
L'anonimato in rete: garanzie, responsabilità, tutele

Giorgio Resta*

SOMMARIO: 1. Premessa. – 2. L'anonimato online: le regole e i modelli. – 2.1. Anonimato come strumento di esercizio della libertà d'espressione. – 2.2. Anonimato come proiezione del diritto alla protezione dei dati personali. – 2.3. Identificabilità imposta per contratto o per legge: le *real name policies*. – 3. Anonimato e responsabilità degli intermediari. – 4. La responsabilità dell'utente anonimo e il problema dell'identificazione in sede processuale. – 5. L'esperienza statunitense: dalle azioni proposte in forma anonima al *John Doe subpoena*. – 6. Prospettive europee. – 7. Itinerari di riforma.

1. Premessa.

Una riflessione sull'anonimato in rete è divenuta ormai ineludibile per effetto del dilagare di ciò che usa definire il “discorso dell'odio”, non certo creato, ma senza dubbio favorito dalla diffusione dei social network e dalla “twitterizzazione” della politica. I commenti gratuitamente offensivi, le risposte aggressive a normali atti di manifestazione del pensiero, i post velenosi e carichi di odio razziale o ideologico, i giudizi sprezzanti su professionisti, insegnanti e imprenditori veicolati dalle piattaforme di *rating* personale, sono altrettanti esempi del crescente degrado del discorso pubblico, agevolato dal meccanismo dell'anonimato¹.

L'anonimato in rete è lecito, e se sì perché garantirlo? Quale il regime degli illeciti commessi in forma anonima? E quali in particolare le tutele civili delle vittime? A queste semplici domande ci si propone di rispondere nel presente scritto, che intende accostarsi ai problemi etici, giuridici e politici dell'anonimato in rete muovendo dalla prospettiva del giuscomparatista.

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

Il primo interrogativo, tra quelli appena formulati, potrebbe essere inteso come una domanda retorica, ma tale non è. È sufficiente volgere un rapido sguardo al di fuori dei confini nazionali per constatare come l'attitudine

* Il presente contributo riprende, integrandole e aggiornandole, alcune considerazioni originariamente svolte in *Dir. Inf.*, 2014, 171-205.

¹ BOHLEN, *Der zivilrechtliche Auskunftsanspruch bei der Bekämpfung von Hass im Internet*, in *NJW*, 2020, p. 1999.

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 giuridici 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 contrattuali². Ciò non toglie che, a uno sguardo di sintesi, può ritenersi prevalente su scala comparatistica un primo modello, il quale è imperniato sul riconoscimento della tendenziale liceità dell'anonimato *online*.

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

Questo modello è ritenuto da molti coesistente ai tratti distintivi dello spazio cibernetico, come sin qui conosciuto³. 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 – 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 individuo (nel senso dell'art. 2 Cost.), ponendolo al riparo dai rischi di intimidazione e stigmatizzazione propri del mondo reale⁴. 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. 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". 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 internauta⁵.

² L'analisi più attenta condotta in materia è quella proposta da 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 Galgano, XLVIII, Padova, 2008.

³ In questa prospettiva si confrontino le puntuali argomentazioni di RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, pp. 389 ss.; MANETTI, *Libertà di pensiero e anonimato in rete*, in *Dir. inf.*, 2014, pp. 139 ss.

⁴ RODOTÀ, *Il diritto di avere diritti*, cit., p. 392; BARNETT LIDSKY - COTTER, *Authorship, Audiences, and Anonymous Speech*, 82 *Notre Dame L. Rev.* 1537, 1574 (2007).

⁵ POUSSON, *L'identité informatisée*, in POUSSON-PETIT, a cura di, *L'identité de la personne humaine. Étude de droit français et de droit comparé*, Bruxelles, 2002, 371; SMITH EKSTRAND, *The Many*

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 democrazia, tale strumento avrebbe un effetto ampiamente positivo sul piano della partecipazione alla vita politica e, dunque, della redistribuzione del potere sociale⁶.

