *La responsabilità civile degli intermediari del commercio elettronico. Contributo allo studio dell'illecito plurisoggettivo permanente,* Napoli, 2003, *passim*; M. Gambini, *La responsabilità civile dell'*internet service provider, Napoli, 2006, *passim;* A. Mantelero, *La responsabilità degli intermediari di rete nella giurisprudenza italiana alla luce del modello statunitense e di quello comunitario*, in *Contr.Impr. Europa, 2*010, p. 529 ss.

del diritto all'anonimato in rete e, di seguito, appurare se l'*hosting provider* sia legittimato a permettere ai fruitori del servizio di esprimersi sulla piattaforma digitale in maniera anonima o impiegando uno pseudonimo.

Problematica ad essa correlata è se, pur non ravvisandosi un fondamento normativo del diritto all'anonimato in rete, riconoscendo tuttavia (solo entro i limiti che si andranno a descrivere) la liceità del comportamento dei fruitori del servizio che interagiscano in rete anonimamente o con pseudonimo[2], sia comunque obbligo dell'*hosting provider* raccogliere e conservare le generalità di questi ultimi, prima di autorizzarli a pubblicare sulla piattaforma digitale. Dal riconoscimento di questo obbligo deriverebbe che la vittima dell'illecito potrebbe ottenere da parte dell'*hosting provider*, su ordine dell'autorità giudiziaria, l'ostensione dei dati identificativi dell'autore anonimo del contenuto pubblicato. Tale obbligo professionale discenderebbe dalla spinta ordinamentale di assicurare il diritto dei terzi lesi alla tutela giurisdizionale effettiva della propria posizione soggettiva, a fronte della salvaguardia della libertà di espressione, del diritto alla riservatezza e del diritto alla protezione dei dati personali degli internauti[3].

Infine, bisogna constatare se, laddove il *provider* non reperisca le generalità del destinatario del servizio, sussista in capo a costui la

[2] Attenta dottrina (G. Resta, *Anonimato, responsabilità, identificazione: prospettive di diritto comparato,* in *Dir. Informaz. e informatica,* 2014, p. 171) si pone il quesito sulla liceità del ricorso all'anonimato ovvero a pseudonimi, nell'ambito delle attività in rete, chiarendo l'importanza della questione, dal momento che la tendenza nei diversi ordinamenti giuridici è varia e la soluzione dipende non solo da interventi normativi formali, ma anche da norme sociali e prassi contrattuali. Sul tema si v. S. Rodotà (*Il mondo nella rete. Quali diritti, quali vincoli,* Roma, 2014, p. 23) che ha autorevolmente sottolineato il valore generale dell'anonimato e dello pseudonimo in rete, sostenendo che solo esprimendo il pensiero senza essere identificati è possibile essere liberi da limitazioni, da discriminazioni e da qualunque forma di censura. Si v. G. Finocchiaro (voce «*Anonimato*», in *Dig.disc.priv., sez. civ., Aggiornamento*, V, Torino, 2010, p. 13 ss.) ha precisato come l'anonimato costituisca il migliore strumento per proteggere la riservatezza ed i dati personali. Si v. V. Zeno Zenkovich, *Anonymous Speech on the internet*, in A. Koltay (a cura di), *The fundamentals of European Thought on Media Law,* Budapest, 2014, p. 103 ss. che procede ad un'attenta disamina di diritto comparato sul riconoscimentro giuridico del diritto all'anonimato in rete.

[3] Si v. G. Resta (*Anonimato, responsabilità, identificazione, op.cit.,* p. 180, (§ 4.1.)) che sottolinea come il contemperamento dei contrapposti interessi debba avvenire in sede giudiziaria.

responsabilità civile per aver, con la propria condotta omissiva di mancata autenticazione dell'autore del contenuto pubblicato sul portale, facilitato/favorito l'illecito altrui[4].

E' opportuno sottolineare che, seppure la tematica sia, da tempo, oggetto di attente disamine dottrinali[5], offre, di recente, interessanti spunti di riflessione, giacchè, a fronte dell'assenza, a livello europeo, sia di un divieto generale all'anonimato in rete, sia dell'imposizione normativa, in capo ai fornitori del servizio, di un obbligo generale di identificazione dei fruitori delle piattaforme digitali, si assiste all'evoluzione dell'orientamento politico che persegue l'obiettivo della maggiore responsabilizzazione degli *internet service providers*.

In taluni Stati membri[6], sono difatti stati emanati disegni di legge che impongono ai prestatori di servizi *on line* l'identificazione degli utenti degli stessi, con la previsione dell'irrogazione di sanzioni, nei casi di inottemperanza.

Inoltre le Istituzioni Europee hanno emanato una serie di atti di *soft law*[7], con i quali incoraggiano l'adozione da parte degli *internet service providers* di «qualunque misura» proattiva, mirante a contrastare i contenuti illegali *on line*, purchè soggetta a garanzie effettive e appropriate che assicurino un comportamento diligente e proporzionato da parte degli stessi.

---

[4] Secondo quanto sostenuto da G. M. Riccio, *Anonimato e responsabilità in* internet, in *Dir.inform. e informatica,* 2000, pp. 325, 331.

[5] *Ex multis,* si v. G.M. Riccio, *Anonimato e responsabilità in* internet, *op.cit*., p. 325 ss.; Id., *Diritto all'anonimato e responsabilità civile del provider,* in L. Nivarra- V. Ricciuto (a cura di), *Internet e il diritto dei privati*, Torino, 2002, p. 27 ss.; R. Natoli, *La tutela dell'onore e della reputazione in* internet*: il caso della diffamazione anonima*, in *Eur.dir.priv.*, 2001, p. 440 ss; M. Manetti, *Libertà di pensiero e anonimato in rete,* in *Dir. dell'informaz. e informatica*, 2014, p. 139 ss.; G. E. Vigevani, *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano*, in *Dir. dell'informaz. e informatica*, 2014, p. 207 ss. Si v., in particolare, G. Resta, *Anonimato, responsabilità, identificazione: prospettive di diritto comparato, op.cit.,* p. 171 ss. il quale, dopo aver analizzato la questione della liceità dell'uso dell'anonimato o dello pseudonomo, nel contesto delle attività *online*, si domanda chi debba rispondere degli illeciti commessi in forma anonima, incentrando l'attenzione su quali siano gli strumenti della vittima dell'illecito, al fine di ottenere da parte del *provider* l'ostensione dei dati identificativi dell'autore del contenuto anonimo.

[6] Si v. § 7.

[7] Si v. § 7.

Alla luce delle considerazioni che si svolgeranno, si avanzerà l'opportunità di introdurre, tra le misure proattive, la "misura precauzionale" dell'identificazione dell'utente del portale, prima di permettergli l'accesso allo stesso.

2.Il riconoscimento del diritto all'anonimato in rete nel sistema statunitense

Seguendo il percorso logico descritto, si precisi innanzitutto che l'anonimato presenta indubbi vantaggi in rete che, caratterizzandosi per l'assenza di limiti, l'immediatezza e l'economicità, assurge a luogo quanto più libero di circolazione di idee ed informazioni -tant'è vero che è comunemente definita «*marketplace of ideas*»-[8], giacché tutela la libertà di manifestazione del pensiero[9], la *privacy* degli internauti e, in senso più ampio, la libera esplicazione della personalità umana, ai sensi dell'art. 2 Cost., proteggendo l'individuo dai rischi di censure. Ciò vale sia per il singolo, sia per i gruppi che si formino in rete, al fine di manifestare critiche, reclamare pretese, partecipare al dibattito pubblico - circostanza che assume preminente valenza, quando si tratti di minoranze etniche, di genere, sociali, etc.[10]

[8] Si v. M. Manetti, *Libertà di pensiero e anonimato in rete*, *op.cit.*, p. 142 (§ 2).

[9] La dottrina puntualizza come il significato della libertà di manifestazione del pensiero, il cui fondamento costituzionale è nell'art. 21, assuma in *internet* nuove implicazioni d'ordine giuridico. Si v. V. Zeno Zenkovich *La libertà di espressione. Media, mercato, potere nella società dell'informazione,* Bologna, 2004, p. 125 ss.; T. E. Frosini (*Il diritto costituzionale di accesso in internet*, in www.rivistaaic.it, 2011, fasc. 1, p. 6), il quale precisa (Id., *Il diritto costituzionale di accesso, op.cit*., p. 8 ss.) come l'esplicarsi della libertà di espressione sia strettamente correlata al diritto di accesso a *Internet*, da qualificarsi come «diritto sociale», ossia una pretesa soggettiva nei confronti delle istituzioni nazionali al servizio universale di *internet* che deve essere garantito a tutti i cittadini, al pari dell'istruzione, della sanità e della previdenza. Sul tema cfr. anche T.E. Frosini, *Il diritto di accesso in* internet, in T.E. Frosini - O. Pollicino - E. Apa - M. Bassini (a cura di) *Diritti e libertà in* internet, *Le Monnier* Università, Milano, 2017, p. 41 ss.

[10] Sul punto si v. G. Resta, *Anonimato, responsabilità, identificazione: prospettive di diritto comparato*, *op.cit.,* p. 174 (§ 2.1.) Sul diritto all'anonimato e l'ostensione dei nomi degli appartenenti a gruppi politici, soprattutto di minoranza, si v. G. M. Riccio, *Diritto all'anonimato e responsabilità civile del provider, op.cit*., p. 27 ss.

Vi sono sistemi giuridici, come quello statunitense, che si caratterizza per la sua «strategia ipeliberista»[11], che hanno valorizzato l'anonimato in rete, pur predisponendo strumenti di tutela effettiva a favore di chi venga danneggiato da un soggetto non identificabile.

In particolare la giurisprudenza statunitense ha dapprima percepito, in linea generale, la scelta di un soggetto di rimanere anonimo come aspetto proprio della libertà di espressione, tutelata nel Primo Emendamento della Costituzione (*the First Amendament's freedom of speech*), per riconoscere successivamente il fondamento costituzionale del diritto di manifestare il pensiero in forma anonima anche in *internet* e configurare la compressione dell'anonimato in rete come una violazione della garanzia costituzionale[12]. La giurisprudenza statunitense persegue così il fine di scongiurare il pericolo che si realizzino i paventati *chilling effects*, c.d. effetti del raffreddamento della rete, quale *marketplace of ideas,* che deriverebbero da restrizioni stringenti del ricorso all'anonimato[13].

In tale cornice, non essendovi dubbio sulla liceità dell'anonimato in rete, in assenza di un'imposizione legislativa che imponga agli *Internet service providers* la previa identificazione dell'utente della piattaforma digitale, spetta unicamente all'autorità giudiziaria raggiungere un punto di equilibrio tra l'aspirazione ad apprestare una tutela rafforzata all'interesse all'anonimato, ispirandosi alla logica del *First Amendament,* e l'esigenza di assicurare alle vittime di contenuti illeciti efficaci strumenti di tutela[14].

Tale funzione è assolta precipuamente quando il soggetto danneggiato esperisca l'azione civile avverso il convenuto ignoto[15]. Codesto strumento

---

[11] Si riferisce all'esperienza statunitense in tali termini, R. Natoli, *La tutela dell'onore e della reputazione in* internet*, op.cit.,* p. 440, 456 s.

[12] Si v. G. Resta, *Anonimato, responsabilità, identificazione: prospettive di diritto comparato*, *op.cit.,*, p. 174 (§ 2.1.); M. Manetti, *Libertà di pensiero e anonimato in rete*, *op.cit.*, p. 143 (§ 2).

[13] Si v. R. Natoli, *La tutela dell'onore e della reputazione in* internet*, op.cit.,* p. 443, il quale approfondisce (Id., *ivi*, p. 447 ss.) l'itinerario legislativo e giurisprudenziale statunitense in tale ambito.

[14] Si v. G. Resta, *Anonimato, responsabilità, identificazione: prospettive di diritto comparato*, *op.cit.,* p. 180 (§ 4.1.).

[15] Per le considerazioni che seguono si v. G. Resta, *Anonimato, responsabilità, identificazione: prospettive di diritto comparato*, *op.cit.,* p. 180 ss. (§ 4.1.)

processuale è proprio degli ordinamenti di *common law* e si è diffuso, sin dal 1848, con il *Code of Civil Procedure* di New York; dopo alterne vicende, i casi di *anonymous litigations* sono aumentati notevolmente, a seguito dell'avvento di *internet*. Qualora l'illecito sia compiuto in forma anonima, il soggetto leso è legittimato ad esperire l'azione contro il convenuto ignoto, rimettendosi ai rimedi processuali ordinari che servano alla sua identificazione, nel corso del contenzioso. Dal punto di vista tecnico, ciò si realizza con lo strumento del *writ of subpoena*, regolamentato dalla *rule 45* delle *Federal Rules of Civil procedure*, con il quale l'autorità giudiziaria intima un terzo soggetto, *non party-witness*, a prestare testimonianza ovvero a fornire documenti rilevanti per la controversia. Nel caso di illecito commesso sul *web*, tale ordine si struttura in duplice fase: in *primis*, si ingiunge all'*internet service provider* di comunicare all'attore l'*IP* dinamico dell'autore della lesione; dopo ci si rivolge all'*access provider*, per acquisire i dati anagrafici dell'intestatario della connessione che corrisponda a tale indirizzo *IP*.

Si puntualizzi che, non essendovi una previsione generale sul modo in cui le corti debbano contemperare tali due contrapposti interessi, la giurisprudenza ha sviluppato criteri cui uniformarsi[16].

Si consideri, in via conclusiva, che la decisione giudiziale dipenderà poi dalle peculiarità del sistema ordinamentale dello Stato confederato degli Stati Uniti d'America, il cui foro sia competente per la controversia. A titolo esplicativo, di peculiare interesse è la sentenza della *Court of Appeal,*

[16] In riferimento al vaglio giudiziale della concessione dell'ordine di *disclosure* dei dati identificativi dell'autore di una presunta diffamazione in rete, numerose pronunce giurisprudenziali hanno elaborato un *test*, stabilendo che, ai fini della prosecuzione della causa giudiziale, debbano essere soddisfatte quattro condizioni: innanzitutto chi si senta diffamato deve contestare il fatto all'autore del messaggio, preferibilmente nel medesimo portale in cui sia stato pubblicato; in secondo luogo, l'attore deve indicare esattamente le affermazioni ritenute lesive, collegandole a ciascun *post* anonimo; in aggiunta, colui che sia incolpato deve avere la possibilità di difendersi dalla richiesta di identificazione; l'attore deve infine provare l'esistenza della fondatezza della pretesa della propria domanda, allegando prove. Il *test*, seppure non univoco, è significativo, in quanto indicativo del *trend* giurisprudenziale di porre limiti ad azioni miranti all'identificazione di autori di affermazioni anonime, al solo fine di scoraggiare, con la minaccia di una causa onerosa, critiche anonime o di effettuare rivalse verso gli stessi. Sul punto si v. M. Manetti, *Libertà di pensiero e anonimato in rete*, *op.cit.,* p. 145 ss. (§ 3).

Second District, Division 1, California, 14 maggio 2014, nel caso *Digital Music News LLC*, *Petitioner, v. Superior Court of Los Angeles County, Respondent; Escape Media Group, LLC, Real Party in Interest*[17]. La Corte si è pronunciata su una richiesta di disvelamento dell'identità di un internauta, effettuata da parte della società *Escape Media Group,* proprietaria di *Grooveshark*, un servizio *on line* che permette di caricare, condividere, scaricare e riprodurre in *streaming file* musicali. La società, citata in giudizio, innanzi al Tribunale di New York da *UMG Recordings*, etichetta discografica che le ha contestato di stimolare gli utenti e gli impiegati a caricare *file* musicali che violino il *copyright*, ha, a sua volta, citato in giudizio la società *Digital Music News*, con sede in California, che gestisce un sito dedicato ai resoconti sull'industria musicale, al fine di ottenere l'ostensione dei dati identificativi di un commentatore anonimo che, utilizzando lo pseudonimo "visitatore", ha postato sul sito due commenti, sostenendo di essere un impiegato di *Grooveshark* e che i suoi dirigenti gli avevano richiesto di caricare un contenuto che violava il *copyright*. La richiesta è stata dettata dall'esigenza di identificare il commentatore anonimo, dal momento che tali dichiarazioni avrebbero potuto pregiudicare la posizione giudiziale di *Escape*, nella controversia con *UMG Recordings*. Essendosi la società *Digital Music News* rifiutata di comunicare le generalità dell'autore anonimo delle affermazioni potenzialmente pregiudizievoli per *Escape*, quest'ultima ha presentato ricorso alla Corte Suprema di Los Angeles.

La Corte ha negato l'ordine di rivelazione dell'identità dell'utente, affermando che il diritto di esprimersi in maniera anonima trae fondamento non solo nel primo Emendamento della Costituzione degli Stati Uniti d'America che riconosce e garantisce la libertà di espressione, ma anche nel diritto alla *privacy* dell'utente delle piattaforme digitali, garantito dall'art. 1, sez. I della Costituzione della California. In sostanza, l'autorità giudiziaria, nell'operazione di bilanciamento tra l'interesse della società *Escape*, potenzialmente offesa dalle dichiarazioni anonime, alla tutela giudiziaria dei

[17] Decisione B242700 pubblicata in https://caselaw.findlaw.com/ca-court-of-appeal/1666563.html. Per le note di commento alla pronuncia che seguono si v. D. Arcuti, *Diritto all'anonimato: libertà di espressione e/o tutela della riservatezza?, i*n https://medium.com, 18 gennaio 2017.

propri diritti, da un lato, e l'interesse sotteso alla posizione soggettiva del "visitatore", dall'altro, ha valorizzato non solo l'interesse di quest'ultimo ad esprimersi in modo anonimo, ma anche il suo diritto alla *privacy*, sostenendo che l'esigenza di tutela dell'utente del servizio dovesse prevalere sull'interesse dell'attore, non essendo l'identità del primo essenziale, ai fini della tutela della posizione giudiziale del secondo nella controversia in atto tra *Escape* e la società *UMG*.

