GIORGIO RESTA

ANONIMATO, RESPONSABILITÀ, IDENTIFICAZIONE: PROSPETTIVE DI DIRITTO COMPARATO

1. Introduzione.

Qualsiasi discorso sul rapporto tra anonimato e diritto necessita in limine di una chiara demarcazione dei temi coinvolti e dei problemi affrontati. Troppe, infatti, sono le questioni giuridiche sollevate dal fenomeno dell'anonimato per condurre una riflessione a carattere sistematico, che riesca a sottrarsi al vizio del formalismo o della superficialità [1]. Dall'anonimato nel campo della filiazione [2] all'anonimato nel diritto tributario [3]; dall'anoni-

* Il presente scritto riproduce, con l'aggiunta di note e con aggiornamenti, la relazione presentata al convegno '*Anonimato, diritti della persona e responsabilità in rete*' organizzato dal Dipartimento di diritto pubblico dell'Università di Milano, dal Dipartimento di scienze giuridiche dell'Università di Milano-Bicocca e dalla Fondazione Calamandrei l'11 novembre 2013. Il lavoro, prima della pubblicazione, è stato sottoposto all'esame della Direzione della Rivista.

[1] Per un analogo ordine di considerazioni v. V. Zeno-Zencovich, *Anonymous Speech on the Internet*, in A. Koltay, a cura di, *The Fundamentals of European Thought on Media Law*, Budapest, 2014 (in corso di pubblicazione). Per una prima introduzione al tema del rapporto tra anonimato e diritto cfr. G. Finocchiaro, voce *Anonimato*, in *Dig. Disc. Priv., Aggiornamento V*, Torino, 2010, 12 ss.; Id., a cura di, *Diritto all'anonimato. Anonimato, nome e identità personale*, in *Trattato di diritto commerciale e di diritto pubblico dell'economia* diretto da F. Galgano, XLVIII, Padova, 2008; v. altresì I. Kerr - V. Steeves - C. Lucock, a cura di, *Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society*, Oxford, 2009.

[2] B. Zypries - M. Zeeb, *Samenspende und das Recht auf Kenntnis der eigenen Abstammung*, in *ZRP*, 2014, 54; E. Wenner, *Allemagne: Le droit aux origines face à l'émergence de l'anonymat (à propos des « casiers à bébé »)*, in J. Pousson-Petit, a

mato nel processo civile [4] all'anonimato nel settore della ricerca biomedica e nel campo dei trapianti di organi e tessuti [5]; dalle opere anonime contemplate dalla legge sul diritto d'autore [6] all'anonimato nella legislazione sulle tossicodipendenze [7]: sarebbe vano andare alla ricerca di regole comuni, possibilmente elevabili a principi, in quanto la tipologia degli interessi sottesi a ciascuna di tali fattispecie è, evidentemente, oltremodo varia ed eterogenea. Ciò è vero ove ci si concentri su un singolo ordinamento [8]; lo è ancor più qualora si adotti un approccio comparatistico. Conviene, dunque, precisare che in questo scritto ci si soffermerà unicamente sull'anonimato nel contesto dei rapporti "on line" [9] e si farà prevalente, anche se non esclusivo, riferimento all'insieme dei problemi attinenti all'esercizio della libertà d'espressione in forma anonima e agli illeciti ad esso correlati. Per contro, non ci si occuperà delle pur importanti questioni concernenti il settore degli scambi negoziali e, dunque, dell'anonimato nella contrattazione *online* [10]; né, se non marginalmente, del tema — la cui rilevanza pratica è davvero cruciale, dato che nessuna attività in rete può essere considerata completamente 'anonima' [11] — relativo al rapporto tra anonimato, *privacy* dell'utente e tecniche di sorveglianza elettronica [12]. Inoltre, ci si concentrerà esclusivamente sui problemi sottesi alla tutela civile dei diritti, mentre non si affronterà il problema della tutela penale. Adottando un me-

cura di, *L'identité de la personne humaine. Étude de droit français et de droit comparé*, Bruxelles, 2002, 797 ss.

[3] F. Pistolesi, *L'oggetto ed i limiti dell'anonimato in tema di cosiddetto "scudo fiscale"*, in *Riv. dir. fin.* 2002, 611 ss.

[4] G. Resta, *Privacy e processo civile: il problema della litigation "anonima"*, in questa *Rivista*, 2005, 681 ss.

[5] Con particolare riferimento alla legge francese sul dono e l'utilizzazione di parti del corpo V. Depadt-Sebag, *Le don de gamètes ou d'embryon dans les procréations médicalement assistées: d'un anonymat imposé à une transparence autorisée*, in *D.*, 2004, 891; per riferimento al diritto italiano sia consentito il rinvio a G. Resta, voce *Doni non patrimoniali*, in *Enc. Dir., Annali*, IV, Milano, 2011, 510 ss., 525.

[6] V. ad es. A. Giannini, *Opere pseudonime e anonime e diritto di rivelazione*, in *Riv. dir. comm.*, 1957, I, 42 ss.

[7] E. Morelato, *L'anonimato nella legislazione speciale sulle tossicodipendenze e sulla protezione degli studenti in stato di disagio*, in G. Finocchiaro, a cura di, *Diritto all'anonimato. Anonimato, nome e identità personale*, cit., 137 ss.

[8] Particolarmente meritorio, rispetto all'ordinamento italiano, è lo studio coordinato da G. Finocchiaro, a cura di, *Diritto all'anonimato. Anonimato, nome e identità personale*, cit., spec. 133 ss.

[9] Per un'introduzione organica ed esaustiva al tema dell'identità digitale v. D. Pousson, *L'identité informatisée*, in J. Pousson-Petit, a cura di, *L'identité de la personne humaine. Étude de droit français et de droit comparé*, cit., 371 ss.

[10] V. ad es. J. Grijpink - C. Prins, *Digital Anonymity on the Internet. New Rules for Anonymous Electronic Transactions? An Exploration of the Private Law Implications of Digital Anonymity*, in 17 *Computer Law & Security Report* 379 (2001).

[11] V. ad es. P. Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 *UCLA L. Rev.* 1701 (2010).

[12] G. Spindler, *Persönlichkeitsschutz im Internet - Anforderungen und Grenzen einer Regulierung*, in *Verhandlungen des 69. Deutschen Juristentages*, Band I, München, 2012, Gntachten F, 1 ss., 92; D.C. Howe - H. Nissenbaum, *Trackmenot: Resisting Surveillance in Web Search*, in I. Kerr - V. Steeves - C. Lucock, a cura di, *Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society*, cit., 417 ss.

todo di indagine di stampo funzionalistico, si cercherà di tratteggiare un panorama di diritto comparato articolato intorno alle seguenti questioni:

a) È lecito il ricorso all'anonimato o a pseudonimi nel contesto delle attività *online* e, in caso affermativo, quali sono i fondamenti e i limiti di una siffatta soluzione?

b) Chi risponde per gli illeciti connessi in forma anonima?

c) Quali sono gli strumenti utilizzabili dalla vittima di un illecito al fine di ottenere l'ostensione dei dati identificativi dell'autore del contenuto anonimo?

2. L'anonimato *online*: le regole e i modelli.

Il primo interrogativo, tra quelli appena formulati, potrebbe essere inteso come una domanda retorica. Non è così. È sufficiente volgere un rapido sguardo al di fuori dei confini nazionali per constatare come l'attitudine dei vari ordinamenti nei confronti della questione della liceità dell'anonimato *online* non sia uniforme, né consolidata in un senso o nell'altro. Del resto, anche all'interno dei singoli sistemi le soluzioni variano sensibilmente a seconda sia delle aree coinvolte, sia dei meccanismi di disciplina considerati, essendo a tal riguardo cruciale la distinzione tra regole formali, norme sociali e prassi contrattuali. Ciò non toglie che, ad una considerazione di sintesi, può ritenersi prevalente su scala comparatistica un primo modello, il quale è imperniato sul riconoscimento di principio della liceità dell'anonimato "on line".

2.1. *Anonimato come strumento di esercizio della libertà d'espressione.*

Questo modello è ritenuto da molti coessenziale ai tratti distintivi dello spazio cibernetico, come sin qui conosciuto [13]. È conforme alla natura della rete e ai suoi caratteri di intrinseca democraticità, si osserva da più parti, incentivare uno scambio quanto più autonomo, libero e decentrato di idee e informazioni e permettere la costruzione di rapporti sociali su base volontaria e persino artificialmente definita. L'anonimato — ivi compreso il ricorso a *network* anonimi come TOR [14] — rappresenterebbe uno dei più importanti strumenti di salvaguardia di tali caratteristiche. Esso, da un lato, consentirebbe la libera manifestazione del pensiero e la libera esplicazione della personalità di ciascun

[13] In questa prospettiva si confrontino le puntuali argomentazioni di S. Rodotà, *Il diritto di avere diritti*, Roma-Bari, 2012, 389 ss.; e da ultimo M. Manetti, *Libertà di pensiero e anonimato in rete*, in questa *Rivista*, n. 2/2014.

[14] K.D. Watson, *The Tor Network: A Global Inquiry Into the Legal Status of Anonymity Networks*, in 11 *Wash. U. Global Stud. L. Rev.* 715 (2012).

individuo (nel senso dell'art. 2 Cost.), ponendolo al riparo dai rischi di intimidazione e stigmatizzazione propri del mondo reale [15]. Dall'altro, esso realizzerebbe il sogno dell'identità postmoderna, consentendo a ciascuno di sfuggire alle gabbie della propria 'biografia', costruendo un'identità fluida, *à la carte*, plasmata su un io desiderato e libero da tutti i vincoli e le convenzioni sociali circa il modo di apparire [16]. In ciò la rete darebbe vita ad un vero e proprio "gioco delle identità", dove i rapporti sociali sarebbero organizzati esattamente attraverso il ricorso a quelle *maschere* che informano sin dalla sua origine, anche etimologicamente, il paradigma occidentale di "persona" [17]. Mascheramento e smascheramento sarebbero resi possibili proprio dal ricorso all'anonimato, o ancor più dalla tecnica dello pseudonimo, il quale permette di attribuire stabilità e ricchezza semantica all'identità digitale eletta dal singolo internauta [18]. Non si tratta, peraltro, di un'esigenza limitata alla posizione dei singoli individui. L'anonimato sembrerebbe offrire benefici non irrilevanti anche dal punto di vista dell'autonomia dei gruppi. Difatti, consentendo alle minoranze (di genere, di ceto, di etnia, di orientamento sessuale) di esprimere critiche, rivendicare pretese e organizzare forme di mobilitazione a un grado di intensità altrimenti impossibile, specie ma non soltanto nei sistemi a scarso tasso di democraticità, tale strumento avrebbe un effetto ampiamente positivo sul piano della partecipazione alla vita politica e, dunque, della redistribuzione del potere sociale [19].

A livello normativo, tale approccio sembra caratterizzare la più parte degli ordinamenti occidentali, ma soprattutto l'esperienza statunitense. Forse sarebbe eccessivo definire l'anonimato un fenomeno "as American as apple-pie" — tanto che una delle più recise affermazioni circa l'immanenza dell'anonimato alla natura

---

[15] S. Rodotà, *Il diritto di avere diritti*, cit., 392; L. Barnett Lidsky - T. F. Cotter, *Authorship, Audiences, and Anonymous Speech*, 82 *Notre Dame L. Rev.* 1537, 1574 (2007); per una valutazione equilibrata del problema v. F. Schauer, *Anonymity and Authority*, in 27 *Journal L. & Politics* 597 (2012).

[16] Per un'attenta discussione di tale profilo v. S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 2004, 139 ss. V. altresì G.W. Penney, *Privacy and the New Virtualism*, in 10 *Yale J. L. & Tech.* 194 (2008); S. Cavagnetto - B. Gahir, *A Formalized Model of Multiple Selves in Mud's*, in 5 *Masaryk U.J. L. & Techn.* 199 (2011); nell'ambito della letteratura sociologica e di psicologia sociale il riferimento d'obbligo è a S. Turkle, *Life on the Screen. Identity in the Age of the Internet*, New York, 1995.

[17] In generale v. Y. Thomas, *Le sujet de droit, la personne et la nature. Sur la critique contemporaine du sujet de droit*, in *Le Débat*, 1998, 85 ss., spec. 97 ss.; Id., *L'essere concreto e la sua persona*, in O. Cayla - Y. Thomas, *Il diritto di non nascere. A proposito del caso Perrouche*, trad. it., Milano, 2004, 110 ss.

[18] D. Pousson, *L'identité informatisée*, cit., 386-390; V. Smith Ekstrand, *The Many Masks of Anon: Anonymity as Cultural Practice and Reflections in Case Law*, in 18 *J.Tech.L.& Pol'y* 1 (2013).

[19] Su tale aspetto può leggersi, in questa *Rivista*, n. 2/2014, il bel saggio di M. Cuniberti, *Democrazie, dissenso politico e tutela dell'anonimato*.

della rete proviene dal *Bundesgerichtshof* tedesco [20] —, ma uno sguardo al dibattito contemporaneo evidenzia immediatamente lo straordinario ruolo e rilievo ad esso attribuito in quel contesto culturale. Benché non manchino argomentazioni di segno opposto, l'assunto per cui l'anonimato rappresenti, oltre che un valore, un vero e proprio diritto fondamentale tutelato in capo agli utenti della rete sembra raccogliere un consenso diffuso [21]. Di riflesso, il tema vero all'interno del dibattito nordamericano non è se il ricorso all'anonimato sia lecito o illecito, essendo la risposta a tale quesito sostanzialmente scontata, quanto piuttosto se sia lecito per le autorità pubbliche limitare, restringere o addirittura precludere il ricorso alle tecniche di anonimizzazione. Due parrebbero le principali premesse socio-culturali, sulle quali riposa un siffatto approccio al tema dell'anonimato. La prima premessa è costituita dalla tradizionale sfiducia nei confronti del potere pubblico e, in particolare, nei confronti di quella microtecnica della sorveglianza che è rappresentata dal documento di identificazione imposto per legge [22]. Com'è noto, nella società americana non si è mai fatto ricorso allo strumento della carta d'identità, avvertita per ragioni politiche, culturali e religiose come un dispositivo oppressivo, intimamente inconciliabile con l'assunto "romantico" della libertà di movimento [23]. È vero che la patente di guida, o il *social security number* hanno egregiamente svolto il ruolo di sostituti funzionali di tale documento e che oggi il diritto dei trasporti — ma la tendenza è di carattere più generale — impone in misura crescente l'uso di documenti ufficiali di identi-

[20] BGH, 23 giugno 2009, *Spickmich.de*, in *NJW*, 2009, 2888 ss., 2892, ove si legge (par. 38): "Die anonyme Nutzung ist dem Internet immanent"; tale formula è ribadita letteralmente da LG Kiel, 6 dicembre 2013, in *BeckRS*, 2014, 03139.

[21] Per una puntuale analisi comparatistica v. V. Zeno-Zencovich, *Anonymous Speech on the Internet*, cit.

[22] In tema v. ora D. Lyon, *Identifying Citizens. ID Cards as Surveillance*, Cambridge, 2009; sulla storia dei strumenti di identificazione dell'individuo e in particolare sul documento di identità v. G. Neyrand, *Identification sociale, personnalisation et processus identitaires*, in J. Pousson-Petit, a cura di, *L'identité de la personne humaine. Étude de droit français et de droit comparé*, Bruxelles, 2002, 93 ss., 98. Per l'esperienza italiana cfr. L. Trucco, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, Torino, 2004, 97 ss.

