

MICHELA MANETTI

LIBERTÀ DI PENSIERO E ANONIMATO IN RETE

SOMMARIO: 1. *Offensive Internet* e diritti dei privati. — 2. Il valore paradigmatico dell'anonimato per la libertà di pensiero. — 3. La funzione informativa della Rete. — 4. L'anonimato come difesa della persona da forme di controllo pervasive. — 5. Alcune provvisorie conclusioni.

1. *OFFENSIVE INTERNET* E DIRITTI DEI PRIVATI.

L'avvento di un nuovo mezzo di comunicazione riapre, inevitabilmente, il discorso sulla libertà di manifestazione del pensiero e sul suo valore nella costellazione dei principi costituzionali. Nell'ambito del dibattito sulle virtualità della Rete il tema dell'anonimato appare da questo punto di vista particolarmente fecondo, in quanto rivela una nuova ed imprevedibile interazione tra lo sviluppo tecnologico e le categorie giuridico-culturali fin qui elaborate.

Sino a qualche tempo fa l'interazione è apparsa, a dire il vero, impossibile, in ossequio ad alcune convinzioni dilagate assieme all'uso della Rete: fra queste, il mito di una natura intangibile del mezzo, nato per l'anonimato e impossibile da correggere; la difficoltà di concepire una disciplina applicabile ai più diversi punti del globo; non ultima, l'imperante esaltazione della libertà della Rete, che pretendendo dai *Provider* assoluta neutralità si è saldata incrollabilmente con l'interesse di questi ultimi a non essere ritenuti responsabili per l'illiceità dei messaggi trasmessi.

Queste convinzioni, nella loro assolutezza, si sono rivelate col tempo semplici leggende. Lawrence Lessig ha dimostrato come il codice o l'architettura che si limita ad individuare il computer dal quale proviene il messaggio non è immutabile, e può ben essere

* 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.

arricchito da meccanismi che consentano l'identificazione del parlante ¹.

È stata altresì sperimentata la possibilità di impedire la ricezione, sul territorio nazionale, di messaggi vietati, sia pure in modi e termini non assoluti.

Quanto all'esaltazione della libertà della Rete, della quale l'anonimato è strumento, essa è stata massicciamente messa in discussione tanto dalle forme di profilazione messe in atto dai *Provider* a scopi commerciali, quanto dai controlli istituiti in modo palese o occulto dai governi degli stessi Paesi occidentali (non solo per sventare le minacce terroristiche, ma anche per spiare le mosse dei loro alleati).

A seguito di queste vicende, venute alla luce più o meno imprevedibilmente, siamo oggi in grado di affermare che i poteri pubblici, nella stragrande maggioranza dei casi, sono perfettamente in grado di identificare il responsabile di un messaggio diffuso in Rete, con i propri mezzi o attraverso la collaborazione dei *Provider*; così come questi ultimi sono in grado di verificare i contenuti dei messaggi trasmessi, attraverso la tecnologia chiamata *Deep Packet Inspection*, onde censurare sistematicamente quelli che risultino sgraditi ².

Vi è da chiedersi allora se non sia preferibile un sistema legale e trasparente di identificazione, che consenta di far valere la responsabilità per gli illeciti commessi attraverso l'uso di Internet non a discrezione dei poteri, pubblici o privati, ma a disposizione di tutti coloro che ne hanno diritto. Accanto ai crimini più eclatanti cui l'uso della Rete si presta, ne esistono infatti altri, in particolare la diffamazione, che colpiscono severamente i diritti costituzionali degli individui: il tema dell'*Offensive Internet* è ormai all'ordine del giorno ³.

Bisogna peraltro considerare che se venisse imposta l'identificazione dell'autore del messaggio, l'anonimato sarebbe automaticamente interdetto — salva l'introduzione di forme di responsabilità concorrenti o sussidiarie analoghe a quelle attualmente vigenti per i giornali e per gli stampati —. Si tratta di una

¹ L. LESSIG, *Code and Other Laws of Cyberspace*, New York 1999; Id., *Code Version 2.0*, New York 2006.