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", ma uno sguardo al dibattito contemporaneo evidenzia immediatamente lo straordinario rilievo ad esso attribuito in quel contesto culturale. Benché non manchino argomentazioni di segno opposto, l'assunto per cui l'anonimato rappresenta, oltre che un valore, un vero e proprio diritto fondamentale tutelato in capo agli utenti della rete sembra raccogliere un consenso diffuso. 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 legge⁷. 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. 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-

Masks of Anon: Anonymity as Cultural Practice and Reflections in Case Law, in 18 *J. Tech. L. & Pol'y* 1 (2013).

⁶ CUNIBERTI, *Democrazie, dissenso politico e tutela dell'anonimato*, in *Dir. Inf.*, 2014, pp. 111 ss.

⁷ FROMKIN, *The Uneasy Case for National ID Cards*, in CHANDER - GELMAN - RADIN, *Securing Privacy in the Internet Age*, Stanford, 2008, 295 ss.; LYON, *Identifying Citizens. ID Cards as Surveillance*, Cambridge, 2009; NEYRAND, *Identification sociale, personnalisation et processus identitaires*, in POUSSON - PETIT (a cura di), *L'identité de la personne humaine. Étude de droit français et de droit comparé*, Bruxelles, 2002, pp. 93 ss., p. 98.

cazione. Tuttavia il rifiuto della “carta d’identità” mantiene, almeno sul piano simbolico, un significato non trascurabile.

La seconda premessa è costituita dal rilievo assunto dalla libertà d’espressione nell’assiologia costituzionale nordamericana⁸. Questo è il profilo che più distintamente emerge a 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 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*, 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 costituzionale⁹.

I due fattori appena ricordati contribuiscono a spiegare la notevole fortuna arrisa all’ideologia dell’anonimato *online* anche al di fuori del suo terreno d’elezione, ossia il mondo degli *hackers* e l’articolata galassia dei movimenti. 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 *online*. Basti ricordare, al riguardo, che in *White v. Baker*¹⁰, 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*¹¹, era stata dichiarata costituzionalmente illegittima una legge della Georgia che proibiva l’uso di nomi falsi in Internet. Inoltre il riferimento al Primo Emendamento svolge un ruolo

⁸ Cfr. tra i molti CARRINGTON, *Our Imperial First Amendment*, 34 *U. Rich. L. Rev.* 1167 (2001); SEDLER, *An Essay on Freedom of Speech: The United States Versus the Rest of the World*, 2006 *Mich. St. L. Rev.* 377 (2006).

⁹ FROMKIN, *Anonymity and the Law in the United States*, in KERR - STEEVES - LUCOCK, a cura di, *Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society*, Oxford, 2009, p. 441; KAMINSKY, *Real Masks and Real Name Policies*, in *Fordham Int. Prop. Media Ent. L. J.* 815, 833 (2013).

¹⁰ *White v. Baker*, 696 F. Supp. 2d 1289 (N.D. Ga. 2010).

¹¹ *ACLU of Ga. v. Miller*, 977 F. Supp. 1228 (N.D. Ga. 1997).

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.

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 protezione dei dati personali (cfr. art. 3 del d.lgs. 196/2003, Codice in materia di protezione dei dati personali, che assegna un valore ordinante al c.d. principio di necessità; ed ora art. 5, c. 1, lett. c del Regolamento UE 2016/679 con riferimento al principio di minimizzazione dei dati). Il trattamento di dati anonimi è quindi elevato a regola di *default*, dalla quale sarebbe possibile discostarsi soltanto quando le particolari finalità del trattamento, nelle singole ipotesi, lo giustificano. 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. Tale prerogativa, già contemplata in un *Considerando* della direttiva 2000/31/CE, è espressamente garantita dalla legge tedesca sui media telematici, la quale rappresenta al riguardo un modello paradigmatico¹². 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, ogniqualevolta ciò risulti tecnicamente possibile e ragionevole. L'utente del servizio ha diritto di essere informato di tale possibilità"¹³. 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 (ed essa non a caso è stata al

¹² SPINDLER, *Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung*, in *Verhandlungen des 69. Deutschen Juristentages*, Band I, München, 2012, Gutachten F, 1 ss., 84; HÄRTING, *Anonymität und Pseudonymität im Datenschutzrecht*, in *NJW*, 2013, p. 2065, p. 2067.