[23] In proposito cfr. A.M. Froomkin, *The Uneasy Case for National ID Cards*, in P. Chander - L. Gelman - M.J. Radin, *Securing Privacy in the Internet Age*, Stanford, 2008, 295 ss.; Id., *Identity Cards and Identity Romanticism*, in I. Kerr - V. Steeves - C. Lucock, a cura di, *Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society*, cit., 248 (il quale osserva che "today, the Anglo-Saxon ideal that in a free country a person should be able to move freely without having to justify himself to authorities — that police have no right to stop you without probable cause and that even when they do one has no obligation to speak to them — is more deeply ingrained in the national psyche than reflected in the Constitution. Many states have stop-and-identify laws that require citizens to identify themselves to police officers. Often, however, these statutes require that an officer have a reasonable suspicion of criminality before making an identity demand"). Sulle premesse comuni ai modelli di *common law* cfr. J. Pousson-Petit, *L'identité de la personne humaine au Royaume-Uni*, in J. Pousson-Petit, a cura di, *L'identité de la personne humaine. Étude de droit français et de droit comparé*, cit., 343 ss., 346.

ficazione [24]. Tuttavia il rifiuto della "carta d'identità" mantiene, almeno sul piano simbolico, un significato non trascurabile. D'altronde, l'assenza della carta d'identità costituisce soltanto un tassello di un approccio più generale al tema dell'identificazione dei soggetti, che si connota proprio per la sua attitudine particolarmente liberale. Non esiste una predeterminazione legale dei nomi attribuibili ai figli [25]; non esistono limiti rigidi alla possibilità di scelta e mutamento del nome [26], non avendo in proposito l'autorità amministrativa alcun potere di sindacato ed essendo rimessi gli eventuali conflitti all'autorità giudiziaria; lo stesso obbligo per il cittadino di identificarsi a seguito di apposita richiesta delle forze di polizia, stabilito dai c.d. *stop and identify statutes*, è in taluni stati subordinato alla presenza di specifici elementi che facciano sospettare la commissione di un illecito amministrativo o penale [27]. L'utopia del cittadino libero di spostarsi e trasferirsi, iscritta nella storia della società americana tanto quanto l'idea della mobilità verticale, benché sempre più erosa dall'avvento delle tecnologie della sorveglianza e dalle politiche di contrasto al terrorismo, continua a orientare il dibattito sui moderni strumenti di identificazione, dai tradizionali tesserini cartacei sino alla biometria [28]. Del pari, essa sembra insinuarsi, sia pure in maniera sottile e non dichiarata, nella discussione sull'anonimato in rete, contribuendo a rafforzare la tesi del diritto di ciascun individuo di spogliarsi liberamente della propria identità reale, assumendo tante identità virtuali quanti sono i contesti comunicativi di riferimento. La seconda premessa è costituita dal rilievo assunto dalla libertà d'espressione nell'assiologia costituzionale nordamericana [29]. Questo è il profilo che più distintamente emerge ad un'osservazione del dibattito. L'anonimato è visto come uno strumento effettivo, spesso indispensabile, di esplicazione del pensiero, e ciò tanto più nello spazio cibernetico, ove sembra realizzarsi l'utopia del perfetto *marketplace of*

[24] A.M. Froomkin, *Identity Cards and Identity Romanticism*, cit., 249; nel campo dei rapporti *online* cfr. C. Sullivan, *Digital identity, privacy and the right to identity in the United States of America*, 29 *Computer L. & Sec. Rev.* 348 (2013).

[25] J.Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, in 113 *Yale L. J.* 1151, 1158, 1216-1219 (2004).

[26] Anche qui è cruciale la derivazione dal modello britannico, cfr. J. Pousson-Petit, *L'identité de la personne humaine au Royaume-Uni*, cit., 349-351; G. Loiseau, *Le nom objet d'un contrat*, Paris, 1997, 53 ss., 61 ss., 108 ss.

[27] Cfr. *Hübel v Sixth Judicial Dist. Court of Nevada, Humboldt County*, 542 U.S. 177 (2004). Per una discussione del significato di tale pronunzia v. A.M. Froomkin, *Identity Cards and Identity Romanticism*, cit., 250.

[28] A.M. Froomkin, *Identity Cards and Identity Romanticism*, cit., 246 ss.; Id., *The Uneasy Case for National ID Cards*, cit.

[29] Cfr. tra i molti P. D. Carrington, *Our Imperial First Amendment*, 34 *U. Rich. L. Rev.* 1167 (2001); R. A. Sedler, *An Essay on Freedom of Speech: The United States Versus the Rest of the World*, 2006 *Mich. St. L. Rev.* 377 (2006); F. Schauer, *The Exceptional First Amendment*, KSG Working Paper No. RWP05-021 17 (February 2005), accessibile all'indirizzo: http://ssrn.com/abstract=668543.

ideas. Pertanto la sua compressione è percepita come un *vulnus* per la garanzia scolpita nel Primo Emendamento della Costituzione. Non a caso, fra i riferimenti che più frequentemente si incontrano negli studi dedicati al rapporto tra anonimato e libertà d'espressione, spicca quello relativo all'uso dello pseudonimo "Publius", impiegato da James Madison, Alexander Hamilton e John Jay per firmare gli articoli poi confluiti nei *Federalist Papers* [30], quasi a voler evocare l'esistenza di un filo rosso tra la manifestazione del pensiero in forma anonima e l'identità americana. Ma la persuasività dell'assunto trae ulteriore forza dalla disamina della giurisprudenza della Corte Suprema in materia di *free speech*, la quale offre molteplici riscontri all'idea che la facoltà di manifestare il proprio pensiero in forma anonima ricada sotto l'orbita della garanzia costituzionale [31]. Da *Talley v. California* (1960) [32] e *McIntyre v. Ohio Elections Commission* (1995) [33], due casi in materia di legittimità delle restrizioni all'anonimato nel campo del *political speech*, sino a *Watchtower Bible v. Village of Stratton* (2002) [34], la Corte ha giudicato costituzionalmente illegittimi provvedimenti statali volti ad imporre requisiti di identificabilità rispetto ad attività quali il proselitismo religioso, la divulgazione di volantini a contenuto politico, etc.

I due fattori appena ricordati contribuiscono a spiegare la notevole fortuna arrisa all'ideologia dell'anonimato "on line" anche al di fuori del suo terreno d'elezione, ossia il mondo degli *hackers* e l'articolata galassia dei movimenti [35]. In particolare, la logica del *free speech* si è rivelata tanto forte da orientare le posizioni delle corti in ordine al problema della legittimità costituzionale delle restrizioni all'uso dell'anonimato "on line" [36].

---

[30] F. SCHAUER, *Anonymity and Authority*, cit., 597; S. ●ASIR, *Anonymity in Cyberspace: Judicial and Legislative Regulations*, in 81 *Fordham L. Rev.* 3651 (2013).

[31] M. FROOMKIN, *Anonymity and the Law in the United States*, in I. KERR - V. STEEVES - C. LUCOCK, a cura di, *Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society*, cit., 441; S. ●ASIR, *Anonymity in Cyberspace: Judicial and Legislative Regulations*, cit., 3663 ss.; M.E. KAMINSKY, *Real Masks and Real Name Policies*, in *Fordham Int. Prop. Media Ent. L. J.* 815, 833 (2013).

[32] *Talley v. California*, 362 U.S. 60 (1960).

[33] *McIntyre v. ●hio Elections Commission*, 514 U.S. 334 (1995), ove si afferma chiaramente, alla p. 342, che "an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment".

[34] *Watchtower Bible & Tract Soc'y of New York, Inc. v. Vill. of Stratton*, 536 U.S. 150 (2002). La decisione concerne un caso di proselitismo *door to door* dei Testimoni di Geova.

[35] Cfr. ad es. ●. NORTON, *2011: The Year Anonymous Took on Cops, Dictators and Existential Dread*, in WIRED, *http://www.wired.com/threatlevel/2012/01 /anonymous-dicators-existential-dread/all/*. Sull'anonimato quale strumento di garanzia del dissenso e della critica politica v. M. CUNIBERTI, *Democrazie, dissenso politico e tutela dell'anonimato*, in questa *Rivista*, n. 2/2014.

[36] In particolare, sulle implicazioni della giurisprudenza della Corte Suprema nel campo dei rapporti telematici v. J. MCNEALY, *A Textual Analysis of the Influence of* McIntyre v. Ohio Elections Commission

Basti ricordare, al riguardo, che in *White v. Baker* [37], una corte distrettuale federale ha ritenuto lesiva del Primo Emendamento della Costituzione federale una normativa della Georgia che stabiliva l'obbligo, per le persone condannate per reati di violenza sui minori e pedofilia, di comunicare preventivamente agli organi di polizia i propri *alias*, pseudonimi, *password* e altri elementi identificativi della propria identità virtuale. Del pari, già nel 1997, nel caso *ACLU of Georgia v. Miller* [38], era stata dichiarata costituzionalmente illegittima una legge della Georgia che proibiva l'uso di nomi falsi in Internet [39]. Inoltre il riferimento al Primo Emendamento svolge un ruolo cruciale, come si vedrà meglio in seguito, in ordine alle decisioni in materia di *disclosure* dell'identità degli autori di contenuti illeciti immessi in rete [40].

2.2. *Anonimato come proiezione del diritto alla protezione dei dati personali.*

Tuttavia, sarebbe erroneo ritenere che un'architettura istituzionale incentrata sulla logica dell'anonimato debba poggiare necessariamente sull'architrave della libertà d'espressione. Questo è certamente uno dei più rilevanti, ma non l'unico interesse perseguito dall'ordinamento attraverso un siffatto meccanismo regolatorio. Un rapido confronto con l'approccio europeo sembra confermarlo. Qui il principio dell'anonimato è penetrato nel tessuto normativo non già (o meglio non unicamente) attraverso il medio logico della libertà d'espressione, bensì per il tramite del diritto alla *privacy*, o più precisamente del diritto alla protezione dei dati personali [41]. Com'è noto, la direttiva 95/46/CE e le normative nazionali contemplano l'anonimato o come criterio idoneo a circoscrivere l'ambito oggettivo d'applicazione della disciplina (*Considerando* (26) [42], o come principio generale al

in Cases Involving Online Anonymous Commenters, 11 *First Am. L. Rev.* 150 (2012); A.W. Branscomb, *Anonimity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspace*, in 104 *Yale L.J.* 1639 (1995).

[37] *White v. Baker*, 696 F. Supp. 2d 1289 (N.D. Ga. 2010).

[38] *ACLU of Ga. v. Miller*, 977 F. Supp. 1228 (N.D. Ga. 1997).

[39] Per un panorama sulle principali normative statali v. S. Qasir, *Anonymity in Cyberspace: Judicial and Legislative Regulations*, cit., 3653, nota 12.

[40] Cfr. *infra*, par. 4.1.

[41] Il duplice fondamento del principio dell'anonimato è nitidamente espresso nella Dichiarazione del Comitato dei Ministri del Consiglio d'Europa del 28 maggio 2003, *Freedom of Communication on the Internet*, il cui art. 7, dedicato all'anonimato, statuisce che: "[i]n order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member States should respect the will of users of the Internet not to disclose their identity". Per una chiara distinzione tra le due basi teoriche dell'anonimato, le quali non sono mutualmente esclusive, ma convergenti, si veda G. Spindler, *Persönlichkeitsschutz im Internet - Anforderungen und Grenzen einer Regulierung*, cit., 33.

[42] "Considerando che i principi della tutela si devono applicare ad ogni informazione concernente una persona identificata o identificabile; che, per determinare se una persona è identificabile, è opportuno pren-

quale deve conformarsi l'attività di trattamento dei dati personali [43]. Davvero emblematico, da questo punto di vista, è l'art. 3 del Codice italiano in materia di protezione dei dati personali, che assegna un valore ordinante al c.d. principio di necessità [44]. Il trattamento di dati anonimi è quindi elevato a modello organizzativo ordinario, dal quale sarebbe possibile discostarsi soltanto quando le particolari finalità del trattamento, nelle singole ipotesi, lo giustifichino [45]. Poiché la fruizione dei servizi telematici implica di regola una cospicua profusione di informazioni personali dal lato dell'utente e una sistematica attività di raccolta e utilizzazione dal lato del fornitore del servizio, in linea di principio il ricorso alle tecniche di anonimizzazione dovrebbe reputarsi non soltanto lecito, ma persino incoraggiato sul piano normativo, in quanto strumentale rispetto all'esigenza di salvaguardare il singolo dalle forme più invasive di sorveglianza elettronica [46]. Ovviamente è necessario distinguere tra i rapporti intercorrenti con l'*access provider* e l'"on line" *service provider* [47]. Nel primo caso vi sono disposizioni che prescrivono persino l'identificazione nominativa del cliente [48], o quanto meno la

dere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona; che i principi della tutela non si applicano a dati resi anonimi in modo tale che la persona interessata non è più identificabile; che i codici di condotta ai sensi dell'articolo 27 possono costituire uno strumento utile di orientamento sui mezzi grazie ai quali dati possano essere resi anonimi e registrati in modo da rendere impossibile l'identificazione della persona interessata".

[43] N. Härting, *Anonymität und Pseudonymität im Datenschutzrecht*, in *NJW*, 2013, 2065.

[44] Tale disposizione stabilisce che "i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità". Sul principio di necessità e sul suo rapporto con il tema dell'anonimato v. E. Morelato, *Il principio di necessità del trattamento: espressione di un nuovo diritto della personalità o regola generale per il trattamento dei dati personali con strumenti informatici?*, in G. Finocchiaro, a cura di, *Diritto all'anonimato. Anonimato, nome e identità personale*, cit., 209; R. D'Orazio, *Il principio di necessità nel trattamento dei dati personali*, in V. Cuffaro - R. D'Orazio - V. Ricciuto, a cura di, *Il codice del trattamento dei dati personali*, Torino, 2007, 19 ss.

[45] In tema E. Morelato, *Il principio di necessità del trattamento: espressione di un nuovo diritto della personalità o regola generale per il trattamento dei dati personali con strumenti informatici?*, cit., 209 ss.

[46] Cfr. E. Pelino, *L'anonimato su Internet*, in G. Finocchiaro, a cura di, *Diritto all'anonimato. Anonimato, nome e identità personale*, cit., 295.

[47] Sul punto v. N. Lugaresi, *Cittadino digitale e anonimato in rete*, accessibile all'indirizzo http://www. http://lugaresiunitn.wordpress.com/diritto-pubblico-di-internet/testi-e-materiali-13-14/, p. 7 del dattiloscritto.