3. L'anonimato in rete in ambito europeo. Il riconoscimento del diritto all'anonimato in rete in Germania

In ambito europeo, le Istituzioni hanno rinvenuto il duplice fondamento del 'principio' dell'anonimato nella tutela sia della libertà di espressione, sia della *privacy*[18], per poi affermare, in più occasioni, che l'anonimato costituisce il migliore strumento per proteggere la riservatezza ed i dati personali[19].

[18] Il duplice fondamento è chiaramente espresso nella Dichiarazione del Comitato dei Ministri del Consiglio d'Europeo del 28 maggio 2003. Sul punto si v. G. Resta, *Anonimato, responsabilità, identificazione, op.cit.,* p. 176, nt. 41 (§ 2.2.). Precisa che tali due basi teoriche non sono esclusive, ma convergenti, G. Spindler, *Persönlichkeitsschutz im Internet- Anforderungen und Grenzen einer Regulierung,* in *Verhandlungen des 69. Deutschen Juristentages*, *Band* I, München, 2012, *Gutachten* F, p. 33.

[19] Si v., in particolare, il considerando 9 della direttiva 2002/58/CE del 12 luglio 2002 del Parlamento europeo e del Consiglio, relativa al trattamento dei dati personali e alla tutela della vita privata nelle comunicazioni elettroniche, già modificata nel 2009 dalla Direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 ed, allo stato attuale, oggetto di riforma. Sul punto G. Finocchiaro, voce «*Anonimato*», in *Dig.disc.priv., sez. civ., Aggiornamento*, V, Torino, 2010, p. 13, nt. 6. D'altronde, negli anni Cinquanta, la dottrina italiana riconduceva il diritto all'anonimato al diritto alla riservatezza, si v. A. Candian, voce «*Anonimato (ditto all')*», in *Enc.dir*., II, Milano, 1985, p. 499 ss. Sull'evoluzione dal diritto alla riservatezza, da intendersi come il diritto ad essere lasciati soli e a respingere le interferenze nella sfera privata dell'individuo, al diritto alla protezione dei dati personali, quale diritto al controllo sulla circolazione dei dati personali, si v., negli anni Settanta, S. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, p. 130. Le linee di elaborazione di tale riflessione si trovano già in P. Perlingieri, *La personalità umana nell'ordinamento giuridico*, Camerino-Napoli, 1972, *passim;* V. Zeno Zencovich, *I diritti della personalità*, in N. Lipari- P. Rescigno (a cura di), *Diritto civile*, I, Milano, 2009, p. 495 ss. Sul tema *amplius* si v. V. Cuffaro, *Il*

Tali fondamenti hanno permeato, sin dalla prima regolamentazione, la disciplina europea della protezione dei dati personali[20], in una duplice direzione: sia delimitando l'ambito oggettivo di applicazione ai soli dati personali, riferibili ad un soggetto identificato o identificabile, e quindi escludendo i dati anonimi[21]; sia ponendosi quale principio generale, in base al quale plasmare l'attività di trattamento dei dati personali. Sul punto si precisi[22] che il legislatore europeo, se, sin dagli esordi della regolamentazione della tematica, esorta i titolari ed i responsabili del trattamento dei dati personali all'attuazione di tecniche di anonimizzazione, nello svolgimento dell'attività di raccolta ed utilizzazione degli stessi[23], al fine di tutelare i dati personali e garantire la riservatezza degli individui; il Regolamento generale sulla *privacy*, di recente emanazione, allo stesso scopo, incoraggia l'impiego della tecnica della «pseudonimizzazione»[24].

---

diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia: elementi per un bilancio ventennale, in V. Cuffaro- R. D'Orazio- V. Ricciuto (a cura di), *I dati personali nel diritto europeo,* Torino, 2018, p. 3 ss.

[20] Sin dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla loro libera circolazione; disciplina abrogata dal Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, entrato in vigore negli Stati membri il 25 maggio 2018 (c.d. Regolamento generale sulla *privacy*). Per un approfondito commento della disciplina attualmente vigente, si v. V. Cuffaro -R. D'Orazio- V. Ricciuto (a cura di). *I dati personali nel diritto europeo*, *op.cit, passim*.

[21] Si v. G. Resta, *Anonimato, responsabilità, identificazione, op.cit.,* p. 177 (§ 2.2.) Secondo quanto previsto dal Considerando 28 del Regolamento generale sulla *privacy,* la disciplina europea sulla protezione dei dati personali non si applica ad informazioni anonime che non si riferiscano ad una persona fisica identificata o identificabile o a dati personali, resi sufficientemente anonimi da impedire o da non consentire più l'identificazione del soggetto interessato. Inoltre, il 28 maggio 2019 è entrato in vigore il Regolamento 1807/2018/UE del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea*,* nel cui ambito di applicazione rientrano, quale esempio specifico di dati non personali, gli insiemi di dati aggregati e anonimizzati usati per l'analisi dei megadati.

[22] Si v. G. Resta, *Anonimato, responsabilità, identificazione, op.cit.,* p. 177, nt. 44 (§ 2.2.).

[23] E pertanto a ridurre al minimo l'utilizzazione di dati personali, escludendone il trattamento, quando le finalità dello stesso possano realizzarsi per mezzo di dati anonimi oppure identificando l'interessato, solo in casi di necessità.

[24] Per «pseudonimizzazione» si intende il trattamento che si colloca "a metà" tra quello concernente i dati personali e quello relativo ai dati anonimi. Il dato pseudonimizzato è un dato reso anonimo in via transitoria, operando uno smembramento di talune

L'impulso legislativo verso l'anonimizzazione dei dati personali assume particolare valenza nei rapporti tra gestori ed utenti delle piattaforme digitali[25], nella misura in cui la decisione dei primi di autorizzare gli utenti a comunicare *on line,* mantenendo l'anonimato o utilizzando pseudonimi, avrebbe l'effetto di assicurare loro il controllo sulla propria identità digitale[26], dando così attuazione al diritto alla protezione dei dati personali[27].

Per tale via il ricorso all'anonimato in rete è lecito, coerentemente alla configurazione dell'anonimato (in senso ampio) quale «una modalità estrema di esercizio del diritto alla protezione dei dati personali»[28].

Tale asserzione è valida in ambito nazionale, ove, da più di un ventennio, si applica la disciplina europea sulla protezione dei dati personali, il cui referente normativo è, dal settembre 2019, il d. lgs. 10 agosto 2018, n. 101, volto ad adeguare il Codice della *privacy* alla nuova normativa europea[29].

---

informazioni che vengono conservate separatamente, al fine di impedire l'identificazione del soggetto. Grazie a tale tecnica, possono compiersi ulteriori trattamenti dei dati, proprio in quanto si abbassa il livello di tutela dell'interessato, in ragione dell'impossibilità di identificarlo. Quando l'identificazione dell'interessato ritorni possibile, il titolare e responsabile del trattamento dovranno rispettare le istanze di tutela previste dal Regolamento. In tal senso, si v. A. Nervi, *Il perimetro del Regolamento europeo: portata applicativa e definizioni,* in V. Cuffaro- R. D'Orazio- V. Ricciuto (a cura di), *I dati personali nel diritto europeo, op.cit.*, p. 176.

[25] Sul punto si v. G. Resta, *Anonimato, responsabilità, identificazione, op.cit.,* p. 177 (§ 2.2.) che richiama l'indicazione del Gruppo Art. 29 nel documento 5/2009 sui *social network* che ribadisce che i *providers* dovrebbero consentire agli utenti di interagire, nell'ambito degli stessi, in maniera anonima o con pseudonimo.

[26] Si v. G. Finocchiaro (*Conclusioni*, in G. Finocchiaro (a cura di), *Diritto all'anonimato,* Padova, 2008, p. 414) che evidenzia come, nella società digitale, l'anonimato assuma sempre più la funzione di garantire il diritto alla ricostruzione dell'identità di un soggetto e il diritto a non subire invasioni nella propria sfera intima e a non essere oggetto di profilazioni: il c.d. «diritto all'inviolabilità della persona elettronica». Sul tema si v. G. Finocchiaro, voce «*Identità personale (diritto alla)*», in *Dig.disc.priv., sez. civ., Aggiornamento,* Torino, 210, p. 737 s; G. Resta, *Identità personale e identità digitale*, in *Dir. Informaz.e informatica,* 2007, p. 511 ss.

[27] Sull'anonimato quale mezzo di attuazione del diritto alla protezione dei dati personali, si v. E. Morelato, *Anonimato e protezione dei dati personali,* in G. Finocchiaro (a cura di), *Diritto all'anonimato, op.cit.,* p. 205 ss; G. Finocchiaro, *Diritto all'anonimato,* in G. Finocchiaro- F. Delfini (a cura di), *Diritto dell'informatica,* Torino, 2014, p. 184 s.

[28] Si v. G. Finocchiaro, voce «*Anonimato*», *op.cit.,* p. 16.

[29] La direttiva 46/95/CE era stata recepita dalla legge 31 dicembre 1996, n. 675, la cui disciplina è, di seguito, confluita nel Codice in materia di protezione dei dati personali,

Non si tralasci, in aggiunta, che la Carta dei diritti fondamentali dell'Unione europea, direttamente vincolante negli Stati membri, ha attribuito il rango di diritto fondamentale al diritto alla protezione dei dati personali, previsto nell'art. 8 (fra i diritti di libertà) che afferma che «ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano»[30].

Per pervenire a tale conclusione, occorre previamente affrontare la questione se il nostro ordinamento riconosca il diritto all'anonimato in rete, come accade in Germania.

In Germania, il § 13, comma 6, *TelemedienGesetz* (la legge sui media telematici) del 26 febbraio 2007[31] ha statuito l'obbligo del *provider* di consentire che l'uso dei servizi telematici ed il relativo pagamento avvengano, in forma anonima o tramite il ricorso allo pseudonimo, ogniqualvolta ciò sia tecnicamente possibile e ragionevole, specificando che l'utente del servizio debba essere informato di tale possibilità.

Tale norma costituisce il cardine della disciplina[32], in quanto ha sancito come, a fronte dell'obbligo suddetto del *provider*, sussista la pretesa degli utenti della rete, giuridicamente riconosciuta e garantita, di usare i servizi telematici in forma anonima oppure con pseudonimo, seppur nei limiti previsti *ex lege.* Il fondamento della norma è stato rinvenuto dalla giurisprudenza e dalla dottrina

---

emanato dal d.lgs. 30 giugno 2003, n. 196. Col d.lgs. 10 agosto 2018, n. 101, il legislatore italiano ha poi provveduto ad adeguare tale normativa al Regolamento generale sulla *privacy* . Sul punto si v. S. Messina, *L'adeguamento della normativa nazionale al Regolamento,* in V. Cuffaro- R. D'Orazio- V. Ricciuto (a cura di), *I dati personali nel diritto europeo, op.cit.,* p. 119 ss.

[30] La Carta dei diritti fondamentali dell'Unione Europea, proclamata a Nizza nel 2000, è divenuta direttamente vincolante negli Stati membri dell'Unione Europea dal 2009, assumendo lo stesso valore dei Trattati europei, come stabilito dal trattato di Lisbona nel 2007. Mentre l'art. 8 riguarda la protezione dei dati personali, l'art. 7 il rispetto della vita privata e familiare. Sul punto si v. R. D'Orazio, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale,* V. Cuffaro- R. D'Orazio- V. Ricciuto (a cura di), *I dati personali nel diritto europeo, op.cit.,* p. 76.

[31] La legge (BGBI I S.179), in vigore dal primo marzo 2007, modificata più volte e di recente dal *Gesetz gegen illegale Beschäftigung und Sozialleistungsmissbrauch* dell'11 luglio 2019 (BGBI I S. 1066).

[32] Per le osservazioni che seguono sulla disciplina tedesca, si v. G. Resta (*Anonimato, responsabilità, identificazione, op.cit.,* p. 175 (§ 2.2.), il quale precisa come tendenzialmente si dichiari la natura imperativa della norma che, avendo fondamento costituzionale, non sarebbe derogabile dall'autonomia privata.

sia nella garanzia costituzionale della libertà di manifestazione del pensiero, ai sensi dell'art. 5 *GrundGesetz*, sia nella disciplina di protezione dei dati personali, dettata dal *BundesdatenschutzGesetz*[33].

Per quanto concerne il formante giurisprudenziale, si consideri che significativamente il *BundesGerichtshof*, la Corte di legittimità, ha sostenuto che «l'anonimato è immanente ad *internet*»[34].

Nel solco di tale indirizzo, la giurisprudenza tedesca maggioritaria si esprime tendenzialmente nel senso di far prevalere l'interesse alla manifestazione del pensiero in modo anonimo (garantito dall'art. 5. *GrundGesetz*, Costituzione tedesca, e dall'art. 10 Carta Europea dei Diritti dell'Uomo), rispetto alla tutela di altri diritti fondamentali[35], quali il diritto all'onore, il diritto alla reputazione, il diritto all'autodeterminazione informativa, il c.d. *Recht auf informationelle Selbstbestimmung*[36].

---

[33] La disciplina della protezione dei dati personali è stata, da ultimo, modificata il 27 giugno 2019 dalla seconda *Gesetz zur Anpassung des Datenschutzrechts an die EU-Verordnung 2016 / 679 und zur Umsetzung der EU-Richtlinie 2016/680*, legge di adeguamento del diritto alla protezione dei dati personali al Regolamento generale sulla *privacy* ed alla direttiva UE del 27 aprile 2016, n. 680 del Parlamento europeo e del Consiglio, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

[34] Si v. *BGH*, 23 giugno 2009- VI ZR 196/08, pubblicata in *Neue Juristische Wochenschrift*, 2009, p. 2892.

[35] Si v. M. Manetti, *Libertà di pensiero e anonimato in rete, op.cit,* p. 147 ss. (§4); G. Giannone Codiglione, *Reputazione* on line, *sistemi di* rating *e anonimato in una recente decisione della Corte di Cassazione Tedesca*, in *Dir.informaz. e informatica,* 2015, p. 169 s. (§ 1).

[36] Il diritto all'autodeterminazione informativa, vale a dire il diritto del singolo a decidere in prima persona sulla cessione e l'uso dei dati che lo riguardino, è stato coniato dalla giurisprudenza costituzionale tedesca che ne ha individuato il fondamento normativo e la garanzia nell'art 2, comma 1, e nell'art. 1, comma 1, *GrundGesetz*. Sul punto si v. G. Giannone Codiglione, *Reputazione on line, sistemi di rating e anonimato in una recente decisione della Corte di Cassazione Tedesca*, *op.cit.*, p.171 s., nt. 13 (§ 3). Paradigmatica è la decisione del *BGH*, sentenza del 23 settembre 2014 (VI ZR 358/13) (disponibile in https://juris.bundesgerichtshof.de) che è intervenuta sul problema della protezione della reputazione *on line* dell'esercente la professione medica, lesa da recensioni anonime di utenti di una piattaforma digitale. Il ricorrente, un ginecologo tedesco, era stato oggetto di alcune valutazioni anonime sul portale *Jamade.de* che raccoglie, conserva e mette a disposizione i dati identificativi (quali il titolo accademico, il nome), di contatto

4. Le limitazioni alla tutela dell'anonimato in rete nell'ordinamento italiano

Tornando al nostro ordinamento, si osservi come, in realtà, il legislatore italiano abbia riconosciuto il diritto soggettivo all'anonimato con riferimento a determinati soggetti a garanzia di interessi eterogenei, in ambiti specifici, in circostanze indicate e per finalità definite che vengono richiamate o meno dal legislatore[37].

(l'indirizzo dove svolge la sua professione, gli orari di ufficio) e di specializzazione dei medici che esercitano la propria professione in Germania, consentendo all'utente di esprimere giudizi sul loro operato. Il sito è organizzato in modo tale che le recensioni, espresse sotto forma di voto oppure con contenuto libero, possano essere pubblicate, anche in modo anonimo, iscrivendosi al sito gratuitamente, mediante la semplice indicazione di un indirizzo *e mail* valido che sarà verificato, durante il processo di registrazione. Il ricorrente ha richiesto al gestore del portale la rimozione dei suoi dati personali, pubblicati sulla piattaforma, fondando la richiesta sulla disciplina di protezione dei dati del *BundesdatenschutzGesetz*, ed il divieto di pubblicare i giudizi sul proprio operato, nella sua pagina profilo (oltre al pagamento delle spese processuali). Tale pretesa è stata correlata alla circostanza che l'immissione di recensioni e commenti, anche in forma anonima, potrebbe dar luogo ad usi diffamatori, lesivi sia del diritto all'identità personale, sia della libertà di esercizio della professione; effetti amplificati dalla possibilità di accedere liberamente ai giudizi anche da parte di utenti non registrati al sito, per mezzo di un motore di ricerca. La Corte, nel valutare le pretese attoree, è stata chiamata ad effettuare un'operazione di bilanciamento tra il diritto alla libertà di espressione del *provider* convenuto, da un lato, e la legittima aspettativa alla protezione della *privacy*, dall'altro lato, azionata nella forma del diritto all'autodeterminazione informativa dell'attore e rafforzata dai potenziali effetti negativi, in termini reputazionali e competitivi, rispetto ad altri medici, anch'essi oggetto di *rating*. La Corte ha rigettato le richieste dell'attore, considerando preminente, rispetto all'interesse alla cancellazione dei dati ed alla non inclusione del professionista nel portale di *rating* professionale, il diritto alla libertà di espressione, riconosciuto in capo alla piattaforma *Jameda.de,* nelle diverse forme di libertà di informazione e del diritto di accesso alle informazioni e della libertà di opinione di tutti i consociati, in ragione della circostanza che l'attività svolta dal prestatore non sia in ambito prettamente economico, ma piuttosto di utilità sociale, in quanto relativa al delicato ambito della salute. Per tale commento alla pronuncia, si v. G. Giannone Codiglione, *Reputazione on line, sistemi di rating e anonimato in una recente decisione della Corte di Cassazione Tedesca*, *op.cit.,* p. 171 ss. (§3).