¹³ § 13, c. 6, *Telemediengesetz* del 26. febbraio 2007, come modificato dall'art. 1 della legge 31 maggio 2010: "Der Diensteanbieter 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".

centro di molteplici controversie giurisprudenziali, in special modo originate dalla regola di uso nominativo del *social network* imposta da Facebook)¹⁴. 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.

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

Anche all'interno degli ordinamenti che stabiliscono in linea di principio la liceità del ricorso a tecniche di anonimato (o addirittura ne sollecitano l'adozione), vi possono essere regole di dettaglio che derogano a tale scelta in casi particolari. 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"¹⁵. 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 pubblicazione di commenti anonimi sul proprio sito internet, ma a condizione di registrarsi presso il sito attraverso il proprio indirizzo di posta elettronica. 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 nominativa¹⁶. 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*.

¹⁴ VG Schleswig, 14-2-2013, Az. 8 B 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.jurpc.de/jurpc/show?id=20130043>; OVG Schleswig-Holstein, 22-4-2013, Az. 4 MB 10/13 in *N/W*, 2013, 1977.

¹⁵ HARTZOG-STUTZMAN, *The Case for Online Obscurity*, 101 *California L. Rev.* 1, 11 (2013).

¹⁶ KAMINSKI, *Reading Over Your Shoulder: Social Readers and Privacy Law*, 2 *Wake Forest L. Rev.* 13, 14 (2012).

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 utenza¹⁷. 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*¹⁸. Tuttavia, a 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. 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.

Ovviamente ciò non significa che in sistemi di democrazia liberale modelli di disciplina incentrati sull'obbligo di registrazione non siano ammissibili (ed è quanto si dirà a proposito del dibattito oggi in atto in Europa, v. *infra* par. 7). Di certo, però, ove non siano presenti garanzie adeguate in termini di *due process* e indipendenza del potere giudiziario, il sistema in oggetto rischia di risultare in un potente mezzo di controllo e repressione del dissenso politico¹⁹.

¹⁷ LEITNER, *To Post Or Not to Post: Korean Criminal Sanctions for Online Expression*, 25 *Temp. Int'l & Comp. L.J.* 43, 61-64 (2011); FISH, *Is Internet Censorship Compatible with Democracy?: Legal Restrictions of Online Speech in South Korea*, 10 *Asia-Pacific J. Hum. Rts & L.*, 43 (2009).

¹⁸ Per approfondimenti v. HU, *Real Name Systems in Chinese Cyberspace. Authentication, Privacy, and State Capacity*, in 4 *Peking U.J. Legal Stud.* 207 (2013).

¹⁹ PIERANNI, *Red Mirror. Il nostro futuro si scrive in Cina*, Roma-Bari, 2020, *passim*.

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. 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 ideologico²⁰. 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 minoranze²¹. Il caso dei *tweet* antisemiti, portato all'attenzione del *Tribunal de Grande Instance* di Parigi, ne costituisce una nitida dimostrazione²².

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, 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*. La Sect. 512 DMCA esonera da responsabilità gli intermediari che realizzano attività di *storage* dei materiali coperti da

²⁰ KEATS CITRON, *Cyber Civil Rights*, 89 *B.U. L. Rev.* 61, 64 (2009); CHOI, *The Anonymous Internet*, 72 *Maryland L. Rev.* 501 (2013).

²¹ KEATS CITRON, *Cyber Civil Rights*, cit., pp. 68-81.

²² TGI Paris, 241-1-2013, *UEJF et autres c. Twitter Inc. et Twitter France*, in *Dalloz*, 2013, p. 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. FRANCILLON, *Messages racistes ou antisémites postés sur le réseau social Twitter*, in *Rev. sc. crim.*, 2013, p. 566.

diritto d'autore, ogniqualevolta costoro abbiano un ruolo meramente passivo e si conformino alla procedura di "notifica e rimozione" prevista dalla legge. A sua volta, la Sect. 230 CDA 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". Tale disposizione è stata interpretata dalla giurisprudenza prevalente nel senso di escludere che un *provider* 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.