[48] Si pensi, ad esempio, all'art. 55, c. 7, del d.lgs. 259/2003 (Codice delle comunicazioni elettroniche) che subordina l'attivazione di un servizio di telefonia mobile con carta pregapagata alla previa identificazione dell'utente da parte dell'impresa di telecomunicazione (tale disposizione è nella pratica molto rilevante, in considerazione dei caratteri del Web 2.0 e della frequenza con la quale l'accesso a Internet è effettuato tramite *smartphone*). I dati così raccolti devono poi essere notificati da parte del gestore del servizio al Ministero dell'interno

conservazione dei dati di traffico [49], rendendo così il principio dell'anonimato inoperante in radice. Per contro questo potrebbe logicamente riespandersi nel quadro dei rapporti tra l'utente e i terzi, divenendo — ovviamente sotto l'egida del consenso dell'interessato — lo strumento principe per assicurare il controllo della propria identità virtuale e dunque l'attuazione del diritto alla protezione dei dati [50]. Molto chiara, in tal senso, l'indicazione del Gruppo Art. 29 nel documento n. 5/2009 sui *social networks*, ove si ribadisce che, sulla base del principio di proporzionalità di cui all'art. 6 della direttiva 1995/46/CE, i *provider* dovrebbero consentire agli utenti di mantenere l'anonimato o far ricorso a pseudonimi nel contesto delle comunicazioni "on line" [51]. Tale prerogativa, già contemplata in un *Considerando* della direttiva 2000/31/CE [52], è espressamente garantita dalla legge tedesca sui media telematici, la quale rappresenta al riguardo un modello

(per un inquadramento di tale disciplina rinvio a G. Resta, *Systematic Government Access to Private-Sector Data in Italy*, in 4 *Int'l Data Privacy L.* 12, 19 (2014). Un analogo sistema di identificazione nominativa dell'utente era prescritto, relativamente all'uso delle reti civiche, dall'art. 7, c. 4, del d.l. n.144/ 2005 (c.d. "decreto Pisanu", convertito in legge con l. 31 luglio 2005, n. 155), il quale imponeva a titolari e gestori di esercizi pubblici, circoli privati e punti di accesso *wi-fi* di identificare gli utenti, registrandone le generalità (v. A. Bonfiglioli, *Il diritto all'anonimato al cospetto della legislazione penale dell'emergenza*, in G. Finocchiaro, a cura di, *Diritto all'anonimato. Anonimato, nome e identità personale*, cit., 229 ss., 247). Tale disposizione è stata ora abrogata dall'art. 2, c. 1•, d.l. 29 dicembre 2010, n. 225 (convertito in legge dalla l. 26 febbraio 2011, n. 10), secondo una prospettiva di politica del diritto orientata a consentire un accesso maggiormente 'aperto' alla rete Internet. L'art. 10, c. 1, del d.l. 21 giugno 2013, n. 69 (convertito in legge dalla l. 9 agosto 2013, n. 98) stabilisce infatti che « l'offerta di accesso alla rete Internet al pubblico tramite tecnologia WIFI non richiede l'identificazione personale degli utilizzatori ». Per i dettagli cfr. G. Giannone Codiglione, *Indirizzo IP, reti wi-fi e responsabilità per illeciti commessi da terzi*, in questa *Rivista*, 2013, 107 ss.; N. Lugaresi, *Cittadino digitale e anonimato in rete*, cit.

[49] Si vedano, per l'ordinamento italiano, gli artt. 122, 123 e 132 del Codice in materia di protezione dei dati personali (circa i quali cfr. E. Pelino, *L'anonimato su Internet*, cit., 295 ss.; A. Cappuccio, Privacy *e comunicazioni elettroniche*, in G.F. Ferrari, a cura di, *La legge sulla privacy dieci anni dopo*, Milano, 2008, 237-246). Su questo tema è necessario richiamare due importanti interventi della giurisprudenza: le decisioni del Tribunale costituzionale tedesco del 2010 [125 BVerfGE 260, 319 (2010)] e del 2012 (1 BvR 1299/05), che hanno prima rilevato vizi di costituzionalità del meccanismo di *data retention* previsto dal *Telekommunikationsgesetz*, poi approvandolo nella sua versione emendata [v. P. Schwartz, *Systematic Government Access to Private-Sector Data in Germany*, in 2 *Int'l Data Privacy L.* 289, 294 (2012)]; nonché la recente ed importante decisione della Corte di Giustizia del 8 aprile 2014, n° C-293/12, che ha invalidato la direttiva 2006/24/CE, in tema di conservazione dei dati di traffico, per contrasto con il sistema dei diritti fondamentali UE.

[50] E. Pelino, *L'anonimato su Internet*, cit., 298.

[51] Art. 29 Data Protection Working Party, *Opinion 5/2009 on online social networking*, 12-6-2009, 11, ove si osserva che "SNS may need to register some identifying data about members but does not need to publish the real name of members on the Internet. Therefore, SNS should consider carefully if they can justify forcing their users to act under their real identity rather than under a pseudonym. There are strong arguments in favor of giving users choice in this respect and in at least one Member State, this is a legal requirement. The argnments are particularly strong in the case of SNS with wide membership".

[52] Nell'ultima frase del *Considerando* 14 si legge: "[l]a presente direttiva non può impedire l'utilizzazione anonima di reti aperte quali Internet".

paradigmatico [53]. Il § 13, comma 6, del *Telemediengesetz* prevede che "il service provider deve permettere che l'uso dei servizi telematici e il relativo pagamento avvengano in via anonima o tramite il ricorso a pseudonimi, ogniqualvolta ciò risulti tecnicamente possibile e ragionevole. L'utente del servizio ha diritto di essere informato di tale possibilità" [54]. Tale regola è particolarmente rilevante, perché sancisce l'esistenza di una pretesa giuridicamente tutelata all'uso dei servizi telematici in forma anonima o tramite pseudonimi, entro i limiti indicati dalla disposizione medesima. Essa appare una diretta emanazione tanto della regola costituzionale sulla libertà di espressione di cui all'art. 5 *Grundgesetz* quanto della disciplina sulla protezione dei dati personali, che anche in Germania trova nel principio di necessità di cui al § 3a del *Bundesdatenschutzgesetz* uno dei suoi cardini fondamentali [55]. Coerentemente, si tende ad affermare la natura imperativa della norma, la quale — anche in quanto espressione della garanzia costituzionale della libertà di manifestazione del pensiero — non sarebbe suscettibile di deroga da parte dell'autonomia privata [56]. A riprova è opportuno ricordare una controversia che ha recentemente opposto l'Autorità di protezione dei dati personali dello Schleswig-Holstein, presieduta da Thilo Weichert, e la società Facebook. L'Autorità garante, in applicazione dei principi posti dal *Bundesdatenschutzgesetz*, aveva intimato a Facebook di modificare la propria *policy* in materia di apertura degli *account* personali, la quale è basata sul principio della identificazione nominativa degli utenti [57]. Ad avviso dell'autorità tale *policy* sarebbe risultata irrimediabilmente in contrasto con la normativa in tema di tutela dei dati personali, letta in combinazione con il § 13 comma 6 del *Telemediengesetz*, alla stregua del quale Facebook avrebbe dovuto concedere un utilizzo anonimo o tramite pseudonimi del servizio di *social networking*. Proposto ricorso amministrativo avverso tale provvedimento, sia il *Verwaltungsgericht* sia l'*Oberverwaltungsgericht* del Land Schleswig-Holstein hanno accolto le censure mosse da Facebook [58]. Tuttavia

[53] G. Spindler, *Persönlichkeitsschutz im Internet - Anforderungen und Grenzen einer Regulierung*, cit., 84; N. Härting, *Anonymität und Pseudonymität im Datenschutzrecht*, cit., 2067.

[54] § 13, c. 6, *Telemediengesetz* del 26. fehhraio 2007, come modificato dall'art. 1 della legge 31 maggio 2010: "Der Diensteanhieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren".

[55] N. Härting, *Anonymität und Pseudonymität im Datenschutzrecht*, cit., 2067; A. Roßnagel - P. Scholz, *Datenschutz durch Anonymität und Pseudonymität. Rechtsfolgen der Verwendung anonymer und pseudonymer Daten*, in *Multimedia und Recht*, 2000, 721, 722.

[56] In questo senso G. Spindler, *Persönlichkeitsschutz im Internet - Anforderungen und Grenzen einer Regulierung*, cit., 83, 120 (con particolare riferimento all'uso di pseudonimi).

[57] W. Ziebarth, *Das Datum als Geisel - Klarnamenspflicht und Nutzeraussperrung bei Facebook*, in *Zeitschrift für Datenschutz*, 2013, 375.

[58] VG Schleswig, 14-2-2013, Az. 8 B

tali tribunali non si sono espressi sul merito della questione, ma hanno basato la decisione unicamente sul profilo internazionalprivatistico della legge applicabile. Considerando, infatti, che tanto la sede legale quanto la collocazione fisica dei server di Facebook sono in Irlanda, le corti hanno ritenuto che la fattispecie dovesse essere governata dal diritto materiale irlandese e non da quello tedesco [59]. Indipendentemente dall'esito della controversia, è significativo il nesso, ivi enfatizzato, tra lo strumento dell'anonimato e la disciplina della protezione dei dati personali. Generalizzando quanto sin qui osservato, si può affermare che l'approccio europeo delinea un secondo modello di giustificazione della tecnica dell'anonimato, non già alternativo bensì cumulativo rispetto a quello della libertà d'espressione: il modello del controllo sulla circolazione dei dati personali [60].

2.3. *Identificabilità imposta per contratto o per legge: le* real name policies.

Il riferimento al caso *ULD Schleswig-Holstein c. Facebook* sposta naturalmente il discorso su un altro piano. Si deve, infatti, notare che, anche all'interno degli ordinamenti che stabiliscono in linea di principio la liceità del ricorso a tecniche di anonimato (o addirittura ne sollecitino l'adozione), vi possono essere regole di dettaglio che derogano a tale scelta in casi particolari [61]. Oppure può avvenire che la norma giuridica venga sostanzialmente svuotata della propria effettività per via di norme sociali o prassi contrattuali con essa contrastanti. Quest'ultima ipotesi è sempre più frequente nel mondo del Web 2.0 e dei *social networks*, che si connota proprio per essere un ambiente tendenzialmente "nonymous", piuttosto che "anonymous" [62]. Il caso di Facebook è stato già ricordato. Ma sono molti gli esempi di rapporti negoziali tra fornitori di servizi della società dell'informazione e utenti, i quali si conformano alla logica dell'identificabilità "imposta". Tra questi è ben noto quello del New York Times, che permette la

60/12 e 8 B 61/12, in *JurPC, Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPc Web Dok n. 43/2013 accessibile all'indirizzo http://www.jnrpc-.de/jnrpc/show?id=20130043; OVG Schleswig-Holstein, 22-4-2013, Az. 4 MB 10/13 in *NJW* 2013, 1977.

[59] In tema v. M. Karg, *Anwendbares Datenschutzrecht bei Internet-Diensteanbietern - TMG und BDSG vs. Konzernstrukturen?*, in *Zeitschrift für Datenschutz*, 2013, 371.

[60] In questa prospettiva v. anche G. Finocchiaro, *Conclusioni*, in Id., a cura di, *Diritto all'anonimato. Anonimato, nome e identità personale*, cit., 414.

[61] Se ne sono ricordati alcuni esempi nel paragrafo precedente. Per ulteriori informazioni v. E. Pelino, *L'anonimato su Internet*, cit., 289 ss.; A. Bonfiglioli, *Il diritto all'anonimato al cospetto della legislazione penale dell'emergenza*, cit., 229 ss.; G. Spindler, *Persönlichkeitsschutz im Internet - Anforderungen und Grenzen einer Regulierung*, cit., 33 ss.

[62] W. Hartzog - F. Stutzman, *The Case for Online Obscurity*, 101 *California L. Rev.* 1, 11 (2013); A. Ottolia, *Privacy e social networks: profili evolutivi della tutela dei dati personali*, in *AIDA*, 2011, 360.

pubblicazione di commenti anonimi sul proprio sito internet, ma a condizione di registrarsi presso il sito attraverso il proprio indirizzo di posta elettronica [63]. Questa è una *policy* condivisa da numerosi *provider*, i quali subordinano l'utilizzazione del servizio all'accesso mediante le credenziali fornite da uno dei principali *social networks*, a loro volta basati su sistemi di identificazione nominativa [64]. In tal modo la regola dell'anonimato viene sostanzialmente erosa per la forza di una prassi contrattuale, la quale, com'è noto, non si ferma di fronte ai confini del diritto nazionale e li travalica anche grazie all'ausilio della tecnologia. Non ci vuol molto a comprendere quali siano gli obiettivi perseguiti attraverso una siffatta tecnica negoziale: dietro le frasi di circostanza di qualche *manager* circa l'esigenza di preservare l'autenticità del messaggio e la responsabilità del loquente, si cela chiaramente l'intento di disporre di una preziosa riserva di dati personali da impiegare per scopi di profilazione e servizi di *direct marketing* [65].

Il caso degli attori privati è significativo, in quanto evidenzia quanto forte possa essere, in questa materia e più in generale nel contesto della società dell'informazione, la *normative Kraft des Faktischen*. Tuttavia esso non revoca apertamente in dubbio la legittimità del modello *normativo* dell'anonimato. Più rilevante, sotto questo profilo, è il riferimento ad alcune esperienze recenti, le quali spingono la logica di contrasto all'anonimato alle sue conseguenze più estreme, tanto da dar vita ad un *terzo modello*. Nel 2003 la Corea del Sud ha iniziato ad applicare una politica di restrizione di commenti e messaggi anonimi, la quale si è prima limitata ai siti con connotazioni politiche; poi, nel 2007, si è estesa a tutti i siti web al di sopra di un certo bacino di utenza [66]. Si è quindi imposto agli utenti di registrarsi al sito previa ostensione del proprio *Resident Registration Number* e si è stabilita la necessità nominatività di qualsiasi commento o messaggio reso pubblico in rete. Nel 2012 la Cina ha introdotto analoghe restrizioni relativamente ai servizi di *microblogging* [67]. Tuttavia, a

[63] R. Pérez-Peña, *New Sites Rethink Anonymous Online Comments*, in *New York Times*, 11-4-2010, accessibile all'indirizzo *http://www.nytimes.com/2010/04/12/technology/12comments.html?_r=0* (ultimo accesso 8 aprile 2014); S. Qasir, *Anonymity in Cyberspace: Judicial and Legislative Regulations*, cit., 3669, nota 157.

[64] E. Pelino, *L'anonimato su Internet*, cit., 301; M. Kaminski, *Reading Over Your Shoulder: Social Readers and Privacy Law*, 2 *Wake Forest L. Rev.* 13, 14 (2012).

[65] Cfr. S. Rodotà, *Il diritto di avere diritti*, cit., 393.

[66] Cfr. J.M. Leitner, *To Post Or Not to Post: Korean Criminal Sanctions for Online Expression*, 25 *Temp. Int'l & Comp. L.J.* 43, 61-64 (2011); E.S. Fish, *Is Internet Censorship Compatible with Democracy?: Legal Restrictions of Online Speech in South Korea*, 10 *Asia-Pacific J. Hum. Rts & L.*, 43 (2009).

[67] Per approfondimenti v. H.L. Hu, *Real Name Systems in Chinese Cyberspace. Authentication, Privacy, and State Capacity*, in 4 *Peking U.J. Legal Stud.* 207 (2013).

differenza della Corea, la disciplina cinese non assoggetta la comunicazione esterna al requisito dell'identificabilità, rimanendo leciti i commenti in forma anonima. Essa prescrive, invece, che il nome reale dell'utente sia registrato al momento dell'apertura dell'*account*, ma non debba essere necessariamente utilizzato in sede di discorso pubblico. È agevole notare come, in tal modo, non si persegua tanto l'obiettivo della protezione degli altrui diritti della personalità, rimanendo possibile diffondere commenti e giudizi di qualsiasi natura (anche diffamatoria) in forma anonima. Si realizza, però, almeno di fatto, la finalità di tacitare il dissenso. L'identità del loquente è, infatti, sempre tracciabile attraverso il riferimento ai dati dell'*account* e ciò produce inevitabilmente un effetto dissuasivo rispetto alle varie forme di critica politica e sociale [68]. È chiaro che, nei sistemi che adottino *real name policies*, il problema non è quello più della legittimità delle restrizioni dell'anonimato, ma torna ad essere quello (dal quale si erano prese le mosse) della stessa liceità del ricorso all'anonimato da parte di qualsiasi soggetto privato.