² Cfr. AMERICAN CIVIL LIBERTIES UNION, *Network Neutrality* 101 (October 2010), 6, in www.aclu.org. Tale potere censorio è riconosciuto ai Provider dalla legge americana tramite la c.d. *Good Samaritan Provision*, mentre altrove si basa sulle condizioni generali dei contratti sottoscritti dagli utenti, che consentono alle compagnie di bloccare o cancellare messaggi da esse ritenuti in buona fede illeciti o dannosi.

³ Cfr. S. LEVMORE, M. NUSSBAUM, *The Offensive Internet. Speech, Privacy and Reputation*, Harvard University Press 2011. Nella dottrina italiana questa preoccupazione è più radicata: v. al riguardo A. PAPA, *Espressione e diffusione del pensiero in Internet*, Torino 2009; M. BETZU, *Regolare Internet. La libertà di informazione e di comunicazione nell'era digitale*, Torino 2012.

prospettiva oggi non inverosimile, dal punto di vista tecnologico, fermo restando il rischio di imporre oneri eccessivi ai *Provider*, che appaiono allo stato gli unici garanti del funzionamento e dello sviluppo della Rete, con evidenti riflessi sull'interesse della collettività a fruirne.

Esiste tuttavia anche un rischio di ordine costituzionale, con specifico riguardo all'esercizio della libertà di pensiero. Per capirlo basta rileggere in controluce la sentenza adottata dalla Corte Suprema degli Stati Uniti nel caso *Reno v. ACLU*⁴, che rappresenta la vera *tête de chapitre* di qualsiasi discorso giuridico sulla Rete. Come è noto, la motivazione enfatizza in modo vibrante i pregi di Internet per la democrazia, salutando nella Rete lo strumento finalmente in grado di consentire a qualunque cittadino l'efficace partecipazione al dibattito pubblico⁵. Come pure è noto, la sentenza in esame non censura tuttavia i limiti apposti dalla legge al *political speech*, bensì all'*indecent speech*, quale forma di pensiero ritenuta pregiudizievole per i minori che hanno accesso ad Internet.

Ora, nessuno è così ingenuo da pensare che il discorso politico non possa assumere forme indecenti, specie se ha origine in ambienti popolari: basta ricordare le critiche rivolte alla giurisprudenza costituzionale italiana, là dove ha ritenuto punibile come vilipendio la critica delle istituzioni che sia svolta in forma rozza o volgare⁶.

Colpisce, piuttosto, che la nobile retorica del *marketplace* venga spesa con riguardo ad una forma di pensiero che nella Rete viene normalmente coperta dall'anonimato (e che probabilmente trova nell'anonimato un potente stimolo). Detto in altri termini, colpisce il fatto che la *Supreme Court* statunitense non esiti a scaricare sulla collettività — nel caso *de quo* sui genitori di figli minori — i rischi derivanti da determinati tipi di messaggi, pur di salvaguardare un forum globale destinato al discorso in forma anonima.

La questione non appare del resto limitata al sistema nordamericano, se si considera che una posizione analoga ha assunto il *Bundesgerichtshof* tedesco nel decretare l'immanenza dell'anonimato alla Rete⁷.

Le riflessioni che seguono sono dedicate ad indagare quali

⁴ *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

⁵ "Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer".

⁶ Sul rischio di discriminazione a danno dei contestatori non abbastanza istruiti v. in particolare la critica di A. PIZZORUSSO (*Foro it.*, 1973, I, 966) alla sentenza n. 16 del 1973.

⁷ V. *infra* par. 4.

possano essere le ragioni profonde di tale atteggiamento, ovvero i buoni motivi che il costituzionalismo occidentale può avere per difendere l'anonimato in Rete.

2. IL VALORE PARADIGMATICO DELL'ANONIMATO PER LA LIBERTÀ DI PENSIERO.

La diffusione di messaggi pubblici in forma anonima vanta una lunga tradizione: sin dall'invenzione della stampa, essa è stata usata per sfuggire non solo alla censura vera e propria, ma anche alla disapprovazione o alla semplice curiosità del proprio ambiente o della opinione pubblica in generale.