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)²³.

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 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*²⁴. 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. 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 commodum eius et incommoda*. Non bisogna tuttavia dimenticare che le pronunzie della Corte sono strettamente legate all'utilizzazione del criterio del margine di ap-

²³ Per una nitida descrizione dell'impianto della direttiva e una comparazione con l'approccio statunitense v. RICCIO, *La responsabilità degli internet providers nel d.lgs. n. 70/2003*, in *Danno e resp.*, 2003, pp. 1157 ss.

²⁴ Corte Europea Dir. Uomo, Grande Camera, 16 giugno 2015, App. n. 64569/09, *Delfi AS c. Estonia*; e già Corte Europea Dir. Uomo, 10 ottobre 2013, App. n. 64569/09, *Delfi AS c. Estonia*, in *Dir. inf.*, n. 1/2014, con nota di 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*.

prezzamento nazionale, sì che non può stupire che nel diverso e più recente caso *Pihl v. Sweden* essa abbia raggiunto una conclusione sostanzialmente opposta, ritenendo che il diniego di tutela rispetto a una diffamazione anonima non integri la violazione dell'art. 8 CEDU²⁵.

Alla soluzione più rigorosa in punto di responsabilità 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 logica economica dei costi e dei benefici²⁶. 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. 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'anonimato²⁷.

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". O si consideri il caso, ancor più rilevante nella pratica, dei siti che propongono servizi di *rating* personale, altrimenti definiti di *social scoring*, come "votail-prof.it", "ratemyprofessors.com" (valutazione dei docenti) o "arzt.weisse-liste.de" (valutazione dei medici), o di *rating* imprenditoriale, come "holidaycheck.com". 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 degli utenti. Saremmo al cospetto di una situazione di questo tipo, ad esempio, ogniqualevolta 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); 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 significato²⁸. In

²⁵ Corte Europea Dir. Uomo, 9 marzo 2017, App. n. 74742/14, *Pihl v. Sweden*.

²⁶ Tale obiezione è riproposta, da ultimo, da VIGEVANI, *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano*, in *Dir. inf.*, pp. 207 ss.

²⁷ In questo senso cfr. OLG Hamburg, 28 marzo 2012, in *ZUM-RD*, 2013, p. 536.

²⁸ 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

tali casi è difficile affermare che il *provider* non abbia svolto – mutuando il lessico e le categorie adottate dalla Corte di giustizia UE²⁹ – 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’intermediario³⁰.

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 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 stesso³¹. 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 giuridica³². 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, oppure perché i dati anagrafici comunicati dall’utente al *provider* potrebbero rivelarsi falsi.

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.

²⁹ 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 NORDEMANN, *Liability of Social Networks for IP Infringements (Latest News): The EU Law Regime after l’Oréal/eBay*; CZYCHOWSKI - NORDEMANN, *Grenzenloses Internet – entgrenzte Haftung. Leitlinien für ein Haftungsmodell der Vermittler?*, in *GRUR-Beilage*, 2014, pp. 3 ss., p. 5.

³⁰ In questo senso SPINDLER, *Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung*, cit., pp. 61 ss.

³¹ SPINDLER, *Rechtsdurchsetzung von Persönlichkeitsrechten. Bussgelder gegen Provider als Enforcement?*, in *GRUR*, 2018, pp. 365 ss.

³² DI CIOMMO, voce *Internet I) Responsabilità civile*, in *Enc. Giur., Agg.*, XIX, Roma, 2001, 5.

Ma anche prescindendo dai problemi di ordine fattuale, vi sono diversi ostacoli giuridici che si frappongono al “superamento del velo”. La protezione 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 e alla protezione dei dati personali³³. 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 un’ampia riflessione, tanto nel contesto dei rapporti *offline* quanto nella sfera telematica.

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

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. 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’attore³⁴. 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. 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.