3. Anonimato e responsabilità degli intermediari.

È evidente che l'adozione di un regime di disciplina incentrato sul principio della liceità dell'anonimato solleva immediatamente il problema della responsabilità per gli atti lesivi di situazioni giuridiche altrui. L'altra faccia della medaglia della maggiore libertà concessa dallo schermo dell'anonimato consiste, infatti, in una riduzione delle barriere, di natura sociale o istituzionale, preordinate a prevenire la commissione di illeciti, sia in ambito patrimoniale sia non patrimoniale [69]. L'anonimato non è sempre sinonimo di redistribuzione del potere sociale, salvaguardia del dissenso politico, sfida alle costrizioni poste dai vincoli sociali e dalle condizioni di contesto. Esso può anche costituire, per via dell'assottigliamento delle norme sociali che governano il discorso nominativo, uno strumento di diffamazione a basso costo, *harassment* sessuale, incitazione all'odio razziale e ideologico [70]. Lo stesso effetto emancipatore dell'anonimato rischia di tradursi — in assenza di appropriati contrappesi istituzionali — nel suo opposto: la mancanza di imputazione soggettiva del messaggio può concretamente costituire un dispositivo nelle mani dei gruppi più violenti e intolleranti per la sopraffazione dei deboli e delle

[68] M.E. Kaminsky, *Real Masks and Real Name Policies*, cit., 878-879.

[69] Sulla duplice natura dell'anonimato v. F. Schauer, *Anonymity and Authority*, cit., 597.

[70] D. Keats Citron, *Cyber Civil Rights*, 89 *B.U. L. Rev.* 61, 64 (2009); B.H. Choi, *The Anonymous Internet*, in 72 *Maryland L. Rev.* 501 (2013); A.W. Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, cit. 1642-43.

minoranze [71]. Il caso dei *tweet* antisemiti, recentemente portato all'attenzione del *Tribunal de Grande Instance* di Parigi, ne costituisce una nitida dimostrazione [72].

Si pone pertanto con immediata evidenza il problema della determinazione dei soggetti chiamati a rispondere per gli illeciti perpetrati in forma anonima. Il pensiero va naturalmente, in primo luogo, al *provider*, in quanto questo è l'unico soggetto agevolmente identificabile dalla vittima di un messaggio lesivo, oltre ad essere di regola la parte dotata della maggiore solvibilità. Si tratta, tuttavia, di una soluzione notoriamente impervia, in quanto confliggente con una politica legislativa che, nell'intento di stimolare lo sviluppo della rete [73], ha cristallizzato ampie sfere di immunità a beneficio degli *Internet providers*. Negli USA, ove tale modello di disciplina ha avuto storicamente origine, la responsabilità dell'intermediario per contenuti anonimi originati da terzi è sostanzialmente esclusa per effetto della sinergia del *Digital Millenium Copyright Act* e del *Communications Decency Act* [74]. La Sect. 512 DMCA esonera da responsabilità gli intermediari che realizzano attività di *storage* dei materiali coperti da diritto d'autore, ogniqualvolta costoro abbiano un ruolo meramente passivo e si conformino alla procedura di "notifica e rimozione" prevista dalla legge [75]. A sua volta, la Sect. 230 CDA — la cui *occasio legis* è costituita dalla decisione *Stratton Oakmont v. Prodigy*, la quale aveva configurato in capo al *provider* un obbligo preventivo di sorveglianza circa i contenuti immessi in rete da terzi [76] — stabilisce che "nessun fornitore o utilizzatore di un servizio interattivo telematico sarà trattato come un editore nei confronti delle informazioni diffuse da un altro prestatore di contenuto" [77]. Tale disposizione è stata interpretata dalla giurisprudenza prevalente nel senso di escludere che un *provider*

[71] Tale aspetto è ben documentato da evidenze empiriche: v. D. Keats Citron, *Cyber Civil Rights*, cit., 68-81.

[72] TGI Paris, 241-1-2013, *UEIF et autres c. Twitter Inc. et Twitter France*, in *Dalloz*, 2013, 300, ove viene concesso un provvedimento cautelare volto ad imporre l'esibizione dei dati nominativi degli autori dei *tweets* antisemiti diffusi attraverso gli *hashtags* "#unbonjuif" e "#unjuifmort"; per una discussione v. J. Francillon, *Messages racistes ou antisémites postés sur le reseau social Twitter*, in *Rev. sc. crim.*, 2013, 566.

[73] Cfr. B.H. Choi, *The Anonymous Internet*, cit., 530.

[74] Per i necessari riferimenti v. R. Petruso, *La responsabilità civile degli e-providers nella prospettiva comparatistica*, in *Eur. dir. priv.*, 2011, 1107; R. Natoli, *La tutela dell'onore e della reputazione in Internet: il caso della diffamazione anonima*, in *Eur. dir. priv.*, 2001, 441 ss., 447; G.M. Riccio, *La responsabilità civile degli* internet providers, Torino, 2002.

[75] Da ultimo v. A. Bertoni - M.L. Montagnani, *Il ruolo degli intermediari Internet tra tutela del diritto d'autore e valorizzazione della creatività in rete?*, in *Giur. comm.*, 2013, 537 ss.

[76] *Stratton Oakmont, Inc.* v. *Prodigy Services Co.*, 1995 WL 323710 (N.Y. Sup. Ct. 1995), ove si afferma la responsabilità di un *provider*, in qualità di *publisher*, per le notizie diffamatorie inserite da un utente anonimo nella bacheca elettronica ospitata dal suo sito *Internet*.

[77] G.M. Riccio, *Diritto all'anonimato e responsabilità civile del provider*, in L. Nivarra - V. Ricciuto, a cura di, *Internet e il diritto dei privati. Persona e proprietà*

possa essere chiamato a rispondere per le notizie pubblicate da terzi, in forma nominativa o anonima, qualora costui non abbia avuto un ruolo "attivo" nel confezionamento del messaggio [78]. L'approccio europeo non si discosta molto da quello statunitense. La disciplina della responsabilità del *provider* delineata dalla quarta sezione della direttiva 2000/31/CE si ispira ad un principio analogo a quello che informa l'architettura del *DMCA*: l'esclusione di un obbligo generale di sorveglianza (art. 15, comma 1) ed esonera della responsabilità del fornitore della società dell'informazione che non sia a conoscenza dell'illiceità dei contenuti immessi in rete da terzi e che, se informato, agisca prontamente rimuovendo l'informazione lesiva (art. 14) [79]. A seguito della trasposizione della direttiva, i casi nei quali è stata effettivamente affermata la responsabilità del prestatore di un servizio della società dell'informazione per fatto di terzi si sono sensibilmente ridotti. In Italia, in particolare, la giurisprudenza ha abbandonato l'approccio più rigoroso adottato in una prima fase [80] e, sia pur con qualche oscillazione, ha fatto proprio il principio per cui il gestore di "piattaforme virtuali", come i *forum* di discussione, non può essere chiamato a rispondere allo stesso titolo di un direttore di giornale, qualora si limiti a svolgere un ruolo di mero intermediario tra l'autore dei contenuti (anche anonimi) e il pubblico e si conformi alle procedure di rimozione previste per legge [81].

In controtendenza rispetto a tale modello si muove la recente decisione della Corte europea dei diritti dell'uomo nel caso ***Delfi c. Estonia***, la quale ha rigettato il ricorso proposto (ai sensi

intellettuale nelle reti telematiche, Torino, 2002, 25 ss., 34.

[78] Per un panorama dettagliato v. la Note di S. McDonald, *Defamation in the Internet Age: Why* Roommates.com *Isn't Enough to Change the Rules for Anonymous Gossip Websites*, in 69 *Florida L. Rev.* 659 (2010).

[79] Per una nitida descrizione dell'impianto della direttiva e una comparazione con l'approccio statunitense v. G.M. Riccio, *La responsabilità degli* internet providers *nel d.lgs. n. 70/2003*, in *Danno e resp.*, 2003, 1157 ss.

[80] Per riferimenti cfr. G. Pino, *Assenza di un obbligo generale di sorveglianza a carico degli* Internet Service Providers *sui contenuti immessi da terzi in rete*, in *Danno e resp.*, 2004, 832, 836.

[81] V. di recente Trib. Viterbo, 14 ottobre 2010, in questa *Rivista*, 2011, 106, con nota di L. Vignudelli, *Il gestore del forum: spunti su identificazione dell'utente, anonimato e (ir)responsabilità*; Trib. Lucca, 20 agosto 2007, inedita (citata da R. Petruso, *La responsabilità civile degli e-providers nella prospettiva comparatistica*, cit.); Trib. Roma, ord. 4 luglio 1998, in questa *Rivista*, 1998, 807 ss., con nota di P. Costanzo, *I newsgroups al vaglio dell'Autorità giudiziaria (ancora a proposito della responsabilità degli attori d'Internet)*. Quanto all'inapplicabilità del regime di responsabilità previsto dall'art. 57 c.p. nei confronti del direttore di un periodico telematico v. Cass. pen., 1 ottobre 2010, n. 35511, in questa *Rivista*, 2010, 895, con nota di C. Melzi d'Eril, Roma locuta: *la Cassazione esclude l'applicabilità dell'art. 57 c.p. al direttore della testata giornalistica* on line; Cass. pen., 29 novembre 2011, n. 44126, in questa *Rivista*, 2011, 795, con nota di G.E. Vigevani, *La sentenza figlia sul direttore del giornale telematico: il caso Hamaui*; sul problema dell'estensione ai giornali "on line" dell'obbligo di registrazione previsto per la stampa cartacea v. Cass. pen., 10 maggio 2012, n. 23230, in questa *Rivista*, 2012, 1119, con nota di P. Di Fabio, *Blog, giornali on line e "obblighi*

dell'art. 10 della CEDU) da un grande portale di informazione a seguito della condanna al risarcimento dei danni non patrimoniali — di entità estremamente modesta — subiti da terzi per messaggi diffamatori anonimi ospitati sul sito del suddetto *provider* [82]. Grande rilievo assume, nel ragionamento della Corte, l'idea di un obbligo positivo di protezione gravante sugli stati e finalizzato ad assicurare una tutela adeguata degli interessi all'onore e alla reputazione, ritenuti parte integrante della garanzia di cui all'art. 8 della Convenzione europea dei diritti dell'uomo [83]. Ad avviso della Corte, una delle possibili tecniche di attuazione di un siffatto obbligo consisterebbe — in alternativa all'identificazione preventiva dell'autore del messaggio lesivo — nell'imputare in capo al gestore del sito una responsabilità per i danni arrecati dai contenuti anonimi, conformemente al criterio del *cuius commoda eius et incommoda* [84]. A questa soluzione si è da sempre obiettato il rischio di dar vita a forme di censura preventiva, arbitrariamente adottate da soggetti privati operanti esclusivamente in base alla

facoltativi" di registrazione delle testate telematiche: tra confusione del legislatore e pericoli per la libera espressione del pensiero su Internet. V. inoltre V. Zeno-Zencovich, *La pretesa estensione alla telematica del regime della stampa: note critiche*, in questa *Rivista*, 1998, 15 ss.; S. Sica, *Responsabilità del provider: per una soluzione "equilibrata" del problema*, in *Corr. giur.*, 2013, 4, 506; S. Sica - G. Giannone Codiglione, *Social network sites e il 'labirinto' delle responsabilità*, in *Giur. Merito*, 2012, 2714.

[82] Corte Europea Dir. Uomo, 10 ottobre 2013, App. n. 64569/09, *Delfi AS c. Estonia*, in questa *Rivista*, n. 1/2014, con nota di F. Vecchio, *Libertà di espressione e diritto all'onore in internet secondo la sentenza Delfi AS contro Estonia della Corte europea dei diritti dell'uomo Libertà di espressione e diritto all'onore in internet secondo la sentenza Delfi AS contro Estonia della Corte europea dei diritti dell'uomo*. Per un'attenta valutazione del possibile impatto della decisione *Delfi AS c. Estonia* sui sistemi giuridici nazionali, ed in particolare su quello tedesco, v. L. Schapiro, *Anhaltende Rechtsunsicherheit für die Betreiber von Internetmeinungsportalen? Das Urteil des EGMR « Delfi AS v. Estonia » und seine Auswirkungen auf die deutsche Rechtslage*, in *ZUM*, 2014, 201. Fra i precedenti più noti in tema di responsabilità dell'*hosting provider* per contenuti anonimi e lesivi di diritti della personalità altrui cfr. TGI Paris, 9 giugno 1998 e App. Paris, 10 febbraio 1999, in questa *Rivista*, 1999, 926 con nota di G.M. Riccio, *La responsabilità del provider nell'esperienza francese: il caso Hallyday*.

[83] La riconducibilità di tali interessi all'ambito di protezione dell'art. 8 è sistematicamente affermata sin dalla decisione della Corte Europea Dir. Uomo, 15 febbraio 2008, App. n. 12556/03, *Pfeifer c. Austria*.

[84] Corte Europea Dir. Uomo, 10 ottobre 2013, App. n. 64569/09, *Delfi AS c. Estonia*, cit. Della pronunzia si confrontino in particolare i parr. 84-92, ove la corte esclude che la stessa adozione di un sistema di filtraggio e di *notice and take down* da parte del *provider* siano elementi idonei a giustificare un esonero della responsabilità. Decisiva appare la considerazione per cui l'intermediario, nel momento in cui renda possibile la pubblicazione di commenti anonimi da parte di utenti non registrati, assume un rischio il quale giustifica l'applicazione di una regola di responsabilità (rilevante qui nell'ottica dell'obbligo positivo di protezione gravante sugli stati) secondo logiche analoghe a quelle operanti *off line* della tutela del danneggiato e della razionale amministrazione dei rischi d'impresa: "The Court has taken note of the applicant company's argument that the affected person conld have brought a claim against the actual authors of the comments. It attaches more weight, however, to the Government's counter-argument that for the purposes of bringing a civil claim it was very difficult for an individual to establish the identity of the persons to be sued. Indeed, for purely technical reasons it would

logica economica dei costi e dei benefici [85]. Tuttavia, una ragionevole restrizione della sfera d'immunità garantita ai fornitori di servizi della società dell'informazione deve ritenersi auspicabile, atteso che in molti casi la stessa strutturazione del sito o la tipologia dei servizi offerti appaiono indici piuttosto univoci del ruolo non meramente passivo svolto dal *provider* e del suo concorso nella produzione dell'evento lesivo [86]. La giurisprudenza è talora giunta a tali conclusioni nel campo della proprietà intellettuale, ritenendo il fornitore di un servizio di *file sharing* responsabile per gli illeciti commessi dagli utenti sotto lo schermo dell'anonimato [87]. Ma tale ragionamento può essere esteso al campo degli illeciti in materia di diritti della personalità. Si pensi, ad esempio, alla proliferazione dei siti di *gossip* finalizzati a sollecitare e sfruttare, per obiettivi di profitto, i messaggi scandalistici e diffamatori, come "JuicyCampus.com" o "DontDateHimGirl.com" [88]. O si consideri il caso, ancor più rilevante nella pratica, dei siti che propongono servizi di *rating* personale, altrimenti definiti di *social scoring*, come "votailprof.it", "ratemyprofessors.com" (valutazione dei docenti) o "arzt.weisse-liste.de" (valutazione dei medici) [89], o di *rating* imprenditoriale, come "holidaycheck.com" [90]. Un'analisi attenta delle modalità organizzative di tali siti dimostra come il *provider* assuma un'iniziativa diretta e svolga un ruolo propulsivo nel sollecitare e presentare i giudizi

appear disproportionate to put the onus of identification of the authors of defamatory comments on the injured person in a case like the present one. Keeping in mind the State's positive obligations under Article 8 that may involve the adoption of measures designed to secure respect for private life in the sphere of the relations of individuals between themselves (see Von Hannover (no. 2), cited above, § 98, with further references), the Court is not convinced that measures allowing an injured party to bring a claim only against the authors of defamatory comments — as the applicant company appears to suggest — would have, in the present case, guaranteed effective protection of the injured person's right to private life. *It notes that it was the applicant company's choice to allow comments by non-registered users, and that by doing so it must be considered to have assumed a certain responsibility for these comments*" (par. 92, cors. aggiunto).