Come dimostra la storia, la scelta dell'anonimato non è dunque caratteristica dei Paesi autoritari: anzi il diritto di rimanere anonimo (ovvero di usare uno pseudonimo) fa corpo *ab origine* con la libertà di creazione letteraria e artistica, che in determinate situazioni potrebbe essere scoraggiata dalla necessità di rivelare l'identità dell'autore.

In questo senso l'anonimato assume un valore paradigmatico per la libertà di pensiero. Esso è capace di valorizzare il messaggio in quanto tale, mettendo tutti gli interessati su di un piede di eguaglianza e sconfiggendo con ciò i pregiudizi dei destinatari non meno dei condizionamenti che gravano sul parlante.

La forma anonima viene invero utilizzata quando si vuole prendere in considerazione esclusivamente il contenuto del messaggio o dell'opera: tipicamente, in campo accademico, dove essa mira ad assicurare la massima oggettività alla valutazione degli studi e delle ricerche altrui. Il presupposto è che le idee debbano valere per la loro qualità intrinseca, e non per l'autorevolezza di chi le va sostenendo; per converso, che esse debbano essere prese in considerazione anche se chi le avanza non ha titoli da vantare.

L'anonimato amplia quindi l'effettivo ed eguale godimento della libertà di pensiero da parte di tutti, permettendo a chiunque di esporre le proprie convinzioni nel *marketplace of ideas* senza tema di ritorsioni o di esclusioni. Dal punto di vista oggettivo, esso arricchisce il dibattito pubblico e ne esalta la funzione di ricerca della verità, sancendo che non è indispensabile sapere chi ha espresso un'idea per stabilire se questa è giusta, e che anzi è forse preferibile non saperlo. Il fatto di confidare esclusivamente nella capacità di discernimento e nell'autonomia intellettuale degli interessati consente invero di realizzare un "autentico incontro di intelletti"⁸.

⁸ "A true meeting of the minds" nelle parole di A. BRANSCOMB, *Emerging Media Technology and the First Amendment*. Ano-

nymity, *Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, in 104 *Yale L. J.* (1995), 1640.

In una parola, il discorso anonimo rappresenta il trionfo dell'argomentazione come più nobile forma di utilizzo della ragione umana.

Ciò non toglie che storicamente l'anonimato abbia celebrato i suoi fasti molto tempo fa, in un contesto aristocratico, oggi forse rinvenibile in comunità ristrette e selettive come è appunto quella accademica, ma non nel discorso pubblico *at large*, dove semmai si è imposta la cultura dell'esibizione e della notorietà a prescindere dal merito dei messaggi diffusi.

L'avvento di Internet ha cambiato radicalmente questa prospettiva. La Rete infatti è il prodotto di una tecnologia che consente lo scambio di informazioni a prescindere dall'immediata identificazione del parlante, rendendo accessibile una forma di anonimato non assoluta, ma sicuramente molto più efficace di quelle fruibili in precedenza. Queste ultime si sono limitate per secoli alle pasquinate e alle scritte sui muri⁹ (peraltro vietate dalla legge); per i cittadini statunitensi, più fortunati, si spingevano sino alla diffusione di volantini anonimi¹⁰.

Alla nascita della Rete (col progetto ARPANET) la modalità anonima è stata usata — nei tradizionali termini aristocratici — per favorire il confronto libero e senza formalità su questioni di interesse tecnico-scientifico; in seguito essa si è tuttavia rivelata appetibile alla generalità dei cibernauti, sino a creare una nuova sfera pubblica nella quale il nome dell'autore del messaggio non è rilevante.

Oggi, a differenza di ieri, è la democraticità del mezzo a rendere superflua l'identificazione: il dialogo si svolge infatti di regola fra persone qualunque, sparse ai quattro angoli del globo, che non hanno particolari titoli da vantare e cui il semplice fatto di indicare il proprio nome non consentirebbe comunque di uscire dall'*anonimato sostanziale* nel quale vivono le une rispetto alle altre.

Ciò traccia una netta differenza rispetto ai mass-media, grazie ai quali solo pochi eletti possono partecipare al dibattito, e dove il nome conta moltissimo: la firma è invero considerata fondamentale, dai lettori, al fine di attribuire il giusto peso all'opinione espressa. Queste regole non cambiano quando i mass-media utilizzano Internet per la propria diffusione (come avviene con le edizioni on line dei giornali cartacei): la sfera pubblica nella quale il discorso si svolge rimane la stessa.