A questo punto due sviluppi paralleli intervennero a modificare il quadro di riferimento. Da un lato si diffuse il ricorso ad azioni proposte in forma anonima (ossia da un *plaintiff* identificato solo attraverso pseudonimi) nel

³³ LIDSKY, *Anonymity in Cyberspace: What Can We Learn from John Doe?*, cit., pp. 1376 ss.; MANETTI, *Libertà di pensiero e anonimato in rete*, in *Dir. inf.*, 2014, pp. 139 ss.; VIGEVANI, *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano*, ivi, pp. 207 ss.

³⁴ RICE, *Meet John Doe: It Is Time for Federal Civil Procedure to Recognize John Doe Parties*, 57 *Un. Pittsburgh L. Rev.* 883, 890-892 (1996).

quadro delle controversie in materia di *constitutional privacy*³⁵. 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 prescrizione³⁶. 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 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.

Con l'avvento di Internet i casi di *anonymous litigation* sono aumentati in misura esponenziale. 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. 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 duces tecum*). Nell'ipotesi degli illeciti commessi *online*, 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. 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

³⁵ 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 temperare 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 RESTA, *Privacy e processo civile: il problema della litigation "anonima"*, in *Dir. inf.*, 2005, p. 681, pp. 696 ss.).

³⁶ RICE, *Meet John Doe: It Is Time for Federal Civil Procedure to Recognize John Doe Parties*, cit., pp. 895 ss.

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. Tuttavia non vi sono indicazioni normative sufficientemente puntuali 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 avrebbe l'effetto opposto di paralizzare l'accesso alla giustizia e la tutela delle vittime di messaggi diffamatori o discriminatori³⁷.

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"³⁸. 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). In una seconda fase, inaugurata dalla decisione *Dendrite International v. Doe*³⁹, 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*. Due sono gli elementi fondamentali del *test* più frequentemente adottato dalle corti. 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.

³⁷ Su questo tema si è stratificata un'ampia letteratura. Tra i molti scritti v. GLEICHER, *John Doe Subpoenas: Towards a Consistent Legal Standard*, 118 *Yale L.J.* 320, 360–61 (2008); 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); LIDSKY, *Anonymity in Cyberspace: What Can We Learn from John Doe?*, 50 *B.C. L. Rev.* 1373 (2009); SOBEL, *The Process That "John Doe" Is Due: Addressing the Legal Challenge to Internet Anonymity*, 5 *Va. J.L. & Tech* 3 (2000); EKSTRAND, *Unmasking Jane and John Doe: Online Anonymity and the First Amendment*, 8 *Comm. L. & Pol'y* 405 (2003).

³⁸ MOORE, *The Challenge of Internet Anonymity: Protecting John Doe on the Internet*, 26 *J. Marshall J. Computer & Info. L.* 469, 472 (2009).

³⁹ *Dendrite Int'l, Inc. v. Doe, No. 3*, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001).

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. In secondo luogo, grava sull'attore l'onere di fornire 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. 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* sino alla prova dell'attitudine a resistere ad una *motion to dismiss*⁴⁰, o infine ad una *motion for summary judgment*⁴¹. Non potendo qui entrare nei dettagli, sarà sufficiente limitarsi a rilevare due dati. Il primo è che il modello di disciplina adottato nel sistema statunitense implica, rispetto alla politica delle *real name policies* discusse in precedenza, 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. 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*)⁴², ma dà vita ad un evidente problema di ragionevolezza della disciplina, alla luce del diverso valore rispettivamente assunto dalla tutela della dignità umana e della proprietà nel quadro dell'assiologia costituzionale.

⁴⁰ *Columbia Insurance Co. v. Seescandy.com*, 185 F.R.D. 573 (N.D. Cal. 1999).

⁴¹ *Doe v. Cahill*, 884 A.2d 451 (Del. 2005).

⁴² 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, LLC*, No. 10-35308, 2011WL 2565618 (9th Cir. June 29, 2011).

6. 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 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)⁴³, 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 una proibizione generalizzata del ricorso all'anonimato o a pseudonimi nelle comunicazioni in rete; 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; 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*. 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 la tutela delle posizioni proprietarie e quella relativa a diritti della personalità. 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 particolarmente incisivo e penetrante⁴⁴. 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 *online* in forma anonima⁴⁵. Nel nostro ordinamento tale strumento è ora co-

⁴³ LAUBER - RÖNSBERG, *Rechtsdurchsetzung bei Persönlichkeitsrechtsverletzungen im Internet Verantwortlichkeit von Intermediären und Nutzern in Meinungsforen und Personenbewertungsportalen*, in *Multimedia und Recht*, 2014, 10, p. 13.