[85] Tale obiezione è riproposta, da ultimo, da G.E. Vigevani, *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano*, in questa *Rivista*, n. 2/2014.

[86] In questa prospettiva v. le considerazioni di V. Zeno-Zencovich, *Anonymous Speech on the Internet*, cit., 16; G. Spindler, *Persönlichkeitsschutz im Internet — Anforderungen und Grenzen einer Regulierung*, cit., 61 ss.

[87] In questo senso cfr. OLG Hamburg, 28 marzo 2012, in *ZUM-RD*, 2013, 536.

[88] In tema S. McDonald, *Defamation in the Internet Age: Why* Roommates.com *Isn't Enough to Change the Rules for Anonymous Gossip Websites*, cit., 271 ss. Nel senso dell'estensione della responsabilità del *provider* per contenuti anonimi immessi da terzi G.M. Riccio, *Diritto all'anonimato e responsabilità civile del provider*, cit., 37.

[89] A. Lauber-Rönsberg, *Rechtsdurchsetzung bei Persönlichkeitsrechtsverletzungen im Internet Verantwortlichkeit von Intermediären und Nutzern in Meinungsforen und Personenbewertungsportalen*, in *Multimedia und Recht*, 2014, 10 ss.; K.N. Peifer - J. Kamp, *Datenschutz und Persönlichkeitsrecht - Anwendung der Grundsätze über Produktkritik auf das Bewertungsportal « pickmich.de »?*, in *ZUM*, 2009, 185.

[90] Per un caso rilevante v. OLG Hamburg, 18 gennaio 2012, in *ZUM-RD*, 2012, 669.

degli utenti. Saremmo al cospetto di una situazione di questo tipo, ad esempio, ogniqualvolta l'intermediario metta a disposizione degli utenti una griglia predefinita di valutazione dei servizi offerti da un professionista liberale o da un insegnante, ove tra i parametri di giudizio sia contemplato il carattere più o meno "sexy", o "trasandato" del soggetto valutato (parametri che, com'è ovvio, possono aumentare il rischio di messaggi lesivi della personalità) [91]; oppure qualora si proceda all'aggregazione per categorie e alla trasposizione in un giudizio di sintesi delle valutazioni individualmente espresse dagli utenti, in modo tale da alterare e 'arricchirne' il significato [92]. In tali casi è difficile affermare che il *provider* non abbia svolto — mutuando il lessico e le categorie adottate dalla Corte di giustizia [93] — un ruolo "attivo" nel sollecitare i messaggi lesivi o nel prestare forme di "assistenza" all'utente al fine di ottimizzare le modalità di presentazione dei servizi. Pertanto, non potrebbe legittimamente invocarsi il particolare regime di esonero della responsabilità delineato dalla direttiva 2000/31/CE e dovrebbe logicamente affermarsi la responsabilità, diretta o a titolo di concorso, dell'intermediario [94].

4. La responsabilità dell'utente anonimo e il problema dell'identificazione in sede processuale.

Sta di fatto, comunque, che il regime di (ir)responsabilità del *provider* adottato dal legislatore comunitario fa sì che il più delle

[91] G. Spindler, *Persönlichkeitsschutz im Internet - Anforderungen und Grenzen einer Regulierung*, cit., 63; A. Lauber-Rönsberg, *Rechtsdurchsetzung bei Persönlichkeitsrechtsverletzungen im Internet Verantwortlichkeit von Intermediären und Nutzern in Meinungsforen und Personenbewertungsportalen*, cit., 11. Per un caso molto rilevante in materia (che però si conclude con un diniego di tutela nei confronti della vittima dell'addebito diffamatorio) v. BGH, 23 giugno 2009, *Spickmich.de*, cit., sul quale si veda il commento di G. Gounalakis - C. Klein, *Zulässigkeit von personenbezogenen Bewertungsplattformen. Die "Spickmich"-Entscheidung des BGH vom 23.6.2009*, in *NJW*, 2010, 566.

[92] Per un esempio significativo tratto dalla giurisprudenza v. LG Kiel, 6 dicembre 2013, in *BeckRS*, 2014, 03139, ove la responsabilità del *provider* viene esclusa. Più esigente nei confronti dei *provider*, in quanto incentrata su una lettura rigorosa della disciplina in materia di protezione di dati personali, è la prospettiva adottata dalle corti francesi: TGI Paris, 3 marzo 2008, accessibile all'indirizzo *https://www.legalis.net / spip.php?page=jurisprudence-decision&id_article=2234*; CA Paris, 25 giugno 2008, accessibile all'indirizzo *http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2349* (cfr. K.N. Peifer - J. Kamp, *Datenschutz und Persönlichkeitsrecht - Anwendung der Grundsätze über Produktkritik auf das Bewertungsportal « spickmich.de »?*, cit,. 185-186).

[93] In particolare v. Corte di Giustizia CE, 12 luglio 2011, C-324/09, *L'Oréal c. eBay International AG*, par. 123, in *AIDA*, 2011, 480, con nota di J.B. Nordemann, *Liability of Social Networks for IP Infringements (Latest News): The EU Law Regime after l'Oréal/eBay*; C. Czychowski - J.B. Nordemann, *Grenzenloses Internet - entgrenzte Haftung. Leitlinien für ein Haftungsmodell der Vermittler?*, in *GRUR-Beilage*, 2014, 3 ss., 5.

[94] In questo senso G. Spindler, *Persönlichkeitsschutz im Internet - Anforderungen und Grenzen einer Regulierung*, cit., 61 ss.; A. Lauber-Rönsberg, *Rechtsdurchsetzung bei Persönlichkeitsrechtsverletzungen im Internet Verantwortlichkeit von Intermediären und Nutzern in Meinungsforen und Personenbewertungsportalen*, cit., 11.

volte l'unica via percorribile per assicurare una prima forma di tutela delle vittime e prevenire la diffusione dei messaggi anonimi a carattere violento, diffamatorio e discriminatorio sia costituita dall'azione diretta nei confronti dell'autore del messaggio stesso. Non si tratta, tuttavia, di una soluzione scevra da difficoltà, in quanto il superamento del velo dell'anonimato e l'imputazione della responsabilità in capo ad un soggetto ben determinato solleva non pochi problemi di natura tecnica, prima ancora che giuridica [95]. Basti notare, dal primo punto di vista, che anche assumendo la collaborazione volontaria del *provider* nell'esibizione dei dati identificativi della fonte del messaggio lesivo, non è detto che ciò permetta l'individuazione della persona fisica responsabile, poiché il messaggio potrebbe essere stato immesso in rete da una postazione pubblica, oppure utilizzando appositi *software* o siti di anonimizzazione [96], oppure perché i dati anagrafici comunicati dall'utente al *provider* potrebbero rivelarsi falsi [97]. Ma anche prescindendo dai problemi di ordine fattuale, vi sono diversi ostacoli giuridici che si frappongono al "superamento del velo". La preservazione dell'anonimato contro la pretesa all'ostensione dei dati nominativi nell'ambito di una controversia giudiziaria potrebbe infatti essere intesa come una proiezione sul piano processuale degli interessi costituzionalmente garantiti alla libertà di manifestazione del pensiero [98] e alla protezione dei dati personali [99]. Per tracciare un quadro sintetico dei problemi coinvolti dal conflitto tra accesso alla giustizia e salvaguardia dell'anonimato converrà prendere le mosse dall'esperienza nordamericana, ove il tema dell'*anonymous litigation* ha sollecitato

[95] Per una limpida esposizione dei problemi tecnici coinvolti v. F. Di Ciommo, voce *Internet I) Responsabilità civile*, in *Enc. Giur., Agg.*, XIX, Roma, 2001, 5.

[96] Con riferimento ai problemi originati dall'impiego della tecnologia TOR, v. ad es. K.D. Watson, *The Tor Network: A Global Inquiry Into the Legal Status of Anonymity Networks*, in 11 *Wash. U. Global Stud. L. Rev.* 715 (2012); per la questione, in parte connessa, degli illeciti compiuti facendo ricorso reti wi-fi aperte v. G. Giannone Codiglione, *Indirizzo IP, reti wi-fi e responsabilità per illeciti commessi da terzi*, cit., 107 ss.

[97] G.M. Riccio, *La responsabilità degli* internet providers *nel d.lgs. n. 70/2003*, cit., 1166.

[98] Questa, come si è osservato in precedenza, è la prospettiva accolta in prevalenza nel sistema statunitense (cfr. L.B. Lidsky, *Anonymity in Cyberspace: What Can We Learn from John Doe?*, cit., 1376 ss.). Per un confronto con la prospettiva italiana v. i contributi di M. Manetti, *Libertà di pensiero e anonimato in rete*; G.E. Vigevani, *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano*; M. Cuniberti, *Democrazie, dissenso politico e tutela dell'anonimato*, tutti in questa *Rivista*, n. 2/2014; v. altresì M. Betzu, *Anonimato e responsabilità in Internet*, in *Costituzionalismo.it*, n. 2/2011.

[99] Emblematiche, a questo riguardo, sono le controversie portate all'attenzione delle corti europee in merito all'accesso dei dati nominativi degli utenti responsabili di *download* di *file* protetti dal diritto d'autore: per un quadro di sintesi v. A. Ottolia, *Proprietà intellettuale e trattamento dei dati personali: riflessioni su privacy "per il sistema" e "nel sistema"*, in *AIDA*, 2010, 319; R. Caso, *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint - Profili di diritto comparato*, in *Dir. Internet*, 2007, 471.

un'ampia riflessione, tanto nel contesto dei rapporti *off line* quanto nella sfera telematica.

4.1. *L'esperienza statunitense: dalle azioni proposte in forma anonima al* John Doe subpoena.

È opportuno ricordare, innanzitutto, che nei sistemi di *common law* la prassi del ricorso a pseudonimi, come Doe, Roe e Poe è molto risalente nel tempo e può essere ricondotta, in particolare, alle controversie in materia possessoria e di diritti reali. La generalizzazione dell'azione di *ejectment* quale rimedio a tutela delle posizioni proprietarie è risultata possibile proprio mediante il ricorso a finzioni giuridiche, le quali avevano come protagonisti personaggi immaginari generalmente designati con i nomi di "John Doe" e "Richard Roe" [100]. Il *Code of Civil Procedure* di New York (1848), opera di David Dudley Field, segna l'ingresso dello schema all'interno di un testo legislativo, quale strumento processuale volto a consentire la proposizione di un'azione civile nei confronti di un convenuto il cui patronimico fosse ignoto all'attore [101]. "When the plaintiff shall be ignorant of the name *of a defendant*, such defendant may be designated in any pleading or proceeding, by any name; and when his true name shall be discovered, the pleading or proceeding may be amended accordingly" [102]. Con il *Field Code* lo strumento in esame si trasforma quindi da elemento di una finzione giuridica a pseudonimo di una persona in carne ed ossa, benché non ancora identificata. Per effetto della rapida diffusione di tale codice, il meccanismo in esame si estese alla gran parte delle giurisdizioni statali e di qui, per effetto della regola processuale che imponeva l'applicazione della legge statale del luogo in cui avesse sede l'organo giudicante, anche alle corti federali [103]. Senonché l'introduzione delle *Federal Rules of Civil Procedure* del 1938 segnò un punto d'arresto, dal momento che tale testo non contemplava la possibilità di agire in forma anonima o nei confronti di un *defendant* anonimo. Di qui un orientamento ondivago e spesso restrittivo della giurisprudenza federale in ordine all'ammissibilità di tale tecnica processuale, il quale proseguì sino agli Sessanta [104]. A questo punto due sviluppi paralleli intervennero a modificare il quadro di riferi-

---

[100] H.J. Berman, *Law and Revolution*, II, *The Impact of the Protestant Reformations on the Western Legal Tradition*, Cambridge-London, 2003, 278.

[101] C.M. Rice, *Meet John Doe: It Is Time for Federal Civil Procedure to Recognize John Doe Parties*, in 57 *Un. Pittsburgh L. Rev.* 883, 890-892 (1996).

[102] Act of April 12, 1848, ch. 379, § 150, 1848 N.Y. Laws 497, 526.

[103] C.M. Rice, *Meet John Doe: It Is Time for Federal Civil Procedure to Recognize John Doe Parties*, cit., 892-893.

[104] Per i dettagli v. C.M. Rice, *Meet John Doe: It Is Time for Federal Civil Procedure to Recognize John Doe Parties*, cit., 894.

mento. Da un lato si diffuse il ricorso ad azioni proposte in forma anonima (ossia da un *plaintiff* identificato solo attraverso pseudonimi) nel quadro delle controversie in materia di *constitutional privacy* [105]. D'altro lato, si moltiplicarono le azioni proposte nei confronti di un *convenuto* anonimo per violazione dei diritti e delle libertà fondamentali, in tutti quei casi nei quali la vittima non fosse stata in grado di identificare in maniera precisa l'effettivo responsabile dell'illecito e ciononostante intendesse radicare una causa, anche al fine di avvalersi degli strumenti della *discovery* e di interrompere il decorso della prescrizione [106]. Si pensi, tipicamente, delle azioni promosse dagli attivisti contro le forze di polizia per la repressione violenta di manifestazioni e altre forme di protesta, particolarmente frequenti nell'epoca — siamo tra gli anni '60 e '70 — delle lotte per i diritti civili e delle proteste contro la guerra nel Vietnam. Su questo terreno, a partire dal celebre caso *Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics* [107], le corti hanno colmato la lacuna legislativa, elaborando un insieme di principi finalizzati a soddisfare le esigenze di parte attrice in punto di proposizione e mutamento dell'azione [108]. Con l'avvento di Internet i casi di *anonymous litigation* sono aumentati in misura esponenziale [109]. Nell'ipotesi di illecito perpetrato in forma anonima, infatti, l'attore non ha altra soluzione se non proporre l'azione nei confronti di un convenuto ignoto, affidandosi ai rimedi processuali ordinari per l'identificazione in corso di causa [110]. Tecnicamente ciò si realizza attraverso lo strumento, disciplinato anche dalla rule 45 delle *Federal Rules of Civil Procedure*, del *writ of subpoena*, il quale consiste nell'intimazione rivolta a un *non-party witness* — altrimenti soccorrerebbero le regole in materia di *discovery* — di prestare testimonianza o produrre uno o più documenti rilevanti per la lite (rispettivamente *subpoena ad testificandum* e *subpoena*

[105] La prima causa di rilievo è *Poe v. Ullmann* [367 U.S. 497 (1961)], avente ad oggetto il problema della legittimità costituzionale delle restrizioni circa l'uso dei contraccettivi, poi definitivamente cassate dalla Corte Suprema con la celebre pronunzia *Griswold v Connecticut* [381 U.S. 479 (1965)]. In seguito la soluzione dell'anonimato dell'attore finirà per consolidarsi nei casi 'sensibili' in materia di libertà di disposizione del corpo, *sexual harassment*, controversie in materia di lavoro e discriminazioni, affermandosi una serie di tecniche di bilanciamento volte a contemperare l'esigenza dell'anonimato con la pubblicità del processo e i diritti alla difesa del convenuto (per una disamina più approfondita di questo sviluppo sia consentito rinviare a G. Resta, *Privacy e processo civile: il problema della* litigation *"anonima"*, in questa *Rivista*, 2005, 681, 696 ss.).

[106] C.M. Rice, *Meet John Doe: It Is Time for Federal Civil Procedure to Recognize John Doe Parties*, cit., 895 ss.

[107] *Bivens v. Six Unknown Named Agents*, 403 U.S. 388 (1971).

[108] C.M. Rice, *Meet John Doe: It Is Time for Federal Civil Procedure to Recognize John Doe Parties*, cit., 919 ss.