[37] Si v. G. Finocchiaro, voce «*Anonimato*», *op.cit*., p. 16. Sul punto si v. anche G. Resta, *Anonimato, responsabilità, identificazione: prospettive di diritto comparato*, *op.cit.,* p. 171 (§ 1). A titolo esplicativo, si citi, tra le varie disposizioni, la disciplina in materia di comunicazioni telefoniche (artt. 123, 126, 129 del Codice di protezione dei dati personali); la disciplina in materia di protezione della riservatezza dei pazienti di dati

L'interpretazione sistematica ed assiologica[38] di tali norme settoriali induce alle conclusioni che seguono.

Non esiste un principio generale che riconosca il diritto all'anonimato e dunque un «diritto autonomo» all'anonimato[39], giacché esso costituisce un diritto solo qualora sia espressamente riconosciuto da leggi speciali[40].

Seppure il diritto all'anonimato, in linea generale, tenda a collocarsi nell'alveo del diritto alla riservatezza e alla protezione dei dati personali – poichè quest'ultimo consiste nel diritto di esercitare il controllo sui propri dati, e trova, di conseguenza, la sua espressione più forte nel diritto di oscurarli[41]-; sebbene il diritto alla protezione dei dati personali puntualmente previsto e disciplinato dal legislatore europeo ed italiano, affondi le proprie radici nell'art. 2 Cost[42], in quanto risulta funzionale al pieno sviluppo della personalità umana; ciononostante non può ravvisarsi nella Costituzione il fondamento del riconoscimento e della garanzia di un diritto "generale"

---

sanitari, ora contenuta nel Regolamento generale sulla *privacy*; le disposizioni riguardanti il diritto all'oscuramento dei dati identificativi nella divulgazione delle sentenze o dei provvedimenti giurisdizionali, dettata dall'art. 52 del Codice di protezione dei dati personali; la disciplina sul «parto in anonimato» che tutela le «madri segrete» che partoriscono in ospedale, ma non riconoscono il proprio figlio (art. 30, comma 2, Decr.pres.rep., 3 novembre 2000).

[38] Secondo autorevole insegnamento, le norme non vanno interpretate in astratto, fermandosi al dato letterale della 'legge formale', ma in relazione al caso concreto, valutato nella sua peculiarità, e calandole all'interno del contesto storico-giuridico attuale. La dottrina precisa come la trasformazione del sistema delle fonti imponga un corrispondente mutamento della teoria dell'interpretazione, laddove le regole della stessa debbano essere adeguate al mutato quadro dell'ordinamento giuridico, caratterizzato dalla presenza della Costituzione e del diritto dell'Unione Europea. Nel rispetto del principio di legalità, la norma deve pertanto essere posta in «relazione dialogica» con il fatto da regolare e l'interpretazione di una disposizione è il risultato del coordinamento con le altre norme dell'ordinamento giuridico e dell'armonizzazione con i principi costituzionali ed i valori normativi. Si v. P. Perlingieri, *Applicazione e controllo nell'interpretazione giuridica,* in *Riv.dir.civ*., 2010, p. 307 ss.; Id., *Interpretazione sistematica e assiologica, situazioni soggettive e rapporto giuridico*, Napoli, 2006, *passim*)

[39] Si v. G.M. Riccio, *Anonimato e responsabilità in* internet, *op.cit.,* p. 325.

[40] Si v. G. Finocchiaro, voce «*Anonimato*», *op.cit*., p. 19.

[41] Si v. G. Finocchiaro, voce «*Anonimato*», *op.cit*., p. 19.

[42] Sul punto si v. G. Finocchiaro, voce «*Identità personale (diritto alla)*», *op.cit*., p. 729.

all'anonimato[43], quale conseguenza automatica del diritto alla "*privacy*", nelle sue diverse declinazioni[44].

Nè può configurarsi il diritto all'anonimato, analogamente al diritto al nome ed al diritto all'identità personale, quale un diritto della personalità umana[45], *ex* art. 2 Cost.

---

[43] Esclude che l'anonimato possa essere configurato quale bene di rilevanza costituzionale D. Tassinari, *Diritto all'anonimato e diritto penale: un (possibile) oggetto di tutela o un* vulnus *per il* law enforcement?, in Aa.Vv. *Diritto all'anonimato. Anonimato, nome e identità personale*, a cura di G. Finocchiaro, *Trattato di diritto Commerciale e di diritto pubblico del'economia,* diretto da F. Galgano, XXIV, Padova, 2008, p. 382.

[44] Si v. G. E. Vigevani, *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano*, *op.cit.*, p. 212 s. (§ 4).

[45] Si v. G. Finocchiaro, voce «*Anonimato*», *op.cit*., p. 18 s. Si osservi che la disamina del riconoscimento e dell'individuazione del fondamento normativo di un (potenziale) diritto all'anonimato in rete solleva la questione della raffigurazione dell'anonimato in rete quale diritto della personalità umana, il cui fondamento possa rinvenirsi nell'art. 2 Cost. Parte della dottrina (G. E. Vigevani, *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano*, *op.cit.*, p. 212 s. (§ 4) ha negato che l'anonimato in rete sia qualificabile quale "nuovo diritto", riconoscibile *ex* art. 2 Cost., da intendersi quale «clausola aperta». Si puntualizzi che l'interpretazione dell'art. 2 Cost. ha avviato il dibattito relativo alla natura «aperta» o «chiusa» della norma. Se parte della dottrina ritiene che la norma costituisca una clausola «chiusa» e che sia una «norma di principio», la cui portata assumerebbe valenza solamente col rinvio ai singoli diritti previsti e regolamentati nella Costituzione; secondo un diverso indirizzo, la norma appare essere una clausola «aperta», in forza della quale sarebbe possibile enucleare "nuovi diritti", espressione delle esigenze emergenti in un determinate contesto storico. Sul tema si v. C. De Martini, *Il diritto all'identità personale nell'esperienza operativa,* in Aa. Vv., *La lesione dell'identità personale e il danno non patrimoniale,* Milano, 1985, p. 94 ss. Nell'ambito della dottrina civilistica, un primo orientamento (c.d. teoria atomistica) ha inizialmente valutato il grado di rilevanza dei diritti della personalità umana, alla stregua delle sole disposizioni puntuali che li statuiscano. Autorevole dottrina (P. Perlingieri, *La personalità umana nell'ordinamento giuridico*, Camerino-Napoli, 1972, p. 11, p. 154 ss.; ID., *La persona umana e i suoi diritti*, Napoli, 2005, *passim*) ha poi diversamente sottolineato il valore precettivo e non meramente programmatico dell'art. 2 Cost., escludendo che lo si possa considerare come norma di semplice rinvio a diritti che siano espressamente previsti nella Costituzione oppure in leggi ordinarie e precisando come tale norma sia in grado di costituire il fondamento di bisogni ed interessi meritevoli di tutela che siano manifestazione del mutamento delle esigenze personalistiche, nel contesto storico-giuridico di riferimento. Secondo tale impostazione, la personalità umana è un valore fondamentale dell'ordinamento giuridico, alla cui base si pone un numero indefinito di situazioni esistenziali, in quanto il sistema protegge il valore della persona umana senza limiti e non può, di conseguenza, esistere un numero circoscritto di interessi da tutelare. Ogni

Il diritto all'anonimato va ricostruito come diritto «frammentario»[46], non avente portata generale, e «relativo», ossia strumentale all'esercizio di diritti di rilevanza costituzionale, quali la salute, la vita, la *privacy* e l'identità personale[47]. Tale diritto trova riconoscimento nel nostro sistema solo «in via mediata», in riferimento ad un altro diritto che si voglia proteggere[48].

La negazione di un autonomo diritto all'anonimato costituzionalmente rilevante non esclude infatti che la Costituzione consenta e garantisca ad un soggetto di nascondere la propria identità, qualora si debbano tutelare i diritti della sfera individuale[49].

---

manifestazione della persona ed ogni sua legittima aspirazione allo svolgimento della personalità umana sono tutelate, secondo modalità non prestabilite: si parla infatti di "atipicità" dei diritti della personalità umana. La personalità va comunque considerata nel suo valore unitario, unico essendo il bene tutelato, tendenzialmente illimitato. Tale ricostruzione, fautrice della c.d. teoria monista, prospetta quindi l'esistenza di un unico diritto della personalità di contenuto indistinto che riassume in sè tutti gli altri, senza indentificarsi tuttavia nella loro somma. Non può nondimeno escludersi che l'ordinamento possa disporre alcune estrinsecazioni della stessa che siano maggiormente qualificanti. Infine, per rispondere alle critiche dei sostenitori della teoria atomista, relative alla moltiplicazione dei diritti della personalità umana che finirebbe col minare il principio di certezza del diritto, si sostiene che i diritti fondamentali della persona richiedono comunque il rispetto dei doveri inderogabili di solidarietà sociale, dal momento che la persona è inseparabile dalla solidarietà, in quanto la cura dell'altro fa parte del concetto stesso di persona. (si v. P. Perlingieri, *Il diritto civile nella legalità costituzionale secondo il sistema italo –comunitario delle fonti*, Napoli, 2006, p. 433 che sostiene che il *personalismo* trae nutrimento dal *solidarismo*, di cui all'art. 2 Cost., in quanto propriamente finalizzato a realizzare il pieno sviluppo della personalità umana). Ne discende che, nella prospettiva costituzionale, la solidarietà esprime la cooperazione e l'eguaglianza, nell'ambito dell'affermazione dei diritti fondamentali di tutti i soggetti. (P. Perlingieri., *Eguaglianza, capacità contributiva e diritto civile*, in *Rass.dir.civ*., 1980, p. 724). L'analisi, a grandi linee, di tale insegnamento induce a riflettere come l'esclusione della configurabilità dell'anonimato in rete quale diritto della personalità umana possa costituire ancora oggetto di futura riflessione. Per un'attenta ricostruzione della teoria atomista e della teoria monista, con particolare attenzione alla dottrina richiamata, si v. R. Ruscica (a cura di), *I diritti della personalità. Strategie di tutela. Inibitoria, risarcimento danni. Internet*, Padova, 2013, p. 40 ss.

[46] Si v. G. E. Vigevani, *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano*, *op.cit.*, p. 213 (§ 4).

[47] Si v. G. Finocchiaro, voce «*Anonimato*», *op.cit*., pp. 15, 16, 19; G. M. Riccio, *Diritto all'anonimato e responsabilità civile del provider, op.cit.,* p. 26.

[48] Si v. G.M. Riccio, *Anonimato e responsabilità in* internet, *op.cit.,* p. 325.

[49] Si v. G. E. Vigevani, *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano*, *op.cit.*, p. 212 s. (§ 4); G. M. Riccio, *Anonimato e responsabilità*

Può, di conseguenza, ricondursi l'anonimato in rete alla funzione di controllo sulla propria identità digitale e collocarlo nell'alveo del diritto alla protezione dei propri dati personali, al quale esso finisce col dare attuazione[50].

Non può viceversa rinvenirsi il fondamento costituzionale dell'anonimato in rete nell'art. 21 Cost.[51], analogamente a quanto assunto dalla dottrina e giurisprudenza statunitense e tedesca che hanno individuato il fondamento costituzionale dell'anonimato in rete, riconosciuto quale vero e proprio diritto fondamentale degli internauti, rispettivamente nel *First Amendament's freedom of speech*[52] e nell'art. 5 *GrundGesetz.*

L'art. 21 Cost.[53] se, per un verso, proclama la libertà di manifestazione del pensiero quale esplicazione dell'autodeterminazione individuale, per altro verso, valorizza i principi di responsabilità personale di chi diffonde informazioni o idee e di trasparenza che informano il nostro ordinamento. L'interpretazione della norma ha condotto la dottrina ad escludere che le manifestazioni del pensiero in forma anonima rientrino nell'ambito della tutela costituzionale e a non ammettere l'esistenza di un diritto costituzionale ad esprimere il pensiero anonimamente. D'altra parte dalla lettura dell'art. 21 emerge chiaramente lo sfavore della Costituzione verso gli scritti anonimi, laddove statuisce, al comma 3, che il sequestro degli stampati possa realizzarsi quando si assista alla «violazione delle norme che la legge stessa prescriva per l'indicazione dei responsabili», consentendo, in tal guisa, al

---

in internet, *op.cit.*, p. 325. Si v. le notazioni di S. Rodotà (*Il diritto ad avere diritti*, Roma-Bari, 2012, p. 392) che specifica come l'anonimato costituisca l'eccezione, nel senso che difficilmente lo si possa intendere quale «elemento costitutivo della versione digitale della cittadinanza», dal momento che è sottoposto ai temperamenti necessari, quando colui che si esprima in rete in modo anonimo commetta un fatto illecito che arrechi danni a terzi.

[50] Si v. G. Finocchiaro, *Conclusioni*, in G. Finocchiaro (a cura di), *Diritto all'anonimato, op.cit*., p. 414.

[51] Si v. G. E. Vigevani, *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano*, *op.cit.*, p. 215 s. (§ 5).

[52] Sul tema si v. V. Zeno Zencovich, *Anonymous speech on the internet, op.cit.,* p. 103 ss.

[53] Per le riflessioni che seguono, si v. G.E.Vigevani, *Anonimato, responsabilità e trasparenza, op.cit.,* p. 215 ss. (§ 5). Sul punto si v. anche M. Betzu, *Anonimato e responsabilità in Internet,* in www.costituzionalismo.it, 6 ottobre 2011, p. 11.

legislatore di statuire delle norme che siano dirette a permettere l'individuazione di un soggetto responsabile della pubblicazione.

Deve, ad ogni modo, affermarsi che, sebbene il nostro ordinamento non riconosca legislativamente un diritto all'anonimato in rete, non esiste comunque un divieto puntuale di manifestare ivi le proprie opinioni in maniera anonima, tanto più che, come visto, l'anonimato in rete rappresenta una declinazione del diritto della protezione dei dati personali[54].

Il ricorso all'anonimato in rete è quindi lecito nel nostro sistema, seppure entro determinati limiti, ossia nella misura in cui l'internauta, che ivi interagisca, tenga una condotta rispettosa dei diritti, facenti capo ai soggetti che costituiscano oggetto dei contenuti, pubblicati sulle piattaforme digitali di cui sia utente[55].

L'anonimato in rete, dal momento che rappresenta una forma di esercizio del diritto alla protezione dei dati personali, come questo diritto, dovrà difatti essere bilanciato di continuo con altri diritti fondamentali[56]. Conseguentemente la pretesa a manifestare le proprie idee in maniera anonima soccomberà, quando vengano lesi interessi costituzionalmente rilevanti, quali, a titolo esplicativo, l'onore, la riservatezza, la reputazione, quale diritto della personalità umana[57], e la reputazione commerciale delle imprese che rinviene la garanzia costituzionale nell'art. 41 Cost[58].

---

[54] Si v. G.E.Vigevani, *Anonimato, responsabilità e trasparenza, op.cit.,* p. 216 (§ 6). Sull'inesistenza, nel nostro ordinamento, di un divieto generale dell'anonimato in rete, si v. anche G.E.Vigevani, *Anonimato, responsabilità e trasparenza, op.cit.,* p. 4.

[55] Si v. anche M. Manetti, *Libertà di pensiero e anonimato in rete, op.cit.*, p. 149 ss. (§ 5), secondo la quale «il pensiero espresso in forma anonima (…) non costituisce di per sé una frode».

[56] Si v. G. Finocchiaro, voce «*Anonimato*», *op.cit*.,p. 19.

[57] Si v. G.E. Vigevani, *Anonimato, responsabilità e trasparenza, op.cit.,* p. 216 (§ 6). Sulla stessa linea, si v. E. Pelino (*L'anonimato su* internet, in Aa.Vv. *Diritto all'anonimato. Anonimato, nome e identità personale*, a cura di G. Finocchiaro, *Trattato di diritto Commerciale e di diritto pubblico del'economia, op.cit.*, p. 293) che puntualizza come l'anonimato, seppur inteso quale strumentale al diritto alla protezione dei dati personali, debba subire una limitazione, dinanzi ad altri diritti prevalenti.

[58] Si condivide l'orientamento che connota la reputazione delle imprese quale diritto di natura patrimoniale, evidenziando come la sua lesione incida sul valore competitivo e sull'aspettativa di guadagno della stessa. Sul punto si v. A. Ricci, *La reputazione: dal concetto alle declinazioni,* Torino, 2018, *passim*. Per comprendere la portata della problematica delle recensioni negative sui prodotti o servizi delle imprese che vanno a

Appare evidente come la demarcazione dei confini di operatività dell'anonimato in rete in tali termini sia espressione dell'esigenza di individuare i responsabili di fatti illeciti[59].

L'anonimato non può quindi essere assoluto[60], sebbene assurga, pur sempre, a interesse prioritario nel mondo digitale, per garantire agli internauti la libertà di manifestazione del pensiero in rete, quale c.d. "*marketplace of ideas*".

In tale ottica, appare come il punto d'incontro tra tale libertà e l'esigenza di tutela della vittima dell'offesa via *internet* sia rinvenibile in quello che è stato definito «anonimato protetto»[61], vale a dire una forma di comunicazione nella quale, pur lasciando liberi gli internauti di esprimersi in maniera anonima o con pseudonimo, essi vengano previamente identificati da parte del *provider*; con la conseguenza che gli autori degli illeciti risultino rintracciabili dal soggetto potenzialmente danneggiato, con la collaborazione del gestore della piattaforma digitale, per ordine e sotto la supervisione dell'autorità giudiziaria.