⁹ Sulla libertà di "scrivere viva o abbasso sul muro" come unica forma di manifestazione del pensiero concessa "al povero cristo" va ricordato V. CRISAFULLI, *Problemmatica della libertà di informazione*, in *Il Politico* 1964.

¹⁰ Nella sentenza *Mc Intyre v. Ohio Elections Commission* 514 U.S. 334 (1995), la Corte suprema USA ha infatti ritenuto che la protezione del I emendamento si estenda alla diffusione di volantini anonimi.

Ma accanto a quella tradizionale — che può concorrere ad ampliare — Internet costituisce, come si è detto, un'altra sfera pubblica, che si può definire virtuale, nella quale l'anonimato rappresenta (non una semplice possibilità, come avviene per gli altri media, ma) la normalità.

E se l'anonimato ha valore paradigmatico o emblematico della libertà di pensiero, la Rete — come mezzo vocato alla forma anonima — assurge a luogo idealtipico del dibattito pubblico, ovvero a sinonimo del perfetto *marketplace*.

Da qui il rinascere, a livello globale, di una utopia — sino a ieri oscurata se non sconfitta dall'egemonia dei mass-media quali grandi intermediari del dibattito pubblico — nella quale alla illimitatezza, economicità e immediatezza del mezzo internettiano si aggiunge la virtù dell'anonimato, che di quel dibattito esalta la libertà e la fruttuosità.

Soprattutto negli Stati Uniti, che hanno tradizionalmente salvaguardato l'anonimato in vari ambiti della vita pubblica, la tematica è considerata assai attuale. In particolare, è attuale oggi, non meno di cent'anni fa, il rischio che determinati messaggi possano essere svalutati in considerazione dell'identità di chi li ha espressi (ad es. un membro di una minoranza razziale, riconoscibile dal cognome), e parallelamente il rischio di auto-censura da parte di chi sa o pensa di appartenere ad una categoria che non viene ascoltata ¹¹.

3. LA FUNZIONE INFORMATIVA DELLA RETE.

Se poi si considera che la diffusione dei messaggi in Internet può svolgere una tipica funzione informativa, si trova un altro motivo per ammettere il ricorso all'anonimato: quest'ultimo appare invero indispensabile per assicurare la protezione della fonte, che è un privilegio generalmente riconosciuto all'attività giornalistica, sia pure con diversa latitudine nei diversi ordinamenti ¹².

È evidente peraltro che nella Rete viene meno, di regola, la distinzione tra la fonte, anonima e non tenuta a rispondere di ciò che ha rivelato, e il giornalista, che è dotato della professionalità indispensabile per vagliare le informazioni e che è deontologicamente tenuto a farlo prima di diffonderle, assumendosene la responsabilità.

Si potrebbe pertanto ritenere che debba venir meno anche il privilegio dell'anonimato: nel comparare l'interesse alla diffu-

¹¹ Come ricorda R. POST, *Constitutional Domains*, Harvard Un. Press 1995, 315 ss., è molto sentito nella dottrina statunitense il rischio che il pervasivo razzismo della società americana sviscoli il contributo delle minoranze al dibattito pubblico.

¹² Cfr. E. BARENDT, *Freedom of Anonymous Expression*, in *Scritti in onore di A. Pace*, II vol., Napoli 2012, 1071 ss.

sione di informazioni pubblicamente rilevanti e il rischio che questa sia fonte di illeciti (dalla diffamazione alla rivelazione di segreti pubblici o privati), quest'ultimo si rivelerebbe talmente alto da imporre senz'altro l'identificazione dell'autore del messaggio.

Resta tuttavia il fatto che senza la protezione dell'anonimato determinate notizie di interesse generale non verrebbero mai conosciute. La disintermediazione caratteristica della Rete (che è l'altra faccia della democratizzazione) non può invero condurre a infirmare la necessità di un controllo capillare sull'esercizio dei poteri pubblici e privati, quale solo la Rete può assicurare, in un mondo dell'informazione dominato a livello globale da ben pochi soggetti.