[109] A.W. Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, cit.

[110] S. Qasir, *Anonymity in Cyberspace: Judicial and Legislative Regulations*, cit., 3673; L.B. Lidsky, *Anonymity in Cyberspace: What Can We Learn from John Doe?*, cit., 1373 ss.

duces tecum) [111]. Nell'ipotesi degli illeciti commessi *on line*, tale ordine assume generalmente una duplice direzione: si ingiunge prima all'*online service provider* (quale ad es. Twitter o Google) di comunicare all'attore l'IP dinamico dell'offensore, per poi rivolgersi all'*access provider* per ottenere il disvelamento dei dati anagrafici dell'intestatario della connessione corrispondente al suddetto indirizzo IP [112]. Poiché l'intermediario "online" ha ben di rado ragione di contestare il provvedimento e notificarlo al convenuto *in pectore*, generalmente le controversie relative all'ammissibilità del *subpoena* si concentreranno soprattutto sul secondo passaggio procedurale. La riconducibilità dell'anonimato all'interno della sfera di protezione del Primo Emendamento costituisce la principale ragione di opposizione al *subpoena*. In linea di massima tale argomento ha incontrato il favore delle corti statunitensi, in quanto le garanzie del Primo Emendamento si ritengono generalmente estensibili alla sfera dei rapporti telematici [113]. Tuttavia non vi sono indicazioni normative sufficientemente puntuali — fatta eccezione per il regime estremamente liberale previsto dalla Sect. 512*h* del DMCA, ritenuto non suscettibile di applicazione generale al di fuori del campo della proprietà intellettuale [114] — sul modo in cui impostare il bilanciamento tra l'interesse alla tutela giudiziaria dei diritti e le prerogative della libertà d'espressione. Si comprende, quindi, come le corti statali e federali abbiano avuto modo di dibattere a lungo sullo *standard* al quale uniformarsi in relazione alle differenti tipologie di 'discorso' coinvolto, essendo a tutti evidente che un regime di *disclosure* troppo liberale avrebbe l'inconveniente di limitare molto il ricorso all'anonimato quale strumento di espressione di dissenso e critica, mentre un regime troppo restrittivo

---

[111] Per alcune informazioni essenziali sullo strumento del *subpoena*, il quale com'è noto ha assunto un ruolo storicamente molto rilevante nello sviluppo del diritto di *equity*, v. G. Lebovits, *Drafting New York Civil-Litigation Documents: Part XXX - Subpoenas*, in 86 *New York State Bar Ass. J.* 4 (2014); circa le differenze intercorrenti tra la disciplina inglese e quella statunitense cfr. V. Barsotti, voce *Subpoena*, in *Dig. disc. priv.*, XIX, Torino, 1999, 75.

[112] S. Moore, *The Challenge of Internet Anonymity: Protecting John Doe on the Internet*, in 26 *J. Marshall J. Computer & Info. L.* 469, 472 (2009).

[113] *Reno v. ACLU*, 521 U.S. 844 (1997).

[114] Tale disposizione stabilisce che in caso di violazione di diritti di proprietà intellettuale, la persona legittimata, dopo avere intrapreso una *notice and take down procedure*, possa presentare presso la cancelleria di *qualsiasi* corte statunitense la domanda volta ad ottenere l'ostensione dei dati anagrafici corrispondenti ad un numero IP previamente identificato attraverso programmi informatici. L'*access provider* che non intenda conformarsi a tale ordine giudiziale dovrà proporre una *motion to quash* per contestarne la legittimità. In tema cfr. A. Kao, *RIAA v. Verizon: Applying the Subpoena Provision of the DMCA*, in 19 *Berkeley Tech. L. J.* 405 (2004); D. Gorski, *The Future of the Digital Millennium Copyright Act Subpoena Power on the Internet in Light of the Verizon Cases*, 24 *Rev. Litig.* 149 (2005); B. Choi, *The Anonymous Internet*, cit., 511 ss.; e in giurisprudenza *RIAA v. Verizon Internet Servs., Inc.*, 257 F. Supp. 2d 244 (D.D.C. 2003), *rev'd*, 351 F.3d 1229 (D.C. Cir. 2003); *RIAA v. Verizon Internet Servs., Inc.*, 240 F. Supp. 2d 24 (D.D.C. 2003, *rev'd*, 351 F.3d 1229 (D.C. Cir. 2003).

avrebbe l'effetto opposto di paralizzare l'accesso alla giustizia e la tutela delle vittime di messaggi diffamatori o discriminatori [115]. In una prima fase, la quale si estende cronologicamente sino alla fine degli anni '90, la concessione dell'ordine di *disclosure* è stata subordinata a presupposti sufficientemente elastici, richiedendosi all'attore di dimostrare, oltre alla rilevanza dell'informazione richiesta e alla sussistenza di un principio di prova, anche il requisito della "buona fede" [116]. Tale approccio non è andato esente da critiche, in quanto risultava di fatto funzionale alle strategie di repressione del dissenso adottate dalle *corporation* nei confronti di privati cittadini, ridotti al silenzio attraverso la minaccia di azioni per *defamation*, rivelazione di informazioni riservate o violazione della proprietà intellettuale (strategie contrastate anche a livello legislativo in diversi stati americani) [117]. In una seconda fase, inaugurata dalla decisione *Dendrite International v. Doe* [118], le corti hanno sensibilmente irrigidito i parametri di giudizio, attribuendo una protezione più intensa all'interesse all'anonimato e quindi alla logica del *First Amendment* [119]. Due sono gli elementi fondamentali del *test* più frequentemente adottato dalle corti [120]. In primo luogo si richiede una notificazione preventiva della domanda giudiziale all'autore del contenuto illecito, il quale deve essere informato della possibilità di proporre una *motion to quash* a tutela del proprio anonimato. Ovviamente, poiché l'attore non è generalmente a conoscenza dell'identità del convenuto, il requisito della notificazione preventiva è inteso in maniera flessibile, ritenendosi sufficiente una notifica in forma elettronica, generalmente attraverso il sito Internet che aveva ospitato l'originario messaggio lesivo [121]. In

[115] Su questo tema si è stratificata un'ampia letteratura. Tra i molti scritti v. N. Gleicher, *John Doe Subpoenas: Towards a Consistent Legal Standard*, 118 *Yale L.J.* 320, 360-61 (2008); R.M. Martin, *Freezing the Net: Rejecting a One-Size-Fits-All Standard for Unmasking Anonymous Internet Speakers in Defamation Lawsuits*, 75 *U. Cin. L. Rev.* 1217 (2007); L.B. Lidsky, *Anonymity in Cyberspace: What Can We Learn from John Doe?*, 50 *B.C. L. Rev.* 1373 (2009); D. Sobel, *The Process That "John Doe" Is Due: Addressing the Legal Challenge to Internet Anonymity*, 5 *Va. J.L. & Tech* 3 (2000); V.S. Ekstrand, *Unmasking Jane and John Doe: Online Anonymity and the First Amendment*, 8 *Comm. L. & Pol'y* 405 (2003).

[116] S. Moore, *The Challenge of Internet Anonymity: Protecting John Doe on the Internet*, cit., 473; S. Qasir, *Anonymity in Cyberspace: Judicial and Legislative Regulations*, cit., 3673.

[117] L.B. Lidsky, *Anonymity in Cyberspace: What Can We Learn from John Doe?*, cit., 1374. Sui c.d. *anti-SLAPP (Strategic Lawsuits Against Public Participation) statutes*, adottati al momento da 20 stati americani, v. S. Qasir, *Anonymity in Cyberspace: Judicial and Legislative Regulations*

[118] *Dendrite Int'l, Inc. v. Doe, No. 3*, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001).

[119] Cfr. K. Wein, *Dendrite v. Doe: A New Standard for Protecting Anonymity on Internet Message Boards*, in 42 *Jurimetrics* 465 (2002); S. Moore, *The Challenge of Internet Anonymity: Protecting John Doe on the Internet*, cit., 478.

[120] L.B. Lidsky, *Anonymity in Cyberspace: What Can We Learn from John Doe?*, cit., 1377.

[121] L.B. Lidsky, *Anonymity in Cyberspace: What Can We Learn from John Doe?*, cit., 1377.

secondo luogo, grava sull'attore l'onere di fornire di seri indizi della fondatezza della domanda principale (sia essa fondata sui *tort* di *defamation*, *false light*, etc.), tali da evidenziare il carattere non bagatellare ed opportunistico della pretesa e da permettere un bilanciamento oggettivo degli interessi confliggenti [122]. Numerose sono le decisioni in materia e differenti i criteri applicati, articolati su una scala di rigore crescente, che va dal semplice requisito della *good faith* [123] sino alla prova dell'attitudine a resistere ad una *motion to dismiss* [124], o infine ad una *motion for summary judgment* [125]. Non potendo qui entrare nei dettagli, sarà sufficiente limitarsi a rilevare due dati [126]. Il primo è che il modello di disciplina adottato nel sistema statunitense implica, rispetto alla politica delle *real name policies* discusse in precedenza [127], una tutela rafforzata dell'interesse all'anonimato, il quale viene sottoposto a bilanciamento con l'interesse alla tutela dei diritti soltanto nella fase (eventuale) del contenzioso e sotto lo stretto controllo dell'autorità giudiziaria. Il secondo è che, ad una considerazione di sintesi degli strumenti normativi utilizzabili e delle concrete applicazioni giurisprudenziali, emerge piuttosto chiaramente come nel conflitto con l'interesse all'anonimato le posizioni proprietarie abbiano generalmente la meglio rispetto alle situazioni della persona. Nelle cause in tema di violazione della proprietà intellettuale, in altri termini, la propensione delle corti a concedere il *John Doe subpoena* appare nettamente maggiore di quanto avvenga nel caso di azioni a proposte a tutela della reputazione e di altri diritti della personalità [128]. Ciò è coerente con l'assunto generale per cui il *commercial speech* gode di una protezione meno intensa rispetto alle altre forme di discorso pubblico (e in particolare rispetto al *political*, *religious* o *literary speech*) [129], ma dà vita ad un evidente problema di ragionevolezza

[122] S. Moore, *The Challenge of Internet Anonymity: Protecting John Doe on the Internet*, cit., 478-479.

[123] *In re Subpoena Duces Tecum to America Online, Inc.*, 52 Va. Cir. 26 (Cir. Ct. 2000); un siffatto modello di disciplina è stato poi recepito nella legislazione della Virginia (S. Qasir, *Anonymity in Cyberspace*, cit., 3674).

[124] *Columbia Insurance Co. v. Seescandy.com*, 185 F.R.D. 573 (N.D. Cal. 1999).

[125] *Doe v. Cahill*, 884 A.2d 451 (Del. 2005).

[126] Per una discussione dei vari criteri elaborati dalle corti v. S. Moore, *The Challenge of Internet Anonymity: Protecting John Doe on the Internet*, cit., 481 ss.; S. Qasir, *Anonymity in Cyberspace*, cit., 366 ss.; R.G. Larson - P.A. Godfread, *Bringing John Doe to Court: Procedural Issues in Unmasking Anonymous Internet Defendants*, in 38 *William Mitchell L. Rev.* 328 (2011). Gli sviluppi più recenti al livello della giurisdizione federale sono analizzati da P.A. Levy, *Developments in Dendrite*, in 14 *Fl. Coastal L. Rev.* 1 (2012).

[127] Cfr. *supra* par. 2.3.

[128] Cfr. *SonyMusic Entm't Inc. v. Does 1-40*, 326 F. Supp. 2d 556 (S.D.N.Y. 2004); nonché i casi più recenti discussi in P.A. Levy, *Developments in Dendrite*, cit., 28 ss.; e B.H. Choi, *The Anonymous Internet*, cit., 508 ss.

[129] Cfr. quanto osservato in *In re Anonymous Online Speakers*, 661 F.3d 1168 (9th Cir. 2011); v. anche *Art of Living Foundation v. Does 1-10*, No. 10-CV-05022-LHK, 2011 WL 5444622 (N.D. Cal. Nov. 9, 2011); *S103, Inc. v. Bodybuilding.com*,

della disciplina, alla luce del diverso valore rispettivamente assunto dalla tutela della dignità umana e della proprietà nel quadro dell'assiologia costituzionale.

4.2. *Prospettive europee.*

Se si volge lo sguardo al di qua dell'Oceano si potrà constatare come, nonostante la diversità delle premesse accolte in punto di tutela della libertà di espressione [130] e la divergenza degli assetti processuali di riferimento (basti ricordare l'impossibilità, nei sistemi continentali, di agire contro un convenuto ignoto, il *John Doe* dell'esperienza USA) [131], i problemi che emergono, e in parte anche le soluzioni operative accolte, non si discostano in maniera radicale da quelle statunitensi. Comune, come si è visto in precedenza, è l'assenza di divieti generalizzati del ricorso all'anonimato e o a pseudonimi nelle comunicazioni in rete [132]; non dissimile è il regime di limitazione della responsabilità del *provider*, benché sul punto le corti europee abbiano manifestato di recente alcuni segnali di insofferenza [133]; analoga è la scelta di traslare il bilanciamento tra la garanzia dell'anonimato e la tutela dei diritti nella fase processuale del contenzioso, astenendosi dall'introdurre obblighi preventivi di identificazione del loquente e rimettendo all'autorità giudiziaria — sia pur nel quadro di vincoli processuali differenti — la decisione in ordine alle richieste di ostensione dei dati identificativi dell'utente avanzate nei confronti del *provider* [134]. Soprattutto, si ripropone anche qui, sia pure in misura meno eclatante, in quanto filtrato dal paradigma del controllo sulla circolazione dei dati personali, lo squilibrio tra tutela delle posizioni proprietarie e tutela dei diritti della personalità [135]. Esso emerge in maniera lampante già al livello del formante legale e si riproduce, sia pure in maniera più attenuata, anche sul piano giurisprudenziale.

Innanzitutto si deve rilevare che, a seguito dell'approvazione della direttiva 2004/48/CE, gli Stati Membri si sono dotati di un sistema processuale di tutela della proprietà intellettuale partico-

LLC, No. 10-35308, 2011WL 2565618 (9th Cir. June 29, 2011).

[130] Cfr. R. Errera, *Freedom of Speech in Europe and in the USA*, in G. Nolte, a cura di, *European and US Constitutionalism*, Cambridge, 2005, 23 ss.; V. Zeno-Zencovich, *Freedom of Expression. A Critical and Comparative Analysis*, Abingdon-New York, 2008, 89 ss.

[131] A. Lauber-Rönsberg, *Rechtsdurchsetzung bei Persönlichkeitsrechtsverletzungen im Internet Verantwortlichkeit von Intermediären und Nutzern in Meinungsforen und Personenbewertungsportalen*, cit., 13.

[132] Cfr. *supra*, parr. 2.1 e 2.2.

[133] Cfr. *supra*, par. 3.

[134] G. Spindler, *Persönlichkeitsschutz im Internet - Anforderungen und Grenzen einer Regulierung*, cit., 58 ss.; A. Lauber-Rönsberg, *Rechtsdurchsetzung bei Persönlichkeitsrechtsverletzungen im Internet Verantwortlichkeit von Intermediären und Nutzern in Meinungsforen und Personenbewertungsportalen*, cit., 13.