Tale costruzione presenta più pregi. Innanzitutto, se si finisce con l'assicurare ai soggetti danneggiati adeguati ed effettivi strumenti di tutela, cionondimeno non si limita l'anonimato in rete, al punto tale da provocare i c.dd. *chilling effects*. Inoltre la "*privacy*" dei fruitori del servizio sarà pur sempre salvaguardata, dal momento che, come ovvio, l'*internet provider*, quale «titolare del trattamento», sarà tenuto a rispettare la normativa sulla protezione dei dati personali e si potrà risalire alle loro generalità «solo in casi eccezionali», ossia unicamente nelle ipotesi in cui l'autorità giudiziaria lo imponga, al fine di garantire ai soggetti danneggiati strumenti di tutela adeguata[62].

---

riverberarsi sulla reputazione commerciale delle stesse, si v. *infra* (§ 5) l'ordinanza Trib. Venezia, 24 febbraio 2015, in *Corr. Giur*., 2016, p. 78 ss.

[59] Si v. M. Manetti, *Libertà di pensiero e anonimato in rete, op.cit.*, p. 150 (*§* 5).

[60] Si v. G. Finocchiaro, voce «*Anonimato*», *op.cit*.,p. 19.

[61] Per tale impostazione e le argomentazioni che seguono, si v. R. Natoli, *La tutela dell'onore e della reputazione in internet, op.cit*., p. 443.

[62] Si v. S. Rodotà, *Il mondo nella rete, op.cit.*, p. 25.

5. La figura "atipica" dell'*hosting provider* «attivo»

Prima di soffermarsi sul tema dell'obbligatorietà dell'autenticazione dei destinatari del servizio da parte degli *hosting providers*, occorrerà tracciare i capisaldi della disciplina nazionale della responsabilità civile dell'*hosting provider* di recepimento della c.d. «direttiva sul commercio elettronico».

È noto che l'art. 15 della direttiva (recepito, nel nostro ordinamento, dall'art. 17, comma 1, d.lgs. 9 aprile 2003, n. 70) ha introdotto il principio generale[63], in forza del quale non grava, in capo a nessuno degli intermediari della rete, l'obbligo generale di sorveglianza delle informazioni che trasmettono o memorizzano, né un obbligo generale di ricerca attiva di fatti o circostanze che indichino la presenza di attività illecite. Alla mancata previsione di un obbligo di sorveglianza si è fatta discendere l'esclusione della responsabilità dell'*internet service provider*[64] per le informazioni trasmesse o memorizzate e le operazioni compiute dall'utente del servizio, purché il primo non intervenga in alcuna modalità sul contenuto o sullo svolgimento delle stesse. Tale regime speciale si differenzia, di fatto, dalle regole generali sulla responsabilità civile, in quanto la sua applicazione determina l'esonero di responsabilità del *provider*, nel caso in cui sussistano le condizioni previste dalla direttiva: il prestatore del servizio *on line* non è obbligato a conoscere le informazioni trasmesse o memorizzate e non risponderà della loro illiceità, se non ne conosca il contenuto. Costui sarà pertanto responsabile solamente quando, pur essendo a conoscenza dell'illecito, non faccia nulla per prevenirlo e/o evitarlo, tenendo, in tal guisa, una condotta non diligente[65].

É altrettanto noto che la disciplina speciale statuisce, in sostanza, un «regime di favore» per l'*internet service provider*[66], fondando la sua

---

[63] Si v. M. Zarro, *La tutela della reputazione digitale quale* «intangible asset», in *Rass.dir.civ*., 2017, p. 1521.

[64] Per le notazioni che seguono si v. L. Vizzoni, *Recensioni non genuine su Tripadvisor; quali responsabilità?,* in *Resp.civ.prev*., 2018, p. 710, (§ 4).

[65] Si v. G. Ponzanelli, *Verso un diritto uniforme per la responsabilità, op.cit.,* p. 8.

[66] La *ratio* ispiratrice della normativa parte dal convincimento che gravare gli intermediari della rete di obblighi di diligenza eccessiva, nell'erogazione del servizio, penalizzarebbe in modo sproporzionato la loro posizione, caricandoli di costi di oneri

responsabilità civile sul criterio di imputazione della colpa, per violazione del dovere di diligenza professionale[67].

In merito alla figura dell'*hosting provider*, il d.lgs. 2003/70 statuisce un principio di non responsabilità delle informazioni memorizzate, salvo che non ricorrano determinati presupposti. Tale principio viene meno: qualora l'*hosting provider* sia effettivamente a conoscenza del fatto che l'attività oppure l'informazione è illecita e, per quanto concerne le azioni risarcitorie, sia al corrente di fatti o circostanze che rendano «manifesta» l'illiceità dell'attività e dell'informazione (art. 16, comma 1, lett. a)); non appena a conoscenza di tali fatti, non agisca prontamente per rimuovere le informazioni oppure per disabilitarne l'accesso (art. 16, comma 1, lett b)) oppure se (ai sensi dell'art. 17, comma 2, lett b)), informato di fatti o circostanze che rendano "manifesto" il carattere illecito o pregiudizievole per qualcuno dell'attività o dell'informazione, non si attivi per riferire all'autorità competente[68].

Ai fini della responsabilità civile dell'*hosting provider*[69], si impone la valutazione della "colpa per negligenza", a fronte dell'allegazione della conoscenza sostanziale di attività o informazioni illecite oppure di fatti o circostanze che rendano l'illiceità dell'attività o dell'informazione manifesta. Tutto ciò non comporta tuttavia l'attivazione del *provider* nel controllare i

---

tecnici (si pensi ai sistemi di filtraggio), per evitare e prevenire la commissione di illeciti. Ciò equivarrebbe a paralizzare o quantomeno a porre dei freni all'attività imprenditoriale, correndosi, tra l'altro, il rischio di alimentare nel mercato oligopoli degli operatori economicamente più forti. In tal senso si v. G.M. Riccio, *Anonimato e responsabilità in i*nternet, *op.cit.,* p. 335) Si è altresì considerato (si v. M. Gambini, *Gli hosting providers tra i doveri di diligenza professionale, op.cit.,* p. 2; G. Ponzanelli, *Verso un diritto uniforme, op.cit.*, p. 8) che un riconoscimento generalizzato della responsabilità civile degli *internet service providers* implicherebbe una limitazione della libertà di manifestazione del pensiero degli utenti di *internet*, poichè i primi, in particolar modo gli *hosting providers*, per evitare il rischio di incorrere nella responsabilità civile, sarebbero indotti a censurare i contenuti di utenti potenzialmente lesivi di diritti di terzi.

[67] Si v. M. Zarro, *La tutela della reputazione digitale*, *op.cit.,* p. 1521.

[68] L'art. 16, comma 3, d.lgs. 2003/70 prevede che l'autorità giudiziaria o quella amministrativa competente possa esigere, anche in via d'urgenza, che l'*hosting provider*, nell'esercizio delle proprie attività, impedisca oppure ponga fine alle violazioni commesse.

[69] Per le considerazioni che seguono si v. M. Cocuccio, *La responsabilità civile per fatto illecito dell'*internet service provider, in *Resp.civ.prev.*, 2015, p. 1319.

contenuti memorizzati, salvo che vi sia una specifica segnalazione da parte «delle autorità competenti»[70].

Esiste perciò, anche per tale figura di *provider*, una «generale esenzione di responsabilità» che non si applicherà qualora, pur essendo a conoscenza di fatti illeciti, non intervenga immediatamente, in conformità a quanto previsto dal legislatore[71].

Ad ogni modo, l'*hosting provider* potrà beneficiare dei limiti della responsabilità, ai sensi dell'art. 14 della direttiva, in linea con quanto previsto dal considerando 42 della medesima, unicamente quando si connoti per lo svolgimento di un'attività «neutra» o meglio per un ruolo «meramente tecnico, automatico e passivo» che implica che il prestatore di servizi non conosca e non controlli le informazioni immesse e memorizzate in rete[72].

---

[70] Si precisi che la giurisprudenza, nell'applicare l'art. 16, d.lgs. 2003/70, è stata chiamata a sciogliere il dubbio se, in capo all'*hosting provider,* gravi l'obbligo di rimozione o disabilitazione all'accesso dei contenuti illeciti, pubblicati dagli utenti sul portale da costui gestito, unicamente a seguito della comunicazione da parte dell'autorità competente e dunque solamente qualora acquisisca una conoscenza «qualificata» del fatto illecito; ovvero se tale obbligo sorga in maniera autonoma, ossia non appena il *provider* venga a conoscenza del contenuto illecito pubblicato, tramite la segnalazione da parte del privato che assuma essere stato leso dallo stesso. Sul tema si v., *ex multis*, E. Tosi, *Contrasti giurisprudenziali in materia di responsabilità civile degli* hosting provider- *passivi e attivi- tra tipizzazione normativa e interpretazione evolutiva applicata alle nuove figure soggettive dei motori di ricerca, social network e aggregatori di contenuti,* in *Riv.dir.ind.*, 2017, p. 73 s. (§ 6); G.M. Riccio, *La responsabilità civile degli* internet providers, *op.cit*., p. 210; S. Sica, *Responsabilità del provider: per una soluzione "equilibrata" del problema*, in *Corr.giur*., 2013, p. 509; B. Panattoni, *Il sistema di controllo successivo: obbligo di rimozione dell'ISP e meccanismi di notice and take down*, in www.dirittopenalecontemporaneo.it, 2018, n. 5, p. 255.

[71] Si specifichi (M. Cocuccio, *La responsabilità civile per fatto illecito, op.cit.,* p. 1319*)* che, ai sensi dell'art. 16, comma 2, d. lgs. 2003/70, l'esenzione non si applica quando il destinatario del servizio agisca sotto l'autorità o il controllo del prestatore. Invero l'*hosting provider* risponderà per fatto illecito altrui, *ex* art. 2049 cod.civ., in concorso con l'autore del medesimo, nei casi in cui quest'ultimo, agendo sotto il controllo dell'organizzazione aziendale del *provider*, ponga in essere attività che ledano i diritti dei terzi.

[72] In tal senso si è sviluppato l'orientamento, ormai consolidato, della Corte di Giustizia dell'Unione Europea, in via di interpretazione del considerando 42 della direttiva, secondo il quale i limiti di responsabilità, previsti dagli artt. 12-14 della direttiva, sono applicabili alla sola condizione che il *provider* non svolga un ruolo «attivo» che gli consentirebbe la conoscenza ed il controllo dei dati forniti dai suoi clienti. Famoso è il *leading case* della Corte di Giustizia UE (Grande sezione), 23 marzo 2010 (domande di pronuncia pregiudiziale, proposte dalla *Cour de Cassation* - Francia), cause riunite da C-

Ciò posto, a fronte di tale quadro normativo, la giurisprudenza si è trovata a dover affrontare la questione se siano tuttora riconducibili alla figura del fornitore di ospitalità, tipizzata dalla direttiva venti anni or sono, gli *hosting providers*, le cui attività siano divenute assai più ampie e variegate, in ragione dell'evoluzione tecnologica[73]. Si è incentrata l'attenzione[74], in particolare, sui servizi offerti dai motori di ricerca (come, a titolo esemplificativo, *Google*), dai *social network* (come *Facebook*) e dagli aggregatori di contenuti pubblicati da terzi, i c.dd. *user generated content* (come, ad esempio, *Youtube*). La giurisprudenza[75] ha evidenziato come tali prestatori di servizi *on line* svolgano attività di indicizzazione, selezione, organizzazione e filtraggio di contenuti digitali diffusi in rete, al fine conseguire utili d'impresa (tramite la raccolta pubblicitaria), puntualizzando

---

236/08 a C-238/08, Google France SARL e Google Inc. c. Louis Vouitton Malletier SA (C-236/08), Google France SARL c. Viaticum SA e Luteciel SARL (C-237/08), Google France SARL, *Centre National de recherche en relations humaine*s (CNRRH) SAR, Pierre Alexis Thonet, Bruno Raboin e Tiger SARL (C-238/08) – citata in T. Scannicchio e N. A. Vecchio, *I limiti della neutralità: la Corte di giustizia e l'eterno ritorno dell*'hosting *attivo,* in www.filodiritto.it, 17 gennaio 2018, nt. 2. Si v. anche la celebre pronuncia della Corte Giustizia UE, 12 luglio 2011, C-324/09, l'Oréal SA e a.c. eBay International AG, in *AIDA*, 2011, p. 480 ss., con nota di J.B. Nordemann, *Liability of Social Networks for IP Infringements (Latest News)*: *The Eu Law Regime after l'Oréal/eBay*; la sentenza della Corte di Giustizia UE, seconda sez., 7 agosto 2018 (causa C 521-17, *Coöperatieve Vereniging SNB-React U.A. c. D.M.*, in T. Scannicchio e N. A. Vecchio, *I limiti della neutralità, loc.op.ult.cit.*).

[73] Circostanza che induce a riflettere sulla necessità della rivisitazione della disciplina della direttiva, la cui redazione risale a quasi un ventennio fa e risulta essere non più attuale. In tal senso, *ex multis,* si v. F. Di Ciommo, *Programmi di filtro e criteri di imputazione/esonero della responsabilità* on line. *A proposito della sentenza Google/Vivi Down,* in *Dir.informaz. e informatica,* 2010, p. 474; L. Bugiolacchi, *(Dis)orientamenti giurisprudenziali in tema di responsabilità degli* internet provider *(ovvero del difficile rapporto tra assenza di obblighi di controllo e conoscenza dell'illecito)*, in *Riv.dir.ind.,* 2010, p. 328; G. Finocchiaro, *Due recenti decisioni giurisprudenziali inducono a riflettere sul tema della responsabilità della Rete*, su www.blog-studiolegalefinocchiaro.it

[74] Per le osservazioni che seguono si v. E. Tosi, *Contrasti giurisprudenziali in materia di responsabilità civile degli* hosting provider- *passivi e attivi, op.cit.,* pp. 84 ss., § 9.

[75] Sul punto, si v. E. Tosi, *Contrasti giurisprudenziali in materia di responsabilità civile degli* hosting provider, p. 84 ss., § 9. Si v. anche R. Gelli (*False recensioni su* TripAdvisor*: accolta l'azione inibitoria promossa dal ristoratore diffamato,* in *Corr.giur.*, 2016, p. 89) secondo il quale, in tali ipotesi, il fornitore di servizi informatici diventerebbe «in una certa misura, *dominus* dei contenuti caricati sul sito».

che esse costituiscono, in realtà, «indici rivelatori di un'attività di interferenza» degli operatori sui contenuti pubblicati dagli utenti sulle piattaforme digitali, in quanto i primi finiscono con l'avere un, seppur minimo, grado di "consapevolezza*"* degli stessi. Le corti sono, di seguito, pervenute alla conclusione che, non potendosi considerare codeste attività degli *hosting providers* meramente automatizzate e passive, tali soggetti debbano essere ascritti ad nuova categoria "più evoluta" e distinta da quella "tipica" disciplinata dal legislatore[76], con la conseguenza dell'esclusione dell'operatività delle deroghe fissate dalla disciplina europea ed italiana.

Un filone giurisprudenziale[77] ha così forgiato la nuova figura soggettiva «atipica» di fornitore dei servizi *on line*, il c.d. «*hosting* attivo», sostenendo che debba essere sottoposto al regime generale della responsabilità civile aquiliana[78].

Tale indirizzo, sebbene sia stato oggetto di critiche dottrinali[79] ed abbia subito battute d'arresto, in ragione dell'evolversi di un diverso orientamento

---

[76] In tal senso, si v. R. Gelli, *False recensioni su* TripAdvisor*, op.cit.*, p. 90.

[77] Il dibattito giurisprudenziale e dottrinale sulla questione è stato aperto dal noto «*leading case*» RTI c. Yahoo, sul quale si è pronunciato il Trib. Milano, sez.spec.prop.ind. e intellettuale, il 9 settembre 2011, n. 10893, segnando, per la prima volta, l'elaborazione della figura dell'«*hosting* attivo» (sentenza pubblicata in *Riv.dir.ind.,* 2012, p. 364 ss., con nota di A. Saraceno, *Note in tema di violazione del diritto d'autore tramite Internet; la responsabilità degli I*nternet service provider). Nei gradi processuali successivi, se la Corte d'Appello di Milano, sez. impr., 7 gennaio 2015, n. 29 aveva riformato la decisione del Tribunale di Milano, puntualizzando che tutti gli *hosting provider* beneficerebbero dell'esenzione di responsabilità, quando non siano a conoscenza diretta del contenuto caricato dell'utente (decisione pubblicata in *Dir.ind*., 2016, p. 166 ss., con nota di M. Iaselli, *Caso Yahoo! Video: la Corte di Appello di Milano non vede responsabilità nell'operato dell'*internet provider); diversamente, di recente, la Corte di Cassazione civ., I sez., con sentenza del 19 marzo 2019, n. 7708 ha riconosciuto la distinzione tra *hosting* passivi ed attivi, cassando con rinvio la pronuncia della Corte d'Appello stessa. Per un commento alla sentenza si v. F. Frigerio, *Responsabilità dell'*hosting provider*: la Cassazione conferma la distinzione tra attivo e passivo,* in *www.filodiritto.it,* 18 aprile 2019.

[78] Si v. E. Tosi, *Contrasti giurisprudenziali, op.cit.*, p. 62 s. (§ 3). Per una ricostruzione dell'evoluzione giurisprudenziale sulla figura dell'*hosting* attivo, si v. L. Bugiolacchi, *Ascesa e declino della figura del* provider *"attivo"? Riflessioni in tema di fondamento e limiti del regime privilegiato di responsabilità dell'*hosting provider, in *Resp.civ.prev*., 2015, p. 1261 ss.; R. Bocchini, *La responsabilità di* Facebook *per la mancata rimozione di contenuti illeciti,* in *Giur.it*., 2017, p. 638 ss.