⁴⁴ Cfr. WALTER - GOEBEL, *Enforcement Directive*, in WALTER - VON LEWINSKY, a cura di, *European Copyright Law. A Commentary*, Oxford, 2010, pp. 1193 ss.; GIUSSANI, *La disciplina comunitaria della tutela giurisdizionale della proprietà intellettuale*, in UBERTAZZI (a cura di), *La proprietà intellettuale*, in *Trattato di diritto privato dell'Unione Europea*, diretto da AJANI e BENACCHIO, Torino, 2011, pp. 459 ss.; NIVARRA, a cura di, *L'enforcement dei diritti di proprietà intellettuale: profili sostanziali e processuali*, Milano, 2005.

⁴⁵ COMOGLIO, *Istruzione e discovery nei giudizi in materia di proprietà industriale*, in AIDA, 2000, 270 ss.; GIUSSANI, *La disciplina comunitaria della tutela giurisdizionale della proprietà intellettuale*, cit., 464.

dificato 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). 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 incisivo⁴⁶.

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. L'art. 15 del Regolamento (UE) 2016/679 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. È ben vero che nella normativa in materia di protezione dei dati è prevista una causa di esclusione del consenso per l'ipotesi del trattamento

⁴⁶ 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 *Dir. inf.*, 2007, p. 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 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. DE CATA, *Il caso “Peppermint”. Ulteriori riflessioni anche alla luce del caso “Promusicae”*, in nota alle pronunzie citate, in *Riv. dir. ind.*, 2008, II, pp. 404 ss., spec. p. 414-425; GIUSSANI, *La disciplina comunitaria della tutela giurisdizionale della proprietà intellettuale*, cit., p. 464; per riferimenti dottrinali e giurisprudenziali circa le misure previste dall'art. 210 c.p.c. v. CARNEVALE, sub art. 210, in COMOGGIO - CONSOLO - SASSANI - VACCARELLA, *Commentario del codice di procedura civile*, III, 1, Torino, 2012, pp. 667 ss.

per “finalità di giustizia”. Tuttavia, essa non appare di per sé idonea a fondare la legittimità di una richiesta di ostensione di dati di terzi in assenza di una base normativa primaria. 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: 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. 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).

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 – 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 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 personali⁴⁷. Dialogando apertamente con la Corte di Giustizia, il *Bundesgerichtshof* tedesco ha accolto una lettura estensiva del § 101 *UrhG*, confermando la legittimità dell’ordine di esibizione anche nelle ipotesi di violazioni non condotte “su scala commerciale”⁴⁸. 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

⁴⁷ 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 par. 55-61), in *Dir. inf.*, 2012, p. 297, con nota di 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, p. 571, con nota di COLANGELO, *Internet e sistemi di filtraggio tra enforcement del diritto d’autore e tutela dei diritti fondamentali: un commento ai casi «Scarlet» e «Netlog»*.

⁴⁸ BGH, 19-4-2012, in *NJW* 2012, 2958, con nota di LADEUR; BRÜGGEMANN, *Urheberrechtsdurchsetzung im Internet. Ausgewählte Probleme des Drittauskunftsanspruchs nach § URHG § 101 UrhG*, in *Multimedia und Recht*, 2013, pp. 278 ss.

risoluta che “in uno stato di diritto neanche Internet può dar vita a spazi privi di regole”⁴⁹.

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.

Di ciò l'esperienza tedesca offre, ancora, 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 conflitto⁵⁰. 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. Tra i casi più significativi merita di essere ricordatao 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 professionalità⁵¹. 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

⁴⁹ BGH, 19-4-2012, cit., 2962: “in einem Rechtsstaat darf auch das Internet keinen rechts-freien Raum bilden”.

⁵⁰ SPINDLER, *Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung*, cit., p. 58.