[135] Cfr. *supra*, par. 4.1.

larmente incisivo e penetrante [136]. Esso annovera al suo interno anche misure istruttorie, e segnatamente lo strumento dell'ordine di esibizione e della richiesta di informazioni su fatti rilevanti per il processo, il quale rende utili servigi anche nel campo degli illeciti commessi "on line" in forma anonima [137]. Nel nostro ordinamento tale strumento è ora codificato negli artt. 156 *bis* e 156 *ter* della legge n. 633/1941, ove si prevede che "qualora una parte abbia fornito seri elementi dai quali si possa ragionevolmente desumere la fondatezza delle proprie domande ed abbia individuato documenti, elementi o informazioni detenuti dalla controparte che confermino tali indizi, essa può ottenere che il giudice ne disponga l'esibizione oppure che richieda le informazioni alla controparte. Può ottenere altresì, che il giudice ordini alla controparte di fornire gli elementi per l'identificazione dei soggetti implicati nella produzione e distribuzione dei prodotti o dei servizi che costituiscono violazione dei diritti di cui alla presente legge" (art. 156 *bis* l. n. 633/1941) [138]. Analogamente dispongono, in materia di privative industriali, gli artt. 121 e ss. del Codice della proprietà industriale. Si può notare, pertanto, come in questa materia il meccanismo ordinario dell'esibizione documentale, previsto dall'art. 210 del codice di procedura civile, sia stato adattato alle peculiarità della materia coinvolta, esteso sotto il profilo dell'ambito soggettivo ed oggettivo d'applicazione e reso più incisivo [139]. Analoghe previsioni si ritrovano, ad esempio, nell'ordinamento tedesco, che ha codificato gli *Auskunftsan-*

[136] Cfr. M.M. Walter - D. Goebel, *Enforcement Directive*, in M.M. Walter - S. von Lewinsky, a cura di, *European Copyright Law. A Commentary*, Oxford, 2010, 1193 ss.; A. Giussani, *La disciplina comunitaria della tutela giurisdizionale della proprietà intellettuale*, in L.C. Ubertazzi, a cura di, *La proprietà intellettuale*, in *Trattato di diritto privato dell'Unione Europea*, diretto da G. Ajani e G.A. Benacchio, Torino, 2011, 459 ss.; L. Nivarra, a cura di, *L'enforcement dei diritti di proprietà intellettuale: profili sostanziali e processuali*, Milano, 2005; G. Cumming - M. Freudenthal - R. Janal, *Enforcement of Intellectual Property Rights in Dutch, English and German Civil Courts*, Alphen aan den Rijn, 2008. In tema va fatto un cenno anche al Regolamento in materia di diritto d'autore sulle reti di comunicazione elettronica recentemente adottato dall'Autorità per le Garanzie nelle Comunicazioni (Delibera n. 680/13/CONS del 12 dicembre 2013).

[137] In generale v. L.P. Comoglio, *Istruzione e discovery nei giudizi in materia di proprietà industriale*, in *AIDA*, 2000, 270 ss.; A. Giussani, *La disciplina comunitaria della tutela giurisdizionale della proprietà intellettuale*, cit., 464.

[138] B. Cunegatti, *Tutela cautelare e rimedi specifici nel diritto d'autore*, in G. Finocchiaro, a cura di, *Diritto all'anonimato. Anonimato, nome e identità personale*, cit., 365; G. Di Fazzio, in L.C. Ubertazzi, *Commentario breve alle leggi su proprietà intellettuale e concorrenza*, V ed., Padova, 2012, 1853.

[139] La giurisprudenza ha sottolineato l'innovatività delle misure previste dalla legge sul diritto d'autore soprattutto sotto il profilo dell'ambito soggettivo d'applicazione dell'ordine di esibizione: cfr. Trib. Roma, ord. 1 marzo 2007, in questa *Rivista*, 2007, 821, ove si afferma che l'art. 156 *bis* l.d.a. avrebbe una portata più ampia del meccanismo previsto dall'art. 210 c.p.c. in quanto l'ordine di esibizione ordinario sarebbe esperibile soltanto "nei confronti della controparte processuale, ossia quella ritenuta antagonista diretta rispetto al diritto azionato", mentre la prima disposizione citata farebbe gravare l'obbligo di ostensione non soltanto in capo all'autore della violazione, ma anche in capo a coloro

sprüche relativi al diritto d'autore nel § 101 *Urhebergesetz*. Il comma 9 di tale norma stabilisce, in particolare, che in caso di richiesta di esibizione dei dati di traffico e dati anagrafici corrispondenti agli indirizzi IP dinamici, il soggetto leso deve inoltrare un'apposita istanza al *Landgericht* competente, la cui sezione civile dovrà giudicare della legittimità di una siffatta domanda, specie alla luce del criterio di proporzionalità richiamato nel comma 4 della norma citata. Tale cognizione si connota come preliminare rispetto ad una seconda fase della controversia, connotata dalla proposizione della domanda di inibizione o risarcimento dei danni nei confronti dell'utente così identificato. Disposizioni analoghe si ritrovano nel § 140b *Patentgesetz*, § 24b *Gebrauchsmustergesetz*, § 46 *Geschmacksmustergesetz*, § 37b *Sortenschutzgesetz* e § 19 *Markengesetz* [140].

Per contro, nel campo della tutela dei diritti della personalità non sono previsti specifici ordini di *disclosure*, assimilabili a quelli forgiati nel settore della proprietà intellettuale [141]. L'art. 12 della direttiva 1995/46/CE contempla il diritto d'accesso, e tuttavia questo è circoscritto unicamente ai rapporti tra l'interessato e il titolare del trattamento: è uno strumento, per così dire, teleologicamente orientato alla riduzione dell'ammontare delle informazioni circolanti e non al suo 'ampliamento' tramite comunicazione di dati di terzi non conosciuti dall'interessato [142]. È ben vero che nella normativa in materia di protezione dei dati è prevista una

che forniscano servizi utilizzati per la violazione dei diritti di proprietà intellettuale (i *provider*); Trib. Roma, ord. 26 aprile 2007, Trib. Roma, ord. 26 aprile 2007, in *Riv. dir. ind.*, 2008, II, 330, 335: "Pur essendo vero che l'*actio ad exhibendum* di cui all'art. 210 c.p.c. non può avere ad oggetto documenti che non abbiano una originaria destinazione probatoria comune alle parti, è altresì vero che a tale regola deroga il combinato disposto degli artt. 156 e 156 *bis* l. 633/1941, in tema di tutela del diritto di autore". Secondo un'altra tesi, la peculiarità delle nuove misure istruttorie andrebbe invece cercata soprattutto sul piano dell'ambito oggettivo d'applicazione: per un'ampia e puntuale trattazione di questi problemi v. M. De Cata, *Il caso "Peppermint". Ulteriori riflessioni anche alla luce del caso "Promusicae"*, in nota alle pronunzie citate, in *Riv. dir. ind.*, 2008, II, 404 ss., spec. 414-425; A. Giussani, *La disciplina comunitaria della tutela giurisdizionale della proprietà intellettuale*, cit., 464; per riferimenti dottrinali e giurisprudenziali circa le misure previste dall'art. 210 c.p.c. v. V. Carnevale, *sub* art. 210, in L.P. Comoglio - C. Consolo - B. Sassani - R. Vaccarella, *Commentario del codice di procedura civile*, III, 1, Torino, 2012, 667 ss.

[140] Per i necessari approfondimenti v. G. Cumming - M. Freudenthal - R. Janal, *Enforcement of Intellectual Property Rights in Dutch, English and German Civil Courts*, Alphen aan den Rijn, 2008, 246 ss.

[141] G. Spindler, *Persönlichkeitsschutz im Internet - Anforderungen und Grenzen einer Regulierung*, cit., 58; C. Czychowski - J.B. Nordemann, *Grenzenloses Internet - entgrenzte Haftung. Leitlinien für ein Haftungsmodell der Vermittler?*, cit., 12.

[142] In generale v. C. Lo Surdo, *Gli strumenti di tutela del soggetto 'interessato' nella legge e nella sua concreta applicazione*, in R. Pardolesi, a cura di, *Diritto alla riservatezza e circolazione dei dati personali*, I, Milano, 2003, 617 ss.; E. Bargelli, *Sub* art. 13, in C.M. Bianca - F.D. Busnelli, a cura di, *Tutela della privacy. Commentario alla l. 31 dicembre 1996, n. 675*, in *Le nuove leggi civili commentate*, 1999, 394 ss., 407 ss.; G. Conte, *Diritti dell'interessato e obblighi di sicurezza*, in V. Cuffaro - V. Ricciuto, a cura di, *La*

causa di esclusione del consenso per l'ipotesi del trattamento per "finalità di giustizia" (art. 24, lett. *f*, d.lgs. 196/2003) [143]. Tuttavia, essa non appare di per sé idonea a fondare la legittimità di una richiesta di ostensione di dati di terzi in assenza di un'autonoma base normativa (quale, ad esempio, quella offerta dall'art. 132 del d.lgs. 196/2003, o nell'ordinamento tedesco dall'art. 14 del *Telemediengesetz*) [144]. Discorso in parte analogo potrebbe farsi per l'obbligo — consistente nel "fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite" — contemplato dall'art. 15, comma 2, della direttiva 2000/31/CE e reso effettivo nel nostro ordinamento dall'art. 17 del d.lgs. 70/2003: esso non soltanto è limitato ai rapporti tra *provider* e utenti vincolati da "accordi di memorizzazione dei dati", ma non pare neanche idoneo a rappresentare un'autonoma base normativa alla quale ricondurre misure istruttorie esperibili a fini di tutela *civile* della personalità [145]. Pertanto, in assenza di disposizioni più specifiche, dovrà farsi necessariamente riferimento agli strumenti processuali ordinari, siano essi di fonte legislativa o giurisprudenziale (come l'*Auskunftsanspruch* fondato sul § 242 *BGB*, noto all'esperienza tedesca) [146].

Questa discrasia sembra riflettersi sul piano del diritto giurisprudenziale. Nel campo della proprietà intellettuale è accolto — sia pure in maniera non incontestata e con soluzioni diversificate a livello nazionale [147] — l'assunto per cui la vittima di un illecito possa ottenere dal *provider* l'ostensione del registro dei dati di traffico e gli ulteriori dati identificativi del responsabile di una violazione. La Corte di Giustizia, pur avendo posto un freno

disciplina del trattamento dei dati personali, I, Torino, 1997, 225 ss., 243.

[143] In tema v. G. Buonomo, *Il trattamento dei dati personali in ambito giudiziario*, in V. Cuffaro - R. D'Orazio - V. Ricciuto, a cura di, *Il codice del trattamento dei dati personali*, Torino, 2007, 277 ss., 284.

[144] Questi argomenti sono stati ampiamente dibattuti nel quadro delle controversie sul *file sharing:* cfr. per riferimenti A. Ottolia, *Proprietà intellettuale e trattamento dei dati personali: riflessioni su privacy "per il sistema" e "nel sistema"*, in *AIDA*, 2010, 319, 335.

[145] Per una valorizzazione di tale norma nel contesto delle azioni di responsabilità civile nei confronti del *provider* v. G.M. Riccio, *La responsabilità degli* internet providers *nel d.lgs. n. 70/2003*, cit., 1166.

[146] G. Spindler, *Persönlichkeitsschutz im Internet - Anforderungen und Grenzen einer Regulierung*, cit., 58.

[147] Emblematica, a questo proposito, è l'esperienza italiana, ove più significative sono state le resistenze giudiziarie alle pretese di ostensione dei dati nominativi degli utenti, in contrasto con i precetti del Codice in materia di protezione dei dati personali: v. in part. Trib. Roma, ord. 19 agosto 2006, in questa *Rivista*, 2007, 815; Trib. Roma, ord. 27 settembre 2006, in *AIDA*, 2007, 960 (accoglimento della domanda di ostensione); Trib. Roma, ord. 1 marzo 2007, cit.; Trib. Roma, ord. 26 aprile 2007, cit. (che accoglie la domanda di ostensione dei dati identificativi dell'utente anonimo proposta in via d'urgenza *ex* art. 156 *bis*); Trib. Roma, ord. 14 luglio 2007, in questa *Rivista*, 2007, 828; Trib. Roma, ord. 22 novembre 2007, in *Foro it.*, 2008, I, 1329 (provvedimento di

all'uso di strumenti di filtraggio e sorveglianza generalizzata, non ha escluso la possibilità che i giudici nazionali ordinino la comunicazione dei dati identificativi del responsabile di una violazione, nel rispetto dei principi di proporzionalità e tutela dei dati personali [148]. Dialogando apertamente con la Corte di Giustizia, il *Bundesgerichtshof* tedesco ha accolto di recente una lettura estensiva del § 101 *UrhG*, confermando la legittimità dell'ordine di esibizione anche nelle ipotesi di violazioni non condotte "su scala commerciale" [149]. Ad avviso del Tribunale Federale, le esigenze di giustizia sarebbero tali da far retrocedere le pur legittime aspettative di *privacy* rivendicate dagli utenti anonimi. Pur rimarcando la necessità di un bilanciamento caso per caso ispirato al principio della proporzionalità, il *BGH* afferma in maniera risoluta che "in uno stato di diritto neanche Internet può dar vita a spazi privi di regole" [150].

Quest'ultima è senza dubbio un'affermazione importante e condivisibile. Il problema è che, non appena si abbandona il terreno della proprietà intellettuale, protetto da reti di filo spinato sempre più fitte ed estese e salvaguardato da *vigilantes* dotati di potenti mezzi tecnologici e ampie risorse finanziarie, il grado di effettività di tale assunto tende a scemare in misura preoccupante. Nel campo dei diritti della personalità, in particolare, l'assenza di strumenti normativi tanto incisivi quanto quelli previsti a tutela delle posizioni proprietarie sembra indurre le corti a un atteggiamento molto più remissivo e rispettoso dell'interesse all'anonimato, a discapito delle stesse esigenze di tutela giudiziaria dei diritti altrove solennemente declamate [151]. Di ciò l'esperienza

---

rigetto della domanda di ostensione); Trib. Roma, ord. 17 marzo 2008, in questa *Rivista*, 2008, 384 (nel senso del rigetto dell'ordine di *discovery*); Trib. Roma, ord. 15 aprile 2010, in *AIDA*, 2010, 999. In tema v. Per una discussione dei casi più rilevanti in materia v. A. Ottolia, *Proprietà intellettuale e trattamento dei dati personali: riflessioni su privacy "per il sistema" e "nel sistema"*, cit., 319 ss.; R. Caso, *Il conflitto tra* copyright *e* privacy *nelle reti Peer to Peer: il caso Peppermint - Profili di diritto comparato*, in *Dir. Internet*, 2007, 471.

[148] Corte giust. Unione europea, 24 novembre 2011, n. 70/10, *Scarlet Extended S A c. Société belge auteurs*; Corte giust. Unione europea, 16 febbraio 2012, n. 360/10, *Belgische Vereniging van Auteurs c. Netlog NV* e Corte giust. Unione europea, 19 aprile 2012, n. 461/10, *Bonnier Audio A B c. Perfect Communication Sweden* A B (di cui si vedano in part. i parr. 55-61), in questa *Rivista*, 2012, 297, con nota di P. Sammarco, *Alla ricerca del giusto equilibrio da parte della corte di giustizia Ue nel confronto tra diritti fondamentali nei casi di impiego di sistemi tecnici di filtraggio*; e in *Nuova giur. civ. comm.*, 2012, I, 571, con nota di M. Colangelo, *Internet e sistemi di filtraggio tra enforcement del diritto d'autore e tutela dei diritti fondamentali: un commento ai casi « Scarlet » e « Netlog »*.

[149] BGH, 19-4-2012, in *NJW* 2012, 2958, con nota di K.H. Ladeur. In tema, anche per ulteriori riferimenti giurisprudenziali, v. S. Brüggemann, *Urheberrechtsdurchsetzung im Internet. Ausgewählte Probleme des Drittauskunftsanspruchs nach § URHG § 101 UrhG*, in *Multimedia und Recht*, 2013, 278 ss.; C. Czychowski - J.B. Nordemann, *Grenzenloses Internet - entgrenzte Haftung. Leitlinien für ein Haftungsmodell der Vermittler?*, cit., 11.