[79] Tra le numerose critiche dottrinali, si v. O. Pollicino (*Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli* Internet service provider, in www.giurcost.otg, p.

che ha, all'opposto, negato la rilevanza della distinzione tra *hosting providers* attivi e passivi[80], si è comunque consolidato. É per di più corroborato dalla decisione della Corte di Cassazione civ., I sez., del 19 marzo 2019, n. 7708 (cit.) che, in quanto prima pronuncia dei giudici di legittimità su tale linea, avrà senz'altro un ruolo «persuasivo» sulle decisioni dei giudici di merito[81].

Secondo la suddetta impostazione, alla figura soggettiva dell'*hosting provider* "attivo" si tornano ad applicare le regole di diritto comune, poste dall'art. 2043 cod.civ., per *culpa in vigilando*[82]. Più specificamente, se, da un lato, di norma, l'*hosting provider* è tenuto a svolgere la propria attività, osservando il criterio di diligenza professionale, *ex* art. 1176, comma 2, cod.civ. che gli impone di intervenire immediatamente, qualora venga effettivamente a conoscenza di contenuti illeciti pubblicati sul portale gestito; dall'altro lato, l'*hosting provider* "attivo" sarà tenuto a prestare la cura,

---

13), secondo il quale l'interpretazione che ha condotto la giurisprudenza a coniare la figura dell'*hosting* attivo sarebbe una «forzatura del dato legislativo».

[80] Si v., *ex multis*, la pronuncia della Corte d'Appello di Milano, 7 gennaio 2015, n. 29, citata; la sentenza del Trib. Roma, sez. XVIII, 15 febbraio 2019, n. 3512 che ha dichiarato la responsabilità del *social network Facebook,* per la pubblicazione sul portale di contenuti audiovisivi di terzi, per mezzo di *link* non autorizzati, conducenti ad un'altra piattaforma, *Youtube*. Secondo il giudice, la dimostrazione dell'effettiva conoscenza dei contenuti illeciti da parte del *provider* rende del tutto irrilevante controllare se l'attività svolta sia riconducibile alla figura dell'*hosting* attivo o a quella dell'*hosting* passivo, dal momento che, anche quest'ultimo dovrà attivarsi, per consentire la rimozione di informazioni illecite immesse sul sito o impedirne l'accesso, non appena riceva la notizia dell'illecito commesso dai fruitori del suo servizio, in ottemperanza all'adempimento del dovere di diligenza professionale, richiesta dal tipo di attività economica svolta. La sentenza è pubblicata in www.francocrisafi.it › web_secondario › sentenze 2019 › tribunale civile.

[81] In tal senso si v. F. Frigerio, *Responsabilità dell*'hosting provider*: la Cassazione conferma, loc.op.ult.cit.*

[82] Si v. R. Gelli, *False recensioni su* TripAdvisor, *op.cit*., p. 90 s.; M. Zarro, *La tutela della reputazione digitale quale* «intangible asset», *op.cit.*, p. 1523 che condivide le argomentazioni di M. Gambini (*Diritti di proprietà intellettuale in rete: criticità e prospettive degli strumenti di tutela nei confronti dei prestatori dei servizi* Internet, in *Rass.dir.civ*., 2016, p. 139), secondo la quale non si dovrebbe negare aprioristicamente la fattispecie della *culpa in vigilando* degli *internet service providers*, dal momento che gli illeciti in rete avvengono, proprio in virtù dell'attività svolta da costoro che dovrebbero, per tale ragione, essere coinvolti nelle responsabilità e nelle operazioni di prevenzione e rimozione dei dati.

l'attenzione e la perizia che gli sono imposte dal tipo di attività esercitata. Ne deriva che, proprio in ragione della particolare caratterizzazione della stessa, l'*hosting provider* attivo potrebbe ricorrere a strumenti tecnici di filtraggio e monitoraggio che individuino la sussistenza di contenuti illeciti -quali, ad esempio, dichiarazioni diffamatorie, piuttosto che espressioni di odio e di razzismo-, al fine di rimuoverli immediatamente o di disabilitarne l'accesso[83]. In altri casi, potrebbe anche impiegare soluzioni, per impedire *a priori* comportamenti illeciti dei propri utenti: in relazione ai siti che pubblichino le recensioni su prodotti e servizi proposti da strutture recettive, l'*hosting provider* potrebbe prevedere un meccanismo - adottato da taluni, come *Airbnb* o *Booking*, e non da altri, quali *TripAdvisor*- che permetta ai fruitori del servizio di pubblicare un'opinione, solamente qualora abbiano effettivamente usufruito del bene o del servizio offerto dall'impresa.

Ne conseguirà[84] che gli *hosting providers* "attivi" che omettano l'uso di tali strumenti tecnici, valutabili alla luce di soluzioni organizzative di un *provider* medio, risponderanno dell'inosservanza degli obblighi di diligenza -cui siano tenuti, in qualità di operatori professionali-, in forza dell'art. 2043 cod.civ., per violazione dei livelli qualitativi da rispettare, nell'esercizio dell'attività economica d'impresa[85].

La loro responsabilità potrebbe escludersi, solo rilevando che l'adozione di tali misure "preventive" dell'evento dannoso non siano esigibili dagli *hosting providers*, in quanto troppo onerose o impossibili da attuare: circostanza che non si verifica tuttavia, come si evince dai potenziali interventi prospettati, nel caso concreto, proprio in ragione della struttura organizzativa sottesa ai fornitori di ospitalità così descritti[86].

---

[83] Per tale soluzione, si v. M. Zarro, *La tutela della reputazione digitale quale* «intangible asset», *op.cit.*, p. 1523.

[84] Si v. M. Gambini, *Diritti di proprietà intellettuale in rete, op.cit.,* p. 139.

[85] Si v. M. Zarro, *La tutela della reputazione digitale quale* «intangible asset», *op.cit,* p. 1524.

[86] Si v. M. Zarro, *La tutela della reputazione digitale quale* «intangible asset», *op.cit,* p. 1524.

6. La responsabilità civile dell'*hosting provider* «attivo» per i contenuti illeciti pubblicati sulla piattaforma digitale da utenti di servizio anonimi o che si esprimano con pseudonimo.

Alla luce di tali riflessioni, si procederà di seguito a rispondere all'interrogativo posto all'inizio se, pur in assenza di una puntuale previsione della direttiva europea che imponga all'*hosting provider* l'identificazione degli utenti della piattaforma digitale gestita, l'*hosting provider* "attivo" debba comunque attivarsi nel reperire e conservare le generalità e gli elementi identificativi dei fruitori del servizio, proprio in ragione del particolare esplicarsi dell'attività svolta.

La questione si pone, dal momento che l'art. 15, comma 2, della direttiva europea prevede che gli Stati membri possano stabilire che gli *internet service providers* siano tenuti a comunicare «senza indugio» alle autorità competenti, a loro richiesta, le informazioni che consentano l'identificazione dei destinatari dei loro servizi «con cui abbiano accordi di memorizzazione dei dati». Il nostro legislatore ha optato per tale soluzione, precisando, in aggiunta, all'art. 17, comma 2, lett. b), d.lgs. 2003/70, che tale comunicazione dovrà essere fornita «al fine di individuare e prevenire attività illecite».

La norma è stata oggetto di interpretazione, diretta a chiarire se costituisca il fondamento normativo di un (potenziale) obbligo dell'*hosting provider* di identificazione dei destinatari del servizio.

Un primo orientamento dottrinale[87], partendo dalla lettura del combinato disposto della norma e del considerando 48 della direttiva sul commercio elettronico – che si impernia sul dovere di diligenza che sia «ragionevole» attendersi dai prestatori di servizi-, perviene alla conclusione che la previsione imporrebbe agli *internet providers* gli obblighi di richiedere ai fruitori del servizio le informazioni che li identifichino, di verificarne la

[87] In tal senso F. Di Ciommo, *La responsabilità civile in Internet: prove di governo dell'anarchia tecnocratica*, in *Resp. Civ.* 2006, p. 562 ss. Valorizza la portata di tale norma, ai fini di fondare la responsabilità civile dei fornitori di servizi *online*, G. M. Riccio, *La responsabilità degli internet* service providers *nel d.lgs. n. 79/2003*, in *Danno e resp.* 2003, p. 1166 ss.

veridicità e di conservarle, per il caso che l'autorità competente ne ordini la trasmissione. In tale ottica[88], la *ratio* della norma sarebbe ravvisabile nell'obiettivo di apprestare un mezzo di tutela per i danneggiati che sia in grado di proteggerli, quando gli autori degli illeciti in rete siano anonimi; l'inadempimento degli obblighi di cooperazione, previsti nella disposizione, quando ne ricorrano tutti i presupposti, determinerebbe, di conseguenza, il sorgere, in capo al *provider*, della responsabilità civile extracontrattuale, ai sensi dell'art. 2043 cod.civ. La dottrina[89] specifica che tale obbligo sarebbe comunque individuabile unicamente in riferimento alla prestazione di servizi che presuppongano un «accordo di memorizzazione dei dati»: ne resterebbero quindi esclusi i servizi, per la prestazione dei quali non sia previamente necessaria la stipula di un contratto, quali, ad esempio, i *forum* di discussione.

Deve, al contrario, concordarsi col diverso indirizzo[90], secondo il quale la norma non farebbe sorgere in capo al *provider* né l'obbligo di richiedere ai fruitori del servizio le informazioni che li identifichino, né l'obbligo di verificare la veridicità delle informazioni da loro trasmesse. La norma imporrebbe piuttosto al *provider* l'obbligo più circoscritto di comunicare al soggetto leso, in sede giudiziaria, su richiesta dell'autorità competente, le informazioni sull'autore dell'illecito «in suo possesso» che permettano l'identificazione dell'utente del servizio – non disponendone in maniera puntuale le modalità[91]. Da tale impostazione si fa derivare che il *provider* potrebbe essere chiamato a rispondere, in sede giudiziaria, solamente nell'ipotesi in cui non trasmetta le informazioni che siano a sua disposizione, in quanto necessarie per l'erogazione del servizio, senza che rilevi la loro veridicità oppure la circostanza che le fornisca in modo parziale o falsato.

---

[88] Si v. C. Menichino, *sub art. 17, d.lgs., 9 aprile 2003, n. 70,* in Aa.Vv., *Codice del Consumo,* a cura di V. Cuffaro, coordinato da V. Barba e A. Barenghi, 3 ed. , Milano, 2012, p. 1273.

[89] Si v. G. Pino, *Assenza di un obbligo generale di sorveglianza a carico degli Internet service providers sui contenuti immessi in rete,* in *Danno e resp*., 2004, p. 839; G. Resta, *Anonimato, responsabilità, identificazione, op.cit.,* p. 182 (§ 4.2.).

[90] Si v. L. Manna, *La disciplina del commercio elettronico*, Padova, 2005, p. 214 s.

[91] Modalità che sono state viceversa precisamente descritte dal legislatore, in una proposta di legge, non ancora approvata (sulla quale si veda *infra* § 6).

Appare evidente come la norma di attuazione della direttiva europea predisponga, in realtà, un «regime di identificazione *a posteriori*» che coinvolge il *provider* in un momento successivo al verificarsi del danno, soltanto qualora l'autorità giudiziaria, a seguito del bilanciamento dei contrapposti interessi, gli ingiunga l'ostensione dei "soli*"* dati identificativi degli utenti della piattaforma, raccolti e conservati[92].

In caso contrario, non si spiegherebbe la ragione per la quale taluni Stati membri dell'Unione Europea, dopo aver recepito la disposizione della direttiva, abbiano, in un secondo momento, dettato apposite norme, per imporre agli *internet service providers* l'obbligo di identificare, in maniera dettagliata (pertanto non solo, ad esempio, attraverso la comunicazione dell'indirizzo *e mail*), gli utenti del servizio, prima di accordare loro l'accesso e la pubblicazione di contenuti sulle piattaforme digitali da loro gestite; disciplinando analiticamente i dati identificativi e statuendo che il *provider* debba raccoglierli e conservarli -pur sempre nel rispetto della disciplina della protezione dei dati personali degli utenti.

Si fa puntuale riferimento alla legislazione francese.

L'art. 6, II, comma 1, legge 21 giugno 2004, n. 575, *pour la confiance dans l'économie numérique***,** di recepimento della direttiva sul commercio elettronico[93], ha previsto che gli *access providers* e gli *hosting providers* (c.dd. *les hébergeurs*) raccolgano e conservino i dati che permettano di identificare chiunque abbia contribuito alla creazione di un contenuto, pubblicato sui portali da loro gestiti, e che l'autorità giudiziaria possa richiedere loro la comunicazione di tali dati.

Successivamente il *Décret en Conseil d'Etat*, 25 febbraio 2011, n. 219, «*relatif à la conservation et à la communication des données permettant*

[92] Si mutua, in tale ambito, l'osservazione fatta da G.M. Riccio, *Anonimato e responsabilità in internet, op.cit., p*. 320, in merito al disegno di legge francese, la proposta *Bloche*, che si poneva nel solco della norma (della quale si sta parlando) della proposta di direttiva sul commercio elettronico.

[93] La legge ha statuito, al *Chapitre* II, «*Les prestataires techniques*», un regime speciale di esonero di responsabilità per il *fournisseur d'accès* (ossia l'*access providers*) che fornisca l'accesso ai servizi di comunicazione, quando non incida in alcun modo sui contenuti trasmessi, e per l'*hébergeur,* ossia l'*hosting provider*. Sul punto si v. M. De Cata, *La responsabilità civile dell'Internet service provider,* Milano, 2010, p. 146.

d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne»[94], ha definito gli obblighi di identificazione cui siano tenuti sia l'*access provider*, sia l'*hosting provider.* In sostanza[95], quando sia stipulato un contratto oppure sia creato un *account* con il fornitore di accesso oppure con il fornitore di ospitalità, costoro dovranno «mettere in opera dei mezzi tecnici per soddisfare le condizioni di identificazione». Tali soggetti dovranno perciò acquisire e conservare, nella misura in cui siano raccolti, i seguenti dati: al momento della creazione dell'*account*, l'identificativo di questa connessione (ad esempio, l'indirizzo *IP* da cui la persona si collega per creare il proprio *account*); il nome e il cognome della persona fisica oppure la ragione sociale della persona giuridica; gli indirizzi postali associati; gli pseudonimi usati; gli indirizzi *e mail* o gli *account* associati; i numeri di telefono; la *password* (se il sistema utilizzato memorizza la *password* in chiaro) e i dati che consentano di verificarla (*hash* o altre tecniche che permettano di memorizzare in modo sicuro una *password*) o di modificarla, nella loro ultima versione aggiornata.

La disciplina[96] descrive, di fatto, precisamente i parametri di diligenza professionale cui debba attenersi il *provider*, in fase preventiva e "precauzionale", rispetto al momento in cui vengano caricati sul sito i contenuti illeciti. Di conseguenza il *provider* che conformi la propria attività professionale alla disciplina particolareggiata finirà col garantire ai terzi lesi dai fruitori del servizio il diritto di attivare rimedi di natura risarcitoria e/o general-preventiva, quand'anche l'autore del contenuto pubblicato si esprima in rete in maniera anonima o con pseudonimo, esperendo l'azione contro il *provider*, al quale l'autorità giudiziaria potrà imporre l'ostensione dei dati identificativi, legislativamente determinati, raccolti e conservati.

Nè si capirebbe la portata dei disegni di legge, approntati di recente da taluni Stati membri (sui quali si v. *infra*) che non solo obbligano gli *internet service providers* ad identificare puntualmente gli utenti del servizio, prima

[94] Ossia «relativo alla conservazione ed alla comunicazione all'autorità giudiziaria dei dati che permettano di identificare qualsiasi fornitore di contenuti messi in rete».
[95] Sul punto si v. E. Freyssinet, *Décret d'application de la LCEN sur la conservation des données par les FAI et hébergeurs,* 4 marzo 2011, in https://blog.crimenumerique.fr/2011/03/04/
[96] Per le riflessioni che seguono, si v. E. Freyssinet, *Décret d'application de la LCEN, loc.op.ult.cit.*

di consentire loro l'accesso e la pubblicazione di informazioni sulle piattaforme digitali, ma prevedono anche, nel caso di inottemperanza all'obbligo, l'irrogazione di sanzioni amministrative.

Ciò detto, se, allo stato attuale, non esiste, nel nostro ordinamento, un obbligo *ex lege*, in capo all'*hosting provider*, di identificazione preventiva degli utenti che pubblicheranno sul portale, potrà cionondimeno delinearsi la responsabilità civile del fornitore del servizio per i contenuti illeciti, pubblicati da utenti che non siano identificabili dal soggetto danneggiato?

Si reputa che la risposta al quesito sia positiva, per i motivi che seguono.

Avendo precipuo riguardo all'*hosting provider "*attivo", si ritiene che il comportamento di identificazione dei fruitori del servizio debba parametrarsi al criterio della diligenza professionale che lo connota[97].

Le piattaforme digitali[98] che forniscano ospitalità ai contenuti pubblicati dagli utenti, nell'impiegare soluzioni organizzative che rispondano al dovere suddetto e siano "ragionevolmente" esigibili, in relazione al tipo di attività economica d'impresa svolta, dovranno attuare tutte le precauzioni necessarie, per impedire la lesione di diritti di terzi. Non si potranno pertanto limitare a richiedere ai fruitori del servizio, ad esempio, il solo indirizzo di posta elettronica, ma saranno tenute ad accertare effettivamente la loro identità.

Conseguentemente si ritiene che, quando l'autorità giudiziaria ordini all'*hosting provider* l'ostensione dei dati identificativi dell'utente (che, alla luce delle prove presentate dal soggetto che asserisca di essere stato leso, abbia presumibilmente tenuto la condotta illecita, imputatagli dall'attore) e il fornitore di ospitalità non li fornisca ovvero fornisca dati non idonei all'identificazione 'reale' dell'utente (a titolo esplicativo, il suo solo indirizzo *e mail*), gli sarà imputabile la responsabilità aquiliana esclusiva, a titolo di colpa omissiva, *ex* art. 2043 cod.civ.