⁵¹ LG München, 3 luglio 2013, in *ZUM*, 2013, p. 979.

*Telemediengesetz*⁵². Altrettanto rilevante è la pronunzia dell'*Oberlandesgericht* di Hamm del 3 agosto 2011⁵³. 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 *Grundgesetz*, attribuendo peraltro notevole rilevanza alla natura di "giudizi di valore" (e non di "statuizioni fattuali") dei messaggi incriminati⁵⁴.

7. Itinerari di riforma.

Alla luce delle difficoltà sopra ricordate, si è aperto negli ultimi anni un ampio dibattito sia in Germania, sia in Francia, Italia, ed Austria, su come assicurare una tutela effettiva dei diritti della persona in Internet, in particolare rispetto agli atti lesivi in forma anonima, senza al contempo intaccare il fondamentale principio della libertà di espressione. Esponenti politici di primo piano, come il presidente del Bundestag Wolfgang Schäuble⁵⁵, hanno apertamente preso posizione per l'introduzione di regimi incentrati sul c.d. *Klarnamspflicht*, ossia l'obbligo di registrazione degli utenti al fine di responsabilizzare l'esercizio

⁵² LG München, 3 luglio 2013, cit., 980. Per un'attenta discussione di questi argomenti v. LAUBER-RÖNSBERG, *Rechtsdurchsetzung bei Persönlichkeitsrechtsverletzungen im Internet Verantwortlichkeit von Intermediären und Nutzern in Meinungsforen und Personenbewertungsportalen*, cit., p. 13-14.

⁵³ OLG Hamm, 3 agosto 2011, in *ZUM-RD*, 2011, p. 684.

⁵⁴ 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 auch für denjenigen besteht, der sich als Patient aus 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".

⁵⁵ <https://www.tagesschau.de/inland/schauble-klarnamenpflicht-soziale-netzwerke-101.html>.

della libertà di manifestazione del pensiero, e indirettamente di assicurare alla vittima di illeciti la facoltà di agire in giudizio ottenendo l'ostensione dei dati identificativi dell'autore dell'illecito⁵⁶.

Queste proposte si sono tradotte in progetti di legge e in alcuni ordinamenti nell'adozione di specifiche normative preordinate al rafforzamento delle misure di protezione dei singoli.

Il primo intervento degno di nota è quello compiuto in Germania. La legge generale sulla tutela dei diritti nei social networks del 1 settembre 2017 (*Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken*), ha introdotto un'apposita modifica dell'art. 14 della legge sui media telematici, al fine di garantire il diritto dei cittadini di ottenere da parte del fornitore di servizi della società dell'informazione l'ostensione di informazioni relative ai propri utenti (dati di connessione e dati di utilizzo), nei limiti in cui ciò sia indispensabile per l'esercizio di azioni giudiziarie derivanti dalla violazione di diritti assoluti a seguito della pubblicazione di contenuti illeciti e suscettibili di sanzione penale ai sensi dell'art. 1, 3° co., della legge medesima⁵⁷. Tra questi rilevano essenzialmente gli illeciti di diffamazione e di divulgazione di immagini attinenti alla sfera personalissima (§ 14 III-*bis* V TMG). Si deve notare che è prevista a tal scopo una riserva di giurisdizione: l'obbligo di *disclosure* sussiste soltanto qualora l'attore abbia previamente ottenuto un provvedimento autorizzatorio da parte del tribunale competente.

Simbolicamente la modifica normativa è importante, ma sul piano operativo la soluzione adottata si è rilevata poco efficace e di fatto non risolutiva⁵⁸, se non altro perché in assenza di un obbligo di registrazione nominativa degli utenti, i *provider* non dispongono sempre delle informazioni necessarie, né sono incentivati ad acquisirle⁵⁹. In secondo luogo, sul piano processuale si rivela necessario una duplice iniziativa dell'attore: quella volta ad ottenere l'autorizzazione giudiziale preliminare, e quella mirata all'ottenimento del provvedimento ingiuntivo nei confronti del fornitore del servizio, il che è ovviamente un fattore dissuasivo alquanto importante.