Grazie alla Rete, questi ultimi possono essere spinti a prendere in considerazione fatti che altrimenti sarebbero destinati a non diventare mai notizie; così come i titolari dei poteri pubblici possono trovarsi a dover modificare la propria agenda. In questo senso Internet funge da sede insostituibile di dibattito su tutte le questioni di interesse pubblico, oltre che da correttivo del sistema tradizionale di informazione.

La questione consiste allora nell'individuare forme di protezione dell'anonimato che siano tali da non privare di tutela i diritti individuali eventualmente lesi.

A tale questione la cultura giuridica statunitense sta da tempo cercando di dare una risposta adeguata, con il concorso dei tribunali e del legislatore. Significativa in tal senso è la vicenda che, attraverso le pronunce di diversi giudici, ha condotto ad elaborare un test destinato a scrutinare l'ammissibilità delle richieste di identificazione dell'autore di una presunta diffamazione avvenuta via Internet.

Si tratta di un test ancora non univoco, che contempla almeno due differenti versioni. Nella prima l'identità dell'autore del messaggio può essere rivelata, ai fini della prosecuzione della causa per diffamazione, soltanto se siano soddisfatte quattro diverse condizioni: in primo luogo, chi si sente diffamato deve contestare il fatto all'autore del messaggio, possibilmente nello stesso "luogo" (newsgroup, blog) dove quest'ultimo è stato pubblicato; in secondo luogo, l'attore deve individuare esattamente, e collegare a ciascun *poster* anonimo, le affermazioni ritenute lesive; in terzo luogo, all'inculpato deve essere dato modo di difendersi dalla richiesta di identificazione; in quarto luogo, l'attore deve dimostrare l'esistenza di un robusto *fumus boni juris* a proprio favore¹³.

La finalità del test in esame consiste nel negare accesso a cause

¹³ In questi termini il test è stato formulato nella sentenza della Corte Suprema

del Delaware *Doe n. 1 v. Cahill* (2005). Il caso riguardava offese, rivolte a personalità

promosse non tanto per ottenere il giusto ristoro da una diffamazione, quanto per individuare e mettere a tacere coloro che diffondono notizie scomode. Nella pratica non è infatti raro che la una volta ottenuta l'identificazione dell'autore del messaggio la causa per diffamazione venga abbandonata: o perché infondata, o perché all'attore interessa più che altro scoraggiare, con la minaccia di una costosa causa, le critiche anonime, se non effettuare ritorsioni più o meno legali nei confronti di coloro che le hanno formulate ¹⁴.

Se infatti chi si sente diffamato lo manifesta con un messaggio pubblicato nella stessa sede di quello originario, l'autore di quest'ultimo può apportare nuove prove a suo favore, dimostrando la verità del fatto; e ancor più la può dimostrare se dopo la contestazione gli è concesso un termine per rivolgersi ad un avvocato al fine di opporsi alla richiesta di identificazione. Una volta soddisfatte queste due condizioni procedurali, il giudice è messo in grado di valutare in via di deliberazione la quarta condizione, di natura sostanziale, che coincide con il merito della causa. E soltanto se quest'ultima viene valutata positivamente l'identificazione del *John Doe* ¹⁵ di turno è concessa all'attore.

In una precedente versione, ancora più protettiva nei confronti dell'autore del messaggio, il test richiede altresì che l'interesse dell'attore sia dotato di una "forza" particolare, tale da prevalere sulla tutela costituzionale della libertà di pensiero in forma anonima ¹⁶. Questa ulteriore condizione, che può essere a rigor di logica considerata una inutile ripetizione o enfaticizzazione del *fumus boni juris*, discende in effetti dalla necessità di ribadire la supremazia del *free speech* nel sistema dei beni garantiti dalla Costituzione statunitense.

Applicare tale condizione sarebbe evidentemente impossibile in Europa, e in particolare in Italia, dove non esiste gerarchia tra la libertà di pensiero, da un lato, e il diritto all'onore e alla reputazione, dall'altro. Meno calzanti appaiono anche altri passaggi del test in esame, dal momento che nel nostro ordinamento la verità del fatto addebitato non fa di regola venire meno la diffamazione (