Il fondamento della responsabilità civile è ravvisabile nella circostanza che la mancata 'reale' identificazione dell'utente del servizio da parte del *provider* integrerebbe una violazione colposa dell'obbligo di diligenza

[97] In tal senso, si v. L. Vignudelli, *Il gestore del f*orum: *spunti su identificazione dell'utente, anonimato e (ir) responsabilità,* in *Dir.Informaz. informatica*, 2011, p. 113.
[98] Si condivide la tesi di G.M. Riccio, *Anonimato in rete e responsabilità in internet, op.cit.,* p. 325 ss.

professionale che finirebbe col garantirne «l'irreperibilità, generata dall'anonimato», agevolandone, con «nesso causale diretto», il comportamento illecito ed il verificarsi dell'evento dannoso per un soggetto terzo[99]. Il prestatore che non provveda all'autenticazione dei destinatari dei servizi risponderà, di seguito, in prima persona ed esclusivamente, dei danni provocati ai terzi dagli illeciti commessi da utenti ai quali abbia concesso di restare anonimi e dei quali non sia riuscito a disvelare l'identità[100].

Tale ricostruzione[101] si pone in linea con le argomentazioni addotte dalla giurisprudenza francese, nelle sentenze relative al caso *Lacoste*[102] ed al caso *Hallyday*[103] che rappresentano dei *leading cases* nel panorama della giurisprudenza degli Stati membri dell'Unione Europea. Tali pronunce infatti hanno avuto il merito di rispondere all'esigenza di non lasciare prive di tutela le istanze della persona, offesa da contenuti illeciti pubblicati su una piattaforma digitale, qualora l'autore delle dichiarazioni diffamatorie non sia stato previamente identificato dall'*hébergeur,* configurandone la responsabilità civile extracontrattuale, secondo le regole di diritto comune, per violazione dell'obbligo di diligenza e prudenza[104], cui quest'ultimo sia tenuto, in qualità di professionista.

---

[99] Si v. G.M. Riccio, *Anonimato e responsabilità in internet, op.cit.,* p. 325; L. Vignudelli (*Il gestore del f*orum: *spunti su identificazione dell'utente, op.cit.,* p. 112 s.) afferma che il comportamento del gestore, riconducibile in astratto all'obbligo generale di prudenza e diligenza, costituisce l'unica via, per assicurare l'individuazione e la condanna dell'autore dell'illecito.

[100] Si v. F. Di Ciommo, voce «Internet*. I) Responsabilità civile», op.cit.,* p. 10.

[101] Elaborata da G.M.Riccio, *Anonimato e responsabilità in* internet*, op.cit.,* pp. 325, 331.

[102] Si v. la sentenza del *Tribunal de Grande Instance di Nanterre*, 8 dicembre 1999, in *Dir.informaz.e informatica*, 2000, p. 307, con nota di G.M.Riccio, *Anonimato e responsabilità in* internet*, op.cit.*

[103] Si v. la sentenza della *Cour d'Appel de Paris*, 10 febbraio 1999, in *Dir.informaz. e informatica,* 1999, p. 926, con nota di G.M.Riccio, *La responsabilità del* provider *nell'esperienza francese. Il caso Hallyday*.

[104] Le sentenze francesi, ancor prima dell'introduzione dell'analitica disciplina di autenticazione dei fruitori del servizio, dettata dal *Décret en Conseil d'Etat*, 25 febbraio 2011, n. 219 hanno fatto riferimento agli artt. 1382 e 1382 *code civil*– vigenti al tempo della pronuncia, prima dell'entrata in vigore della riforma del *Code civil* francese, a seguito della quale, dal primo ottobre 2016, le (medesime) disposizioni di cui agli artt. 1382 e 1383 del codice civile napoleonico sono contenute, rispettivamente, negli artt. 1240 e 1241 *code civil.*

Sulla stessa scia, si colloca l'insegnamento della Corte Europea dei diritti dell'uomo che, nella pronuncia Delfi c. Estonia[105], ha posto, in capo agli Stati membri, l'obbligo di adottare misure idonee a tutelare i soggetti lesi dalla pubblicazione di contenuti illeciti su piattaforme digitali, mettendo in evidenza la necessità di identificazione del soggetto responsabile. La Corte ha precisato che, in assenza di una norma che puntualmente imponga ai *providers* l'obbligo di preventiva identificazione dei fruitori del servizio, autori di contenuti caricati sui portali da loro gestiti; in alternativa, spetterà all'autorità giudiziaria impiegare misure in grado di proteggere i soggetti danneggiati da contenuti anonimi, imputando, qualora ne ricorrano i presupposti, la responsabilità civile ai c.dd. fornitori di ospitalità. In particolare, saranno civilmente responsabili gli *hosting providers* che traggano benefici economici, nell'ospitare contenuti illeciti, ammettendone la pubblicazione anche in forma anonima[106].

L'art. 1382 *code civil* ha rappresentato la norma centrale del sistema francese di responsabilità civile, prevedendo che «ogni fatto dell'uomo, che causa danno ad altri, obbliga colui, per la cui colpa è avvenuto, a risarcirlo»; l'art. 1383 *code civil* ha dettato il principio della sussistenza della responsabilità non solo per i danni imputabili a fatto proprio, ma anche per tutti i danni, cagionati per negligenza o imprudenza. La medesima disciplina di tali due norme è contenuta, a partire dal primo ottobre 2016, negli artt. 1240 e 1241 *code civil*, modificati dall'art. 2 dell'*ordinnance* del 10 febbraio 2016, n. 131. La riforma del codice civile francese ha operato una modifica della collocazione topografica della responsabilità extracontrattuale. Sulla riforma della responsabilità in Francia, si v. G. Alpa, *Riforma della responsabilità civile francese,* in *Contr.impr.,* 2018, p. 1 ss.

[105] La Corte si è inizialmente espressa in camera singola, il 10 ottobre 2013, App. n. 64569/09 (decisione pubblicata in *Quad.cost.*, 2014, pp. 457 ss., con nota di G.E.Vigevani, *La responsabilità civile dei siti per gli scritti anonimi: il caso Delfi c. Estonia*) e successivamente, in composizione di *Grand Chambre,* il 16 giugno 2015, confermando la decisione presa inizialmente (in *www.echr.coe.int*). La Corte è stata chiamata a decidere sul bilanciamento tra l'esigenza di garantire la libertà di espressione degli utenti di un portale ed il diritto al rispetto della vita privata di soggetti terzi danneggiati da dichiarazioni diffamatorie, ivi pubblicate in forma anonima. La Corte EDU ha ritenuto che la decisione del giudice estone avesse raggiunto tale equilibrio, condannando un gran portale di informazione che operava sia in veste di editore, pubblicando *on line* articoli di giornale, sia in veste di *hosting provider*, mettendo a disposizione degli utenti della piattaforma appositi spazi, a margine degli articoli, sui quali questi ultimi potevano esprimere le proprie opinioni, anche in forma anonima.

[106] La Corte ha suggerito il metodo- già previsto nel settore della stampa, nel quale, per ogni scritto illecito, deve essere individuabile un soggetto responsabile che sia l'autore, il direttore o lo stampatore- di imputare la responsabilità civile al soggetto che tragga benefici economici

Deve puntualizzarsi che la Corte EDU, a seguito della contestazione che l'indirizzo tracciato determinerebbe il rischio che i gestori delle piattaforme digitali diano vita a forme di censura preventive, per evitare di incorrere in responsabilità civile[107], è poi pervenuta ad un'interpretazione restrittiva della *ratio decidendi* della pronuncia della *Grande Chambr*e[108]. In successive decisioni[109], è stato così chiarito come il far ricadere la responsabilità civile "in modo automatico" sui gestori dei siti, per i danni provocati sui portali da dichiarazioni diffamatorie anonime di utenti (come nei casi specifici, e da contenuti illeciti in senso ampio), possa avere conseguenze negative sulla loro attività, inducendoli a chiudere lo spazio preposto ai commenti oppure a controllare, in maniera non imparziale, i contenuti delle recensioni, per poi eliminarli in modo arbitrario[110], provocando, in tal guisa, i paventati *chillings effects* sulla libertà di espressione in rete.

Dalla lettura delle argomentazioni delle decisioni assunte, emerge come la linea direttrice, tracciata dalla Corte Europea dei diritti dell'uomo, indirizzi i

---

dalla pubblicazione di commenti. Sul punto si v. G. E. Vigevani, *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano, op.cit*., p. 218 (§ 6).

[107] Si è sostenuto (G.E.Vigevani *La responsabilità civile dei siti per gli scritti anonimi: il caso Delfi c. Estonia, op.cit.*, p. 502) che costoro, spinti esclusivamente da interessi di carattere economico, potrebbero essere indotti ad eliminare arbitrariamente non solo i messaggi davvero illeciti, ma anche quelli "pericolosi", in quanto aventi ad oggetto confutazioni severe nei confronti di terzi. D'altra parte, le medesime critiche furono mosse alle pronunce francesi suddette da parte dalla dottrina che manifestò il rischio di *overdeterence*, in quanto molti *providers* oscurarono numerosi siti, per il timore di essere poi ritenuti responsabili dei contenuti illeciti ospitati. Sul punto si v. M. De Cata, *La responsabilità civile dell'Internet service provider*, *op.cit*., p. 137.

[108] Si v. R. Petruso, *Responsabilità delle piattaforme* online*, oscuramento di siti* web *e libertà di espressione nella giurisprudenza della Corte europea dei diritti dell'uomo*, in *Riv.informaz. e informatica,* 2018, p. 515 (§ 2.3).

[109] Si v. la sentenza Corte EDU, 2 febbraio 2016 (ric. N. 22947/13), pronunciata in merito al caso *Magyar Tartalomszolgáltatók Egyesülete e Index.HU ZRT c.* Ungheria (caso n. 22947/13). La pronuncia è pubblicata in www.echr.coe.int; per un commento si v. F. Falconi, *La responsabilità dell'*internet provider *tra libertà di espressione e tutela della reputazione altrui*, in *La Comunità internazionale,* 2016, p. 240. Si focalizzi l'attenzione anche sulla sentenza Corte EDU, 9 marzo 2017 (ric. N. 74742/2014), relativa al caso *Rolf Anders Daniel Pihl c.* Svezia, disponibile in www.echr.coe.int. Per un commento si v. R. Petruso, *Responsabilità delle piattaforme* on line*, oscuramento di siti* web *e libertà di espressione*, *op.cit.*, p. 514 (2.3.).

[110] Si v. S. Vimercati, *La Corte di Strasburgo torna sulla responsabilità del gestore del sito: il caso Rolf Anders Daniel Pihl c. Svezia*, in www.medialaws.it, 11 ottobre 2017.

giudici nazionali a valutare la sussistenza o meno della responsabilità civile dei fornitori di ospitalità sul proprio portale, operando un «ragionevole»[111] bilanciamento degli interessi coinvolti nel caso concreto[112].

Per quanto attiene la posizione giuridica degli *hosting provider* "attivi", i giudici dovranno valutare che costoro, in quanto esercenti un'attività imprenditoriale, sono tenuti ad operare sul mercato digitale, conformandosi a *standard* elevati di diligenza professionale; circostanza dalla quale far discendere l'obbligo all'impiego di misure "precauzionali", rispetto al momento in cui vengano caricati sul sito i contenuti da parte dei frutitori del servizio. I *providers* saranno così tenuti ad identificare questi ultimi, prima di consentire loro l'accesso alle piattaforme digitali gestite, ed a conservare, nel rispetto della normativa della protezione dei dati personali, le informazioni raccolte, per le ipotesi in cui, in sede giudiziaria, ne venga richiesta l'ostensione.

L'adempimento di tale obbligo da parte dei fornitori di ospitalità, che si esplichi permettendo agli utenti del portale, secondo la tecnica dell'«anonimato protetto»[113], la possibilità di interagire in rete anonimamente o con pseudonimo, condurrà a salvaguardare due interessi: sia l'interesse/«l'aspirazione» del fruitore del servizio «a non rivelare la propria identità nell'esercizio della libertà d'espressione»[114]; sia l'interesse dei soggetti danneggiati alla tutela giurisdizionale effettiva dei propri diritti.

---

[111] Sulla «ragionevolezza» quale «canone ermeneutico ed argomentativo», «filo conduttore» di ogni ragionamento giuridico, per il contemperamento di principi ed interessi, in coerenza col sistema giuridico di riferimento e tutti i suoi valori, cfr. G. Perlingieri, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015, pp. 16-29, p. 43, p. 135.

[112] Più precisamente i giudici, al fine di individuare la disciplina «più adeguata» al caso concreto, dovranno valutare il fatto, operando un bilanciamento tra gli interessi, i principi ed i valori normativi che esso ha espresso, avendo riguardo al contesto storico-giuridico di riferimento. Si v. P. Perlingieri, *Formazione dei giudici e Scuola superiore della magistratura*, in *Giust.proc.civ.*, 2007, p. 313 che afferma che il «bilanciamento degli interessi e dei valori, ragionevolezza, adeguatezza, proporzionalità, valenza dei principi sono canoni ermeneutici (…) che, come tali, contribuiscono (insieme) al ridimensionamento di vecchi brocardi, duri a morire, come *in claris non fit interpretatio* e *dura lex sed lex*, che dovranno essere (…) conformi alla legalità costituzionale ed europea».

[113] Prospettata da R. Natoli, *La tutela dell'onore e della reputazione in internet, op.cit.*, p. 443.

[114] Secondo la locuzione impiegata dalla Corte europea dei diritti dell'uomo, nella sentenza Delfi c. Estonia citata, al punto 92.

Nel caso in cui i contenuti illeciti ledano i diritti di terzi, sarà quindi compito dell'autorità giudiziaria, nell'operazione di contemperamento dei contrapposti interessi, pervenire ad una decisione che garantisca ai soggetti danneggiati adeguata ed effettiva tutela giurisdizionale delle posizioni soggettive lese, assicurando che, qualora non siano ristorabili dall'autore anonimo (o che abbia agito con pseudonimo) del contenuto illecito, in quanto non rintracciabile, entri in gioco la responsabilità civile di coloro che abbiano facilitato la condotta illecita, omettendo la misura precauzionale dell'identificazione dello stesso.

Ciò detto, si formula, in via conclusiva, l'auspicio che, nel nostro ordinamento, si consolidi un filone giurisprudenziale in tale direzione. Ad oggi, poche sono le pronunce in tal senso.

Appaiono, senza dubbio, condivisibili le conclusioni cui è pervenuto il Tribunale di Venezia, con l'ordinanza del 24 febbraio 2015[115], adottata nell'ambito di un procedimento cautelare, ai sensi dell'art. 700 cod.proc.civ. Il provvedimento ha qualificato il portale *TripAdvisor* come *hosting provider* "attivo", sostenendo che esso agisca quale erogatore di un «servizio integrato» che offre prestazioni aggiuntive, rispetto alla mera intermediazione di dati ed informazioni, per ottimizzare il funzionamento della piattaforma e per fornire agli utenti «consigli affidabili di veri viaggiatori», ponendosi, di conseguenza, nei loro confronti come una fonte di informazione qualificata. Il giudice che, in sede cautelare, ha ordinato a *TripAdvisor* di rimuovere la recensione controversa su un ristorante, dopo aver accertato i suoi contenuti diffamatori e anche non veritieri, ha svolto anche considerazioni che sono entrate nel merito della questione. Precipuamente dalla connotazione del gestore del portale quale *hosting provider* "attivo" l'autorità giudiziaria ha fatto discendere, in linea con l'orientamento dei *leading cases* francesi, che costui debba rispondere direttamente degli illeciti commessi dai propri utenti «allorquando, con la propria condotta omissiva, magari anche solo di tipo colposo, abbia facilitato/favorito l'illecito altrui»; sottolineando come l'attività di controllo

[115] Pubblicata in *Corr.giur*., 2016, p. 78 ss., con nota di R. Gelli, *False recensioni su Tripadvisor, op.cit*. Per le notazioni che seguono sui punti salienti della pronuncia, si v. L. Vizzoni, *Recensioni non genuine su Tripadvisor; quali responsabilità?, op. cit*, p. 713, (§ 5).

sull'autenticità delle recensioni sia dovuto, anche in considerazione della circostanza che le modalità di funzionamento della piattaforma permettono agli utenti di esprimersi in forma anonima, "garantendosi" così, di fatto, l'anonimato del recensore. In sostanza, in ragione di quanto stabilito, in via generale, dall'art. 2043 cod.civ., sussisterebbe sul fornitore di ospitalità, prima ancora dell'obbligo di risarcire il danno, l'obbligo di prevenirlo e di controllare le recensioni postate dagli utenti e quindi anche l'obbligo di identificarli, al fine di impedire quelle che siano apertamente diffamatorie e quelle che non siano state pubblicate da veri viaggiatori.

A diversa conclusione è pervenuto il Tribunale di Grosseto che si è pronunciato, con sentenza del 12 giugno 2016, n. 46, sull'azione promossa dal titolare di una struttura alberghiera che, danneggiato dalla pubblicazione di una recensione negativa, da lui considerata falsa e diffamatoria, ha richiesto il riconoscimento della responsabilità civile concorrente di *TripAdvisor*: responsabilità, secondo il ricorrente, imputabile al portale, per non aver né impedito, né rimosso la pubblicazione, a seguito di segnalazione, e per non aver consegnato all'impresa i dati identificativi dell'autore della dichiarazione. Il Tribunale ha innanzitutto sostenuto che *TripAdvisor* debba essere qualificato come *hosting provider* passivo, poiché non "interferisce" con il contenuto delle recensioni pubblicate, sebbene abbia adottato filtri automatizzati, volti a bloccare la pubblicazione di recensioni espressamente inopportune o fraudolente; per poi escludere la configurabilità, in capo a quest'ultimo, di una responsabilità per gli illeciti commessi dai propri utenti, non essendo, in ogni caso, tenuto a controllare preventivamente i contenuti pubblicati sulla piattaforma, in conformità a quanto disposto dagli artt. 16 e 17 del d.lgs. 70/2003[116].