⁵⁶ Nel nostro paese può ricordarsi il dibattito originato dalla proposta del deputato di Italia Viva Luigi Marattin: https://www.ilsole24ore.com/art/sui-social-network-solo-documento-d-identita-proposta-italia-viva-pro-e-contro-ACKsYNv?refresh_ce=1.

⁵⁷ Per un'attenta analisi v. SPINDLER, *Rechtsdurchsetzung von Persönlichkeitsrechten. Bussgelder gegen Provider als Enforcement?*, cit., p. 372.

⁵⁸ BOHLEN, *Der zivilrechtliche Auskunftsanspruch bei der Bekämpfung von Hass im Internet*, in NJW, 2020, p. 1999; PILLE, *Der Grundsatz der Eigenverantwortlichkeit im Internet*, in NJW, 2018, p. 3545.

⁵⁹ SPINDLER, *Rechtsdurchsetzung von Persönlichkeitsrechten. Bussgelder gegen Provider als Enforcement?*, cit., p. 372; PILLE, *Der Grundsatz der Eigenverantwortlichkeit im Internet*, cit., p. 3546.

Anche alla luce di queste considerazioni, appare preferibile la soluzione proposta dal governo austriaco, che ha presentato di recente un organico disegno di riforma della disciplina degli illeciti anonimi in rete⁶⁰.

Esso è incentrato su tre principi fondamentali. Il primo è quello dell'obbligo di registrazione nominativa degli utenti gravante sui fornitori di servizi della società dell'informazione sopra una certa soglia dimensionale (più di 100.000 utenti registrati o più di 500.000 Euro di fatturato annuo), i quali mettano a disposizione del pubblico "forum" aperti per lo scambio di comunicazioni, valutazioni e altre forme di manifestazione del pensiero (§§ 2-3). Il secondo è quello della possibilità di uso anonimo, o meglio tramite pseudonimi, dei servizi in oggetto: l'obbligo di registrazione, che è condizione indispensabile per l'utilizzo dei forum, deve essere adempiuto fornendo prova delle generalità e dei dati anagrafici effettivi della persona; è tuttavia fatta salva la possibilità di adottare uno "username" fittizio per l'attività in rete (§ 3, IV). Il terzo principio è quello dell'obbligo di comunicazione dei dati identificativi dell'autore di un post illecito gravante in capo al fornitore del servizio e a beneficio di qualsiasi terzo il quale dimostri che l'accesso a tali informazioni è indispensabile per l'esercizio di un'azione in giudizio finalizzata alla tutela civile dell'onore o di altri interessi della persona destinatari di protezione penale (§ 4).

Rispetto alla normativa tedesca, si supera il principio della riserva di giurisdizione e si prevede uno specifico obbligo di registrazione nominativa degli utenti, il che darebbe certamente vita ad un regime maggiormente garantistico sul piano della tutela della persona, ma alquanto invasivo sul piano della libertà di impresa e potenzialmente dissuasivo su quello della libertà di manifestazione del pensiero. Di qui le molte, prevedibili, voci critiche espresse nei confronti del disegno di legge⁶¹.

Come si vede, il bilanciamento non è semplice ed è suscettibile di trovare soluzioni diverse a seconda delle preferenze giuspolitiche manifestate da ciascun ordinamento. Quello che si può auspicare è che, indipendentemente dal merito delle soluzioni, ci si persuada della necessità di affrontare apertamente il problema in oggetto, superando la situazione attuale di anarchia espressiva e di elevata lacunosità nel sistema di protezione della persona umana rispetto alle varie, subdole, forme di "odio online".

⁶⁰ *Entwurf: Bundesgesetz, mit dem ein Bundesgesetz über Sorgfalt und Verantwortung im Netz erlassen und das KommAustria-Gesetz geändert wird* (2019), accessibile all'indirizzo https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Begut&Dokumentnummer=BEGUT_COO_2026_100_2_1631073.

⁶¹ Ad es. v. <https://apps.derstandard.at/privacywall/story/2000103738487/warumnationalratsabgeordnete-der-digitalen-ausweispflicht-nicht-zustimmen-duerften>.