[150] BGH, 19-4-2012, cit., 2962: "in einem Rechtsstaat darf auch das Internet keinen rechts-freien Raum bilden".

[151] Cfr. l'analisi A. Lauber-Rönsberg, *Rechtsdurchsetzung bei Persönlichkeits-*

tedesca offre una limpida testimonianza. L'assenza di un rimedio specifico, quale quello previsto in materia di proprietà intellettuale, ha indotto a ricorrere a strumenti sussidiari, come l'*Auskunftsanspruch* atipica, basata sul § 242 *BGB* e la cui concessione è rimessa al prudente apprezzamento del giudice, chiamato ad operare un delicato bilanciamento degli interessi in conflitto [152]. L'esito di tale bilanciamento non è scontato e predeterminabile in astratto. Tuttavia, in diversi casi recenti, concernenti addebiti lesivi della reputazione espressi all'interno di siti di *personal rating*, l'ordine di *disclosure* è stato sistematicamente negato. Il caso più recente è quello deciso il 3 luglio 2013 dal *Landgericht* di Monaco e avente ad oggetto la valutazione negativa operata dall'utente di un sito di *rating* professionale nei confronti di un medico pediatra, accusato di incompetenza e scarsa professionalità [153]. Nel rigettare la domanda di ostensione dei dati nominativi proposta dalla vittima nei confronti del gestore del *Bewertungsportal*, la Corte ha sottolineato che: *a*) l'utilizzazione anonima del sito è normativamente prevista dal § 13 *Telemediengesetz*; *b*) tale disciplina osta al trattamento di dati personali (ivi compresa la comunicazione a terzi) per finalità diverse da quelle prescritte dalla legge; *c*) il § 14, comma 2, di tale legge prevede la comunicazione dei dati a terzi nei soli casi di richieste dell'autorità giudiziaria e di polizia finalizzate alla prevenzione e alla repressione di determinati reati, nonché alla *tutela dei diritti di proprietà intellettuale*, ma non nelle ipotesi di lesione di diritti della personalità; *d*) l'*Auskunftsanspruch* atipica di cui al § 242 *BGB* è esclusa in quanto prevale nella materia dei servizi telematici la norma speciale del § 14 *Telemediengesetz* [154]. Altrettanto rilevante è la pronunzia dell'*Oberlandesgericht* di Hamm del 3 agosto 2011 [155]. La Corte ha rigettato la richiesta di ostensione dei dati relativi all'identità di un paziente, autore di messaggi lesivi della personalità di uno psicoterapeuta, sulla base di un duplice ordine di considerazioni. In primo luogo la Corte ha attribuito un particolare rilievo sistematico al § 13 del *Telemediengesetz*, che, come si è più volte ricordato, riconosce il diritto di utilizzare i servizi Internet in forma anonima. In secondo luogo essa ha espressamente ricondotto l'interesse all'anonimato alla garanzia costituzionale della libertà di comunicazione di cui all'art. 5

rechtsverletzungen im Internet Verantwortlichkeit von Intermediären und Nutzern in Meinungsforen und Personenbewertungsportalen, cit., 13 ss.

[152] G. SPINDLER, *Persönlichkeitsschutz im Internet - Anforderungen und Grenzen einer Regulierung*, cit., 58.

[153] LG München, 3 luglio 2013, in *ZUM*, 2013, 979.

[154] LG München, 3 luglio 2013, cit., 980. Per un'attenta discussione di questi argomenti v. A. LAUBER-RÖNSBERG, *Rechtsdurchsetzung bei Persönlichkeitsrechtsverletzungen im Internet Verantwortlichkeit von Intermediären und Nutzern in Meinungsforen und Personenbewertungsportalen*, cit., 13-14.

[155] OLG Hamm, 3 agosto 2011, in *ZUM-RD*, 2011, 684.

Grundgesetz, attribuendo peraltro notevole rilevanza alla natura di "giudizi di valore" (e non di "statuizioni fattuali") dei messaggi incriminati [156]. In considerazione dei notevoli problemi incontrati nella pratica sono state proposte soluzioni alternative, come l'inasprimento del regime di responsabilità del *provider* [157], o l'estensione in via legislativa alle ipotesi di violazione dei diritti della personalità dell'ordine di *disclosure* previsto nella materia della proprietà intellettuale [158].

5. Considerazioni conclusive.

Nell'introdurre il discorso sin qui condotto si è fatto cenno all'esigenza di "contestualizzare" temi e problemi dell'anonimato, guardandosi dal rischio di appiattire questioni oggettivamente eterogenee in nome di un malinteso spirito sistematico. Nel concludere la riflessione è bene conformarsi ad un'analoga direttiva, evitando di rincorrere l'allettante, quanto ingenua, prospettiva di individuare modelli regolatori 'ottimali'. Ciò risulterebbe non soltanto in contrasto con l'elevata complessità delle problematiche coinvolte, che richiedono risposte tipicamente "a geometria variabile", ma anche con un canone metodologico alquanto diffuso — benché non incontrastato — nell'ambito della scienza della comparazione giuridica. Piuttosto che nel fornire soluzioni *ready-made*, l'utilità dell'approccio comparatistico risiede soprattutto nell'evidenziare problemi e spiegarne le connessioni con le particolari condizioni di contesto di un determinato ordinamento o tradizione giuridica.

Un primo problema che è emerso è quello dell'effettiva attuazione pratica della pretesa individuale all'anonimato (riconduci-

[156] OLG Hamm, 3 agosto 2011, cit., 685, ove si osserva che: "Die für das Internet typische anonyme Nutzung entspricht zudem auch der grundrechtlichen Interessenlage, da eine Beschränkung der Meinungsfreiheit auf Äußerungen, die einem bestimmten Individuum zugerechnet werden, mit Art. GG Artikel 5 Abs. GG Artikel 5 Absatz 1 Satz 1 GG nicht vereinbar ist. Die Verpflichtung, sich namentlich zu einer bestimmten Meinung zu bekennen, würde allgemein die Gefahr begründen, dass der Einzelne aus Furcht vor Repressalien oder sonstigen negativen Auswirkungen sich dahingehend entscheidet, seine Meinung nicht zu äußern. Dieser Gefahr der Selbstzensur soll durch das Grundrecht auf freie Meinungsäußerung entgegengewirkt werden (BGH *ZUM* 2009, Seite 753). Es bedarf keiner näheren Ausführung des Senats dazu, dass die Gefahr des Eintritts negativer Auswirkungen insbesondere anch für denjenigen besteht, der sich als Patient ans dem Behandlungsbereich der Psychotherapie unter Angabe seiner persönlichen Daten zu erkennen gibt. Vorliegend kommt hinzu, dass der Kläger die Auffassung vertritt, dass ihm gegenüber dem anonymen Verfasser der Äußerung ein Schadensersatzanspruch wegen der Verletzung von Pflichten aus dem Behandlungsvertrag zusteht, sodass die Preisgabe der Anonymität des Verfassers auch aus diesem Grund zu der in Art. GG Artikel 5 Abs. GG Artikel 5 Absatz 1 GG geschützten Meinungsfreiheit in Widerspruch stünde".

[157] G. Spindler, *Persönlichkeitsschutz im Internet - Anforderungen und Grenzen einer Regulierung*, cit., 59 ss.

[158] A. Lauber-Rönsberg, *Rechtsdurchsetzung bei Persönlichkeitsrechtsverletzungen im Internet Verantwortlichkeit von Intermediären und Nutzern in Meinungsforen und Personenbewertungsportalen*, cit., 13-14.

bile, a seconda dei casi e degli ambienti culturali di riferimento, alla libertà di espressione o al diritto alla protezione dei dati personali), al cospetto di un'evoluzione dell'ambiente telematico che tende a divenire sempre più "nonymous" e sempre meno "anonymous" [159]. Quali sono le strategie giuridiche utilizzabili per assicurare una effettiva salvaguardia dell'interesse a manifestare il proprio pensiero in forma anonima, oltre che a fruire dei servizi telematici senza subire forme sottili ma invasive di sorveglianza elettronica? Una risposta sufficientemente univoca è stata offerta dall'ordinamento tedesco, che ha configurato un obbligo del *provider* — e correlativo diritto dell'utente — di permettere, ove tecnicamente possibile e ragionevole, l'utilizzazione dei servizi telematici in forma anonima [160]. E tuttavia questa risposta, che risponde a una logica di diritto territoriale, si scontra con la natura a-territoriale della rete e con la difficoltà di chiudere in una maglia di regole statuali attività che lo stesso diritto globale ha configurato come libere di spostarsi nei luoghi ritenuti socialmente e economicamente più convenienti. Il caso *ULD Schleswig-Holstein c. Facebook* ha fatto emergere in maniera nitida i limiti intrinseci di una soluzione 'locale' [161].

Un secondo problema evidenziato è relativo allo squilibrio che connota, in molteplici sistemi giuridici, il rapporto tra anonimato e responsabilità. Le soluzioni sin qui elaborate al fine di assicurare un'adeguata tutela civile alle vittime di illeciti non possono ritenersi ancora soddisfacenti. Non a caso si sono registrati alcuni sviluppi significativi su entrambi i fronti della responsabilità: quello dell'intermediario professionale e quello dell'utente anonimo. Dal primo punto di vista si sono moltiplicate le voci tese a sostenere la necessità di un ridimensionamento del regime di limitazione della responsabilità del *provider*, talora invocando un vero e proprio obbligo — una sorta di *Verkehrssicherungspflicht* — consistente nell'accertamento preventivo dell'identità dell'utente [162]. Tale obbligo non precluderebbe la facoltà per il singolo di interagire anonimamente nei rapporti con i terzi (prerogativa aprioristicamente esclusa dalle più rigide tra le *real name policies*), ma farebbe salva — ribadita la riserva di giurisdizione —

[159] E ciò non soltanto in considerazione dei caratteri che distinguono il Web 2.0 (alle quali si è fatto cenno in precedenza, par. 2.3) ma anche della maggiore capacità individualizzante dell'Internet Protocol Versione 6 (cfr. per i dettagli tecnici B. Freund - C. Schnabel, *Bedeutet IPv6 das Ende der Anonymität im Internet? - Technische Grundlagen und rechtliche Beurteilung des neuen Internet-Protokolls*, in *Multimedia und Recht*, 2011, 495 ss.).

[160] Cfr. *supra*, par. 2.2.

[161] Cfr. *supra*, par. 2.2.

[162] In questo senso v. G. Spindler, *Persönlichkeitsschutz im Internet - Anforderungen und Grenzen einer Regulierung*, cit., 112; V. Zeno-Zencovich, *Anonymous Speech on the Internet*, cit,. 16; G.M. Riccio, *La responsabilità degli* internet providers *nel d.lgs. n. 70/2003*, cit., 1166; M. Betzu, *Anonimato e responsabilità in Internet*, cit., 13-15; in giurisprudenza v. Corte Europea Dir. Uomo, 10 ottobre 2013, App. n. 64569/09, *Delfi AS c. Estonia*, cit.

l'identificabilità dell'utente in caso di commissione di fatti illeciti. Si tratta di una prospettiva in linea di massima promettente e condivisibile, non soltanto perché in linea con le indicazioni del Gruppo Art. 29 [163], ma anche perché riprodurrebbe un modello di disciplina speculare a quello delineato dalla direttiva 2004/23/CE in materia di donazione, conservazione e impiego di cellule e tessuti per uso umano [164], assegnando di fatto ai *provider* un ruolo di *trusted third parties*; tuttavia sarebbe difficile ipotizzarne un'elaborazione coerente in via giurisprudenziale, essendo invece auspicabile un meditato intervento legislativo che si preoccupi di assicurarne il coordinamento con la normativa in materia di protezione dei dati personali. Dal secondo punto di vista sono state avanzate alcune perplessità nei confronti del sistema processuale di identificazione del responsabile di illeciti "on line" (sia di quello adottato nell'ordinamento statunitense, sia di quello presente in alcuni sistemi continentali), in quanto eccessivamente farraginoso e spesso *overprotective* dell'interesse all'anonimato, a detrimento delle esigenze di tutela giudiziaria dei diritti altrui [165].

Il terzo problema, strettamente connesso a quello appena evidenziato, consiste nell'*enforcement* selettivo dell'interesse all'anonimato. Come si è cercato di chiarire in precedenza, una tendenza univoca percorre tutti i sistemi, sia pure in forme e con intensità differenti [166]. Essa è costituita dalla propensione ad accordare una tutela forte alle posizioni proprietarie e una più debole alle situazioni della persona. Quando l'anonimato si presenta come strumento di violazione dei diritti di proprietà intellettuale (tipicamente nelle ipotesi di *file sharing*), le barriere frapposte dall'ordinamento a protezione della "on line" *obscurity* tendono a farsi molto tenui. Quando invece la posizione contrapposta è di natura non proprietaria, l'aspettativa di anonimato si riespande sensibilmente, sino in alcuni casi a paralizzare le stesse possibilità di accesso alla tutela giurisdizionale. Tale duplicità di regime potrebbe forse essere spiegata argomentando in base alla diversa rilevanza del "discorso" operato in forma anonima: nel secondo caso una vera e propria forma di manifestazione del pensiero; nel primo caso un atto privo (almeno il più delle volte) di autonoma valenza 'comunicativa' e non sussumibile all'interno della sfera di protezione della libertà di espressione. Ma prima ancora si potrebbe addurre, quale principale fattore esplicativo,

[163] Art. 29 Data Protection Working Party, *Opinion 5/2009 on online social networking*, 12-6-2009, 11, ove si afferma che un siffatto obbligo sarebbe in linea con la disciplina in materia di protezione dei dati.

[164] Circa la quale v. G. Resta, voce *Doni non patrimoniali*, cit., 527.

[165] A. Lauber-Rönsberg, *Rechtsdurchsetzung bei Persönlichkeitsrechtsverletzungen im Internet Verantwortlichkeit von Intermediären und Nutzern in Meinungsforen und Personenbewertungsportalen*, cit., 13 ss.

[166] Cfr. *Supra*, par. 4.2.

la particolare capacità di incidenza sulle dinamiche parlamentari dell'industria dell'intrattenimento, la quale è riuscita sin dall'epoca degli accordi *TRIPS* a persuadere il legislatore della necessità di introdurre strumenti di tutela della proprietà intellettuale — tra i quali rientra anche l'ordine di *disclosure* — particolarmente incisivi e efficaci [167]. Strumenti, questi, non a caso assenti nel campo dei diritti della personalità, dove il pubblico dei controinteressati è molto ampio ed eterogeneo, dunque difficile da coordinare, e dove i soggetti maggiormente preoccupati di orientare a proprio vantaggio il processo legislativo sono le imprese editoriali e di comunicazione di massa [168]. Tali fattori aiutano forse a comprendere la suddetta disparità di regime; non già, però, a giustificarla.

Abstract

This paper provides a comparative analysis of the most relevant issues related to online anonymity. It deals with three main question: a) *is anonymity allowed?;* b) *is the online provider liable for torts committed by anonymous defendants?;* c) *what are the legal instruments available to 'discover' the identity of an anonymous defendant?It concludes by criticizing the current overprotection of intellectual property rights vis-à-vis privacy and personality rights.*

[167] In tema v. ad es. J. Lapousterle, *L'influence des groupes de pression sur l'élaboration des normes. Illustration à partir du droit de la propriété littéraire et artistique*, Paris, 2009, *passim*.

[168] In tema cfr. le considerazioni di V. Zeno-Zencovich, *Freedom of Expression. A Critical and Comparative Analysis*, cit., 17 ss.