In tale panorama giurisprudenziale, in cui poche sono le pronunce sul tema e gli orientamenti giurisprudenziali sono difformi, assume preminente rilevanza la sentenza del Consiglio di Stato, 15 luglio 2019, n. 04976, in merito alla portata del controllo che gli *hosting providers* debbano effettuare

[116] Per un commento alla decisione, inedita (di cui un riassunto è in www.blogstudiolegalefinocchiaro.it), si v. M. Simoni, *La responsabilità degli* hosting provider *quali prestatori "automatici, tecnici e passivi" della società dell'informazione*, in *Dir.ind*., 2017, p. 455 ss.

sui contenuti pubblicati dagli utenti del servizio, ponendo l'accento sulla necessità della verifica dell'esistenza degli stessi.

Il Consiglio di Stato ha accolto il ricorso, presentato dall'Autorità Garante della Concorrenza e del Mercato che ha richiesto la riforma della sentenza del T.A.R. Lazio –che aveva annullato la sanzione pecuniaria che l'Autorità aveva irrogato a *TripAdvisor*, per una pretesa pratica commerciale scorretta, consistente nella diffusione di informazioni ingannevoli sulle fonti delle recensioni[117].

Il Consiglio di Stato ha irrogato al gestore del portale una sanzione pecuniaria amministrativa per pratica commerciale scorretta, sostenendo che la condotta del *provider* sia idonea a «falsare in misura apprezzabile il comportamento del consumatore medio in relazione ai servizi promossi» dalla piattaforma.

La pronuncia evidenzia come sia compito degli *hosting providers* imporre rigide linee guida alle quali gli utenti del servizio debbano attenersi,

[117] Si fa riferimento al provvedimento del 19 dicembre 2014, con il quale l'*Antitrust* aveva accertato la scorrettezza della pratica commerciale realizzata da *TripAdvisor*, dal settembre 2011, inibendone la continuazione ed irrogando una sanzionae amministrativa in solido in capo a *TripAdvisor LLC* (società statunitense) e *TripAdvisor Italy* s.r.l. L'Autorità aveva rilevato come il gestore del sito promuova l'affidabilità e l'attendibilità delle recensioni pubblicate, con la conseguenza di far credere ai consumatori medi che si tratti di recensioni autentiche e genuine, postate sul portale da veri viaggiatori, ed aveva anche puntualizzato come tali condotte commerciali del *provider* assumano un ruolo centrale, nell'indirizzare le decisioni dei consumatori. Si puntualizzava che il gestore del sito non esegue controlli in tal senso e che la diffusione di pratiche commerciali tramite *internet* rafforzerebbe il carattere ingannevole delle informazioni diffuse sul portale. Di seguito, il TAR Lazio ha accolto, con sentenza 13 luglio 2015, n. 9355, la domanda delle due società sanzionate che hanno proposto ricorso amministrativo, capovolgendo la decisione dell'Autorità e confutando la responsabilità del gestore del portale per le pubblicazioni dell'utente. Il giudice amministrativo ha affermato che le recensioni pubblicate sul sito debbano intendersi come «vere», nel senso che «costituiscono opinioni di gente comune e non di professionisti renumerati a tale scopo, come facilmente percepibile». Se quindi le valutazioni non possono essere ricondotte a *TripAdvisor*, si giunge alla conclusione che il *provider* non possa influenzare le scelte dei consumatori e che debba così escludersi la sussistenza di una pratica commerciale scorretta. Tanto più che, secondo il giudice amministrativo, l'internauta che consulti siti, quali *TripAdvisor*, avrebbe una certa dimestichezza nel vagliare le opinioni espresse sulle strutture recettive. Per il commento alle due decisioni si v. L. Vizzoni, *Recensioni non genuine su Tripadvisor; quali responsabilità?, op. cit*, p. 713 ss. (§ 6).

individuare metodi idonei a rimuovere prontamente le recensioni che si discostino dalle stesse e approntare strumenti di controllo, idonei a verificare che il recensore quantomeno esista[118].

La decisione, incoraggiando gli *hosting providers* ad adottare "misure proattive" per contrastare gli illeciti *on line*, rispecchia l'esigenza, sempre più avvertita anche dalle Istituzioni europee, di una maggiore responsabilizzazione dei prestatori di servizi ed evidenzia come costoro debbano adoperarsi, in particolare, anche sul piano dell'identificazione degli utenti e del controllo della veridicità delle informazioni da questi fornite.

7. Prospettive *de jure condendo*

La ricostruzione nei termini suddetti della responsabilità civile dell'*hosting provider* per la pubblicazione di contenuti illeciti di utenti anonimi o che abbiano usato uno pseudonimo assume nuova valenza, di recente, per due ragioni.

Innanzitutto si sta assistendo, nell'ambito di taluni Stati membri dell'Unione Europea, all'emanazione di disegni di legge che impongono ai *providers* l'obbligo di identificazione degli utenti del servizio, prima del loro accesso ai portali gestiti, statuendo l'irrogazione di una sanzione amministrativa, nel caso di inottemperanza. Ne deriva che, in una prospettiva *de jure condendo*, all'introduzione *ex lege* di tale obbligo conseguirà che la mancata identificazione dell'utente, da parte del fornitore del servizio, integrerà, *ex se*, gli estremi di una condotta illecita, dalla quale far discendere, in caso di mancata ostensione, per ordine dell'autorità giudiziaria, dei dati identificativi dello stesso al terzo danneggiato, la responsabilità civile per i danni derivanti a costui dai contenuti illeciti pubblicati anonimamente ovvero con pseudonimo sulla piattaforma digitale.

[118] Si v. D. Marino, *Recensioni false: TripAdvisor sanzionata dal Consiglio di Stato, 19 luglio 2019*, in https://www.personaedanno.it/articolo/recensioni-false-tripadvisor-sanzionata-dal-consiglio-di-stato

Si menzioni, *in primis*, l'art. 1 del disegno di legge italiano n. 4692, «Introduzione del divieto dell'uso anonimo della rete *internet* e disposizioni in materia di tutela del diritto all'oblio», presentato alla Camera dei Deputati, il 10 ottobre 2017. La norma ha introdotto il divieto di immettere, in maniera anonima nel *web*, contenuti in qualsiasi forma (testuale, sonora, audiovisiva o informatica, comprese le banche dati), imponendo agli *internet service providers* che gestiscano le piattaforme digitali, destinate alla pubblicazione ed alla diffusione di informazioni presso il pubblico, l'obbligo di registrare gli utenti, tramite il loro nome, la parola d'accesso, l'indirizzo di posta elettronica ed il codice fiscale; statuendo, per coloro che non ottemperino, la punizione al pagamento di un'ammenda pari a cinque milioni di euro. In aggiunta, secondo una prassi già adottata da alcuni *providers* (quali, ad esempio *Airbnb*), si dispone che, terminata la procedura di registrazione, il sistema dovrebbe inviare un messaggio elettronico di conferma dell'iscrizione all'indirizzo di posta elettronica inserito, attraverso il quale il destinatario, ove diverso dall'utente registrato, potrebbe effettuare l'apposita segnalazione.

Si richiami altresì il disegno di legge austriaco (134/ME XXVI. GP - *Ministerialentwurf – Gesetzestext)*, presentato il 10 aprile 2019[119] dal Governo di destra conservatore austriaco di ÖVP e FPÖ, il cui titolo è «*Bundesgesetz über Sorgfalt und Verantwortung im Netz*» («Legge federale sulla diligenza e la responsabilità in rete»), definito all'interno del Governo «Divieto digitale del mascheramento».

Il provvedimento[120] statuisce, al § 1, che i prestatori di servizi *internet* che dovranno sottostare alla legge saranno obbligati a pretendere dagli utenti la creazione di un profilo di registrazione, prima di consentire loro di pubblicare. La finalità di tali previsioni è promuovere un'interazione rispettosa tra gli utenti e facilitare l'esperimento dell'azione giudiziaria da parte dei soggetti lesi da contenuti illeciti. L'obbligo graverà, dal 2020, in capo ai gestori di piattaforme che abbiano centomila o più utenti ovvero un fatturato maggiore dei cinquecentomila euro: disposizione dalla quale deriva

[119] Pubblicato in https://www.parlament.gv.at/

[120] Per il commento che segue nel corpo del testo, si v. *Österreich plant Identifizierungspflicht im Internet,* in *https://www.br.de/nachrichten/netzwelt/ oesterreich-plant-identifizierungspflicht-im-internet, RNEQgDJ,* 10 aprile 2019.

l'applicabilità anche ad *internet providers* internazionali, quali *Facebook*, *Twitter* ed *Instragram* che dovranno nominare un responsabile per l'intera Austria che garantirà il rispetto delle nuove norme e dovrà intervenire rapidamente. I *providers* che non ottemperino a tale obbligo potranno essere soggetti a sanzioni amministrative, fino ad un ammontare di cinquecentomila euro. Gli utenti dovranno creare un profilo di registrazione, indicando, in ogni caso, il proprio nome e cognome ed indirizzo, fermi restando gli obblighi di protezione dei dati personali cui i *providers* saranno tenuti: nel trasmetterli all'autorità competente, dovranno difatti conformarsi a quanto stabilito dal § 4 del progetto di legge. Gli utenti, previamente identificati dai *providers*, potranno pur sempre interagire sui portali con nomi di fantasia. Si consideri infine che il disegno di legge non ha prestabilito le modalità, con le quali i *providers* dovranno identificare gli utenti, giacché si è pensato di lasciarli liberi, dal momento che potrebbero esservi opzioni migliori e più economiche rispetto ad altre - pur essendo stato specificato nei lavori preparatori che, senza dubbio, sarebbe possibile, ad esempio, attraverso il numero di cellulare, il codice SMS e la conferma di ricezione dello stesso.

In ambito europeo la Commissione ha adottato, negli ultimi anni, una serie di atti di *soft law*[121], nei quali ha fornito agli Stati membri incisivi *incipit* nella promozione della responsabilizzazione degli *hosting providers*

[121] Si precisa (A. Algostino, *La* soft law *comunitaria e il diritto statale: conflitto fra ordinamenti o fine del conflitto democratico*? in *www.costituzionalismo.it*, 2016, fasc. 3, p. 256, pp. 258 ss., pp. 267-268) che la locuzione «*soft law*» si riferisce ad una pluralità di atti eterogenei che, «nella duttilità e flessibilità di forme e legittimazione», presentano l'elemento in comune di esercitare effetti giuridici rilevanti, sebbene non abbiano efficacia giuridica vincolante. In tale contesto la *soft law* può scaturire sia dalle istituzioni pubbliche, sia da soggetti privati, sia dalla combinazione dell'operato dei soggetti pubblici o privati. Altra dottrina (A. Poggi, *Soft law nell'ordinamento comunitario,* in *www.astridonline*, p. 4 che condivide l'orientamento di L. Selden, *Soft Law in European Community Law*, Oxford, 2004, p.112) ha poi puntualizzato come gli atti di *soft law* vengano normalmente classificati, sulla base della funzione che svolgono, in tre categorie: gli atti di *«pre-law»* -ossia gli strumenti preparatori di atti giuridici vincolanti, come i Libri bianchi, i Libri Verdi-; gli atti di «*post-law»* -vale a dire gli strumenti di interpretazione di atti vincolanti, quali le comunicazioni interpretative, le linee guida ed i codici di condotta- e gli atti di *«para-law»* qualificabili come strumenti alternativi ad atti vincolanti, tra i quali si fanno rientrare le comunicazioni non interpretative, le raccomandazioni ed i pareri.

maggiore, rispetto a quella prevista nella disciplina attualmente vigente. L'obiettivo perseguito è la modernizzazione della normativa, in considerazione dell'evoluzione tecnologica che si è avuta, rispetto al momento dell'emanazione della direttiva *e-commerce*, e di aggiornamento della stessa, al fine di colmare le lacune e superare le incertezze sollevate, nel corso del tempo, dall'applicazione della disciplina europea e delle legislazioni nazionali di recepimento.

Per questa via, la Commissione Europea, il 6 maggio 2015, ha emanato una Comunicazione[122] al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle regioni, dal titolo «Strategia per il mercato unico digitale»[123]. Al punto 3.3.2. «Contrasto ai contenuti illeciti su *internet*», la Commissione Europea, nel constatare che, in più della metà dei casi, gli interventi contro i contenuti illeciti sono spesso inefficaci e poco trasparenti e che le divergenze tra le diverse prassi nazionali possono ostacolare il rispetto delle norme e minare la fiducia degli utenti nel mondo *online*, ha posto la questione sull'opportunità di innalzare il livello generale di protezione dal materiale illecito su *internet*. La Commissione si è riproposta pertanto di vagliare l'esigenza di presentare nuove misure, al fine di fronteggiare i contenuti illeciti in *internet* e di valutare, a tale scopo, l'opportunità di imporre ai *providers* «di esercitare una maggiore responsabilità e diligenza nella gestione delle reti e dei sistemi (doveri di diligenza)».

Di qui hanno fatto seguito ulteriori interventi della Commissione europea.

Si segnala la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, del 28 settembre 2017, dal titolo «Lotta ai contenuti illeciti *online*. Verso una maggiore responsabilizzazione delle piattaforme *on line*»[124].

La Commissione europea si è impegnata a verificare l'esigenza di prevedere nuove misure, per garantire l'efficienza e la tempestività degli interventi dei

[122] Si ritiene (A. Poggi, *Soft law nell'ordinamento comunitario, op. cit*., p. 18) che le Comunicazioni costituiscano la tipologia di *soft law* più consistente nei settori strategici per la realizzazione del mercato comune: esse sono difatti costruite con la finalità di indirizzare, in determinati settori, l'attività degli Stati membri e dei soggetti privati – nel caso specifico, gli *internet service providers*.

[123] Documento COM (2015) 192 *final.*

[124] Documento COM (2017) 555 *final.*

providers, non solo nella fase di rimozione dei contenuti illeciti, ma altresì nell'ottica della loro prevenzione. A tal fine, si delinea la valutazione dell'adozione di eventuali misure legislative da parte degli Stati membri, al fine di aggiornare ed adeguare il quadro normativo attualmente vigente[125].

La Comunicazione[126] ha offerto una serie di orientamenti e principi, per indirizzare gli *hosting providers* ad incrementare la lotta contro i contenuti illeciti *online*, in cooperazione con le autorità nazionali, con gli Stati membri e con i portatori di interessi pertinenti. Si è posta la finalità di agevolare ed intensificare l'attuazione di "buone pratiche", non solo al fine di rimuovere e disabilitare l'accesso a contenuti illeciti che siano stati segnalati ai *providers*, ma anche per individuarli e prevenirli, mediante l'impiego, da parte di questi ultimi, di «misure proattive». La Commissione ha rilevato come le piattaforme digitali dispongano, ad oggi, solitamente di «mezzi tecnici per identificare e rimuovere» i contenuti illeciti e che, alla luce del «progresso tecnologico nell'elaborazione di informazioni e nell'intelligenza artificiale», l'utilizzo delle tecnologie di individuazione e di filtraggio automatico sta divenendo uno strumento ancora più importante, per contrastare i contenuti illeciti *online*.

Alla Comunicazione ha fatto seguito la Raccomandazione (UE), 1 marzo del 2018, n. 334, della Commissione Europea «sulle misure per contrastare efficacemente i contenuti illegali *on line*».

Tale atto[127] si è posto nel solco dell'orientamento politico già enunciato dalla Commissione Europea nella Comunicazione del 2017, con l'obiettivo di darvi concreta attuazione. Il provvedimento, seppur privo, *ex* art. 288 del TFUE, di efficacia vincolante nei confronti degli Stati membri dell'Unione Europea ai quali è diretto, seppur e sebbene inidoneo ad imporre obblighi giuridici, ha ciononostante posto una serie di princípi comuni non vincolanti, suggerendo loro delle linee guida di azione[128].

---

[125] Si v. M. Mazzonetto, *Il problema dei contenuti illegali on-line: la risposta della Commissione Europea*, 29 marzo 2018, in *www.dirittodellinformatica.it*

[126] Come precisato nel punto 1 «Introduzione».

[127] Sul punto si v. M. Mazzonetto, *Il problema dei contenuti illegali on-line, loc.op.ult.cit.*

[128] La raccomandazione è una fonte del diritto europeo, qualificabile, come visto, come atto di *soft law*. Tale provvedimento può essere rivolto sia agli Stati membri, sia ai soggetti di diritto interno, operanti nel settore di riferimento. La raccomandazione

Il provvedimento incisivamente esordisce, al punto 1, Capo I, «Obiettivo e definizioni», dichiarando che, in riferimento ai contenuti pubblicati dagli utenti delle piattaforme digitali, gli Stati membri ed i fornitori del servizio di ospitalità sono «incoraggiati ad adottare misure effettive, appropriate e proporzionate», per contrastare i contenuti illeciti *on line*, in conformità ai principi stabiliti nella Raccomandazione stessa[129].

Si prevede[130] «un doppio canale di misure», destinate ad elevare gli *standard* di diligenza degli *hosting providers*: ossia interventi sia *ex post*, sia *ex ante*.

Sul piano della prevenzione, la Commissione, al fine di garantire una risposta più rapida nella rilevazione e successiva rimozione dei contenuti illeciti, prevede innanzitutto il rafforzamento: della collaborazione tra i prestatori di servizi di *hosting* che, ove opportuno, dovrebbero condividere tra loro esperienze, soluzioni tecnologiche e le "buone pratiche", anche dando luogo ad iniziative di cooperazione, relative a codici di condotta, protocolli d'intesa ed altri accordi volontari[131]; della collaborazione tra *hosting providers* e gli Stati membri che dovrebbero predisporre procedure accelerate, per trattare le segnalazioni che provengano dalle autorità competenti[132]; della collaborazione tra gli *hosting providers* ed i «segnalatori attendibili» («comprese le organizzazioni non governative e le associazioni

---

permette alle istituzioni europee di rendere note le proprie posizioni sull'evoluzione futura della propria azione e di suggerire linee di azione, senza imporre obblighi giuridici a carico dei destinatari. Sul punto si v. G. Tesauro, *Diritto Comunitario*, *terza ed.,* Padova, 2003, pp. 144-146; https://europa.eu/european-union/eu-law/legal-acts_it.

[129] Oltre che nel rispetto della Carta dei diritti fondamentali dell'Unione Europea: precisamente nel rispetto del diritto alla libertà di espressione e di informazione, del diritto alla protezione dei dati personali e di altre disposizioni europee, relative al commercio elettronico ed alla concorrenza.

[130] Sul punto, si mutuano le notazioni di G.G.Codiglione (*La nuova legge tedesca per l'enforcement dei diritti sui social network*, in *Dir.informaz. e informatica*, 2017, p. 734 s.), di commento alla Comunicazione COM (2017) 555 *final*, *supra* menzionata.

[131] Coinvolgendo, in particolare, gli *hosting providers* che abbiano risorse limitate, in ragione della loro dimensione o della scala sui cui operino. Si v. punto 28, Capo II, «Collaborazione tra prestatori di servizi di *hosting*».

[132] Si v. punto 23, Capo II, «Collaborazione tra prestatori di servizi di *hosting* e gli Stati membri».

di categoria»)[133], realizzabile tramite la previsione di procedure accelerate, per il trattamento delle segnalazioni di questi ultimi, e la pubblicazione di condizioni chiare e obiettive, per stabilire quali soggetti, che dispongano di competenze necessarie e svolgano la propria attività in modo diligente, possano essere così qualificati[134].

Il provvedimento, facendo proprio il contenuto della Comunicazione, promuove in maniera più analitica l'adozione, da parte degli *hosting providers*, di «misure proattive opportune, proporzionate e specifiche» che siano efficaci, nell'individuare e rimuovere i contenuti illeciti, per ridurre i rischi di lesione dei diritti di terzi[135]. Tali misure potrebbero comprendere l'uso di strumenti automatizzati, solo quando ciò risulti «appropriato e proporzionato», in taluni casi sotto il controllo dell'intervento umano, e pur sempre a condizione che siano accompagnate da «garanzie effettive ed appropriate», in particolare da «misure di salvaguardia», di cui ai punti 19 e 20.

Nell'ambito delle misure operative che gli *hosting providers* debbano adottare *ex post*, la Raccomandazione, al fine di aumentare le tutele dei soggetti danneggiati dagli utenti delle piattaforme digitali, stimola l'impiego di misure idonee a garantire una risposta più veloce ed efficace, sia nel rimuovere i contenuti illeciti, pubblicati sui portali, sia nel rilevarli – ponendo particolare accento sulle modalità di funzionamento del meccanismo della segnalazione degli illeciti ai *providers* da parte dei soggetti privati lesi ovvero da parte di «segnalatori attendibili».

Il provvedimento invita gli Stati membri ad agevolare la soluzione stragiudiziale delle controversie, relative alla rimozione di contenuti illegali o alla disabilitazione dell'accesso ai medesimi, ed incoraggia gli *hosting providers* a consentire l'uso di meccanismi per la risoluzione stragiudiziale medesima, se disponibile negli Stati membri[136].

Si osservi infine che la Raccomandazione non pone in discussione il regime speciale di responsabilità degli *internet service providers*, in linea con

[133] Si v. considerando 29 della Raccomandazione.
[134] Si v. i punti 25, 26, 27, Capo II, «Collaborazione tra i prestatori di servizi di *hosting* e i segnalatori attendibili».
[135] Si v. punto 18, Capo II, «Misure proattive».
[136] Si v. i punti 14, 15, Capo II, «Risoluzione extragiudiziale delle controversie».

la Comunicazione 28 settembre 2017, ove si puntualizza che l'adozione di misure proattive da parte dei *providers* non implica, di per sè, automaticamente che l'*hosting provider* vada collocato tra gli *hosting* "attivi", con la conseguente perdita del beneficio dell'assoggettabilità dello stesso al regime speciale di responsabilità civile, tracciato dalla direttiva europea. La Commissione ha chiarito (punto 3.3.1.) che i fornitori di ospitalità non dovranno essere scoraggiati, nell'adozione di misure proattive efficaci, dal timore della perdita del beneficio della deroga alla responsabilità civile[137].

La Commissione europea non intende difatti sovvertire il «regime di favore», introdotto dalla disciplina europea della responsabilità civile degli *internet service provider*, e ciò appare evidente dalla circostanza che le «misure proattive» previste non intaccano il principio generale, in forza del quale non gravi, in capo a nessuno dei fornitori di servizi *on line*, né l'obbligo generale di sorveglianza delle informazioni che trasmettono e memorizzano, né l'obbligo generale di ricerca attiva di fatti o circostanze che indichino la presenza di attività illecita.

Alla luce di tali osservazioni, può affermarsi[138] che la linea direttrice della Raccomandazione sia la promozione della diffusione, su tutto il territorio dell'Unione Europea, di una «responsabilità sociale d'impresa». La Commissione europea stimola la responsabilizzazione sociale degli *hosting providers,* quale strumento che «dal basso» contrasti la diffusione di contenuti illeciti *on line*.

A tal uopo, sebbene la Raccomandazione non abbia carattere vincolante, non si esclude che possa produrre effetti giuridici a livello nazionale[139], sia stimolando gli *hosting providers* ad impiegare le misure operative

[137] Tanto più che tali obblighi preventivi sembrano collocarsi nell'ambito del considerando n. 48 della direttiva 2000/31/CE che prevede che la medesima non pregiudica la possibilità degli Stati membri di chiedere ai prestatori di servizi, che abbiano informazioni sui loro utenti, «di adempiere al dovere di diligenza che è ragionevole attendersi da loro ed è previsto dal diritto nazionale, al fine di individuare e prevenire taluni tipi di attività illecite». In tal senso si v. G.G. Codiglione, *La nuova legge tedesca, op.cit.*, p. 735, nt. 20.

[138] Per le considerazioni che seguono si v. M. Mazzonetto, *Il problema dei contenuti illegali on-line, loc.op.ult.cit.*

[139] Secondo l'autorevole insegnamento di G. Tesauro, *Diritto Comunitario, op.cit.,* p. 145.

"virtuose", delineate dalla Commissione; sia influendo, sul piano istituzionale, sugli indirizzi delle autorità giudiziarie e sull'evoluzione degli interventi normativi futuri degli Stati membri.

Sotto il primo punto di vista, la responsabilizzazione sociale degli *hosting providers* potrebbe costituire un punto di partenza e di indirizzo di costoro all'impiego di una maggiore diligenza nella gestione delle reti e dei sistemi delle piattaforme digitali. La Commissione spinge tali soggetti all'adozione di protocolli d'intesa, codici di condotta ed accordi privati; anche se deve precisarsi che, senza dubbio, sarebbe più efficace il loro impiego non solo a livello nazionale o europeo, considerando che i maggiori *global players* sono i fornitori di servizi statunitensi[140]. Tali strumenti di autoregolamentazione avrebbero il merito non solo di inviduare, prevenire e quindi contrastare i contenuti illeciti, ma anche di arginare il pericolo della perdita di competitività dei fornitori di ospitalità "più attenti" nel contrasto degli illeciti[141]. Si comprende bene come l'adozione di misure proattive isolatamente, da parte di taluni *providers*, avrebbe difatti l'effetto di indurre gli utenti a stipulare i contratti con le piattaforme digitali "meno attente" al contrasto degli illeciti che non le impieghino, al fine di sentirsi meno controllati sui contenuti da pubblicare e per non correre il rischio della rimozione degli stessi dal sito.

In riferimento al formante legislativo, si precisi che, in realtà, il considerando 41 della Raccomandazione prevede che la Commissione europea monitorerà (oltre alle misure impiegate dagli *hosting providers*) i provvedimenti concretamente assunti dai singoli Stati membri, in risposta alle indicazioni contenute nella medesima.

Si confida sull'effetto "persuasivo" della Raccomandazione che avrà il "potere (europeo) di indirizzo politico" dei legislatori nazionali[142]. I principi

[140] Si v. R. Natoli, *La tutela dell'onore e della reputazione in* internet*, op.cit.,* p. 466.
[141] Si v. R. Natoli, *La tutela dell'onore e della reputazione in* internet*, op.cit.,* p. 466.
[142] Pone l'accento sul valore "persuasivo" degli atti di *soft law* R. Mandrellotti, *Sistema delle fonti e indirizzo politico nelle dinamiche dell'integrazione europea,* Torino, 2004, p. 192. L'autore sostiene che la *soft law*, più che fonte del diritto, sarebbe direttamente collegata con il «potere comunitario di indirizzo politico»; ragion per cui gli «atti atipici» costituirebbero «strumenti di diritto mite», corredati di un'efficacia giuridica molto minore, rispetto alle fonti tipiche, e sarebbero volti a perseguire obiettivi politici, attraverso la loro persuasione.

comuni, contenuti nel provvedimento, seppur non vincolanti, costituiranno, senz'altro, linee guida per i legislatori degli Stati membri, nella previsione di «misure effettive, appropriate e proporzionate», per fronteggiare i contenuti illeciti *on line*, nell'ottica della maggiore responsabilizzazione degli *hosting providers*.

D'altra parte è già accaduto, in altri ambiti, che un provvedimento di *soft law*, quale la Raccomandazione, rendendo nota la posizione delle Istituzioni Europee sull'evoluzione futura della propria azione, senza imporre obblighi giuridici agli Stati membri, li abbia poi influenzati, conducendoli ad emanare provvedimenti legislativi in conformità alle linee di azione ivi suggerite[143].

In considerazione di quanto detto, ci si domanda sull'opportunità di includere, tra le misure proattive degli *hosting providers* da incoraggiare, a livello europeo e nazionale, anche l'identificazione dei destinatari dei servizi, prima di consentire loro l'accesso ai portali gestiti, seguendo la tecnica del c.d. «anonimato protetto».

L'identificazione dei fruitori del servizio da parte di fornitori di ospitalità costituirebbe un valido strumento per contrastare gli illeciti *on line*, sortendo, come le altre misure proattive, l'effetto della maggiore responsabilizzazione

[143] Si fa precipuo riferimento alla Raccomandazione della Commissione europea dell'11 giugno 2013 (2013/396/UE) «relativa a princípi comuni per i meccanismi di ricorso collettivo di natura inibitoria e risarcitoria negli Stati membri che riguardano violazioni di diritti conferiti dalle norme dell'Unione», alla quale ha fatto seguito, in linea con l'orientamento politico della Commissione europea di non delimitare lo strumento processuale di tutela collettiva risarcitoria alla sola protezione del consumatore o utente ovvero ad ambiti prettamente settoriali, l'emanazione di provvedimenti innovativi di taluni Stati membri che hanno ampliato l'ambito oggettivo e soggettivo di applicazione della disciplina originaria in materia. Su questa linea, si segnala la legge italiana del 12 aprile 2019, n. 31, recante «Disposizioni in materia di azione di classe» che entrerà in vigore un anno dopo la pubblicazione sulla Gazzetta Ufficiale; la legge francese la *loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle* che detta disposizioni generali sull'*action de groupe devant le juge judiciaire*, pur enunciando che son fatte salve le disposizioni speciali, previste in numerosi ambiti, dalla disciplina: sulla lotta contro la discriminazione; dal *code du travail* (nel settore del lavoro); dal *code de l'environnement* (in ambito ambientale); dal *code de la santé publique* (codice della salute) e dalla disciplina relativa alla protezione dei dati personali**.** Sui principi espressi dalla Raccomandazione, mi si consenta di rinviare a G. D'Alfonso, *Illeciti di massa e controversie transfrontaliere. Strumenti di tutela collettiva risarcitoria e competizione tra sistemi giurisdizionali,* in *Rass.dir.civ.*, 2013, p. 150 ss.

degli *hosting providers*. Si rilevi anche, aspetto di non poco momento, che l'impiego di tale misura metterebbe al riparo i fornitori di ospitalità, che diligentemente identifichino gli utenti del servizio, dal rischio di imputazione della responsabilità civile esclusiva per i contenuti illeciti di autori non identificabili –rischio che potrebbe divenire sempre più pregnante, qualora il *trend* giurisprudenziale *supra* richiamato si consolidi negli Stati membri dell'Unione europea, oltre che presso le Corti europee.

Non si sottovaluti inoltre che tale misura avrebbe altresì un effetto "deterrente" nei confronti degli utenti che, nella consapevolezza di poter essere identificati innanzi all'autorità giudiziaria, seppur abbiano interagito in rete anonimamente, sarebbero dissuasi dalla pubblicazione di contenuti illeciti.

La misura proattiva, così definita, non influirebbe infine sul regime speciale di responsabilità civile degli *hosting providers*, dal momento che non scalfirebbe in alcun modo il principio secondo il quale i *providers* non debbano esercitare un obbligo di monitoraggio dei contenuti pubblicati, nè debbano attivarsi nella ricerca degli stessi, poichè si collocherebbe temporalmente, prima ancora del momento in cui gli utenti del servizio accedano al portale, e non inciderebbe in alcun modo sul controllo dei contenuti ivi pubblicati.

In realtà, tale misura è già impiegata da alcuni portali (quali *Airbnb*).

Si hanno tuttavia dubbi che l'identificazione degli utenti possa costituire oggetto di accordi volontari, protocolli d'intesa o codici di condotta ad ampio raggio che siano stipulati da un numero elevato di *hosting providers*, in ragione della circostanza che una misura del genere potrebbe implicare la perdita di competitività sul mercato digitale.

Si pensi a quanto accaduto a *Facebook*[144]. Si premetta che, ai fini dell'iscrizione al *social network,* è sufficiente che l'utente stipuli un contratto, indicando il proprio nome e cognome e l'indirizzo *e mail*. *Facebook*, dopo aver scoperto che taluni utenti utilizzavano il nome d'arte, *Drag Queen,* aveva disabilitato diversi *account*. A seguito di tale *policy*, numerosi utenti, per reazione, hanno abbandonato *Facebook*, per iscriversi ad *Ello*, un *social*

[144] Sulla vicenda di Facebook, si v. S. Arcuti, *Diritto all'anonimato: libertà di espressione e/o tutela della riservatezza, o.c.*

network che consente l'utilizzo anonimo del portale ovvero con pseudonimo. Per tale ragione il *social network* ha comunicato, nel 2014, il mutamento della sua "*real name policy*", al fine di evitare di perdere utenti. La nuova *policy* non solo non impone loro l'utilizzo del nome vero, ma soprattutto non prevede né la richiesta di una copia del documento d'identità del sottoscrittore del contratto, nè alcun controllo di veridicità delle informazioni rese.

Si osservi anche che, seppur si volesse immaginare che i legislatori degli Stati membri incoraggino gli *hosting providers* all'adozione della misura proattiva dell'identificazione degli utenti dei portali, certamente l'imposizione *ex lege* di misure di autenticazione degli stessi, sul modello della legislazione francese, sarebbe più efficace, al fine di garantire la tutela giurisdizionale effettiva dei soggetti lesi dai contenuti illeciti *on line*. Cionodimeno, ad oggi, pochi sono gli Stati membri che si muovono in tale direzione, poichè, a livello politico, si ergono spinte contrarie, motivate dall'esigenza di impedire gli effetti del raffreddamento della rete: ne è un esempio il disegno di legge italiano, ormai arenato in Parlamento da più di due anni.

Per tali ragioni, nell'ottica *de jure condendo,* deve giungersi alla conclusione che la vera spinta verso la maggiore responsabilizzazione degli *hosting providers*, in particolar modo in merito all'identificazione dei destinatari dei servizi, dovrebbe preferibilmente avvenire dal formante legislativo europeo, sebbene i segnali propulsivi in questa direzione si rinvengono finora unicamente in atti di *soft law*.

Si auspica un intervento armonizzante di *hard law* in tal senso, poichè le istanze di evoluzione del mercato digitale sempre più globale necessitano di regole comuni e condivise. Solo la previsione armonizzante, a livello europeo, di misure che determinino una maggiore responsabilizzazione degli *hosting providers* può essere idonea ad incrementare la fiducia degli utenti nel mercato digitale, renendo efficente la strategia di impulso dello stesso.

Diritto Mercato Tecnologia

Numeri Speciali

2016 Lo Statuto Etico Giuridico dei Campioni Biologici Umani
a cura di Dario Farace

2017 Il Mercato Unico Digitale
a cura di Gianluca Contaldi

2018 La Ricerca su Materiali Biologici di Origine Umana:
Giuristi e Scienziati a confronto
a cura di Alberto M. Gambino, Carlo Petrini e Giorgio Resta

2019 La Tassazione dell'Economia Digitale tra Sviluppi Recenti
e Prospettive Future
a cura di Alessio Persiani

La rivista "Diritto Mercato Tecnologia" intende fornire un costante supporto di aggiornamento agli studiosi e agli operatori professionali nel nuovo scenario socio-economico originato dall'interrelazione tra diritto, mercato e tecnologia, in prospettiva interdisciplinare e comparatistica. A tal fine approfondisce, attraverso studi nei settori privatistici e comparatistici, tematiche afferenti in particolare alla proprietà intellettuale, al diritto antitrust e della concorrenza, alle pratiche commerciali e alla tutela dei consumatori, al biodiritto e alle biotecnologie, al diritto delle comunicazioni elettroniche, ai diritti della persona e alle responsabilità in rete.

ISSN (Online Edition): 2239 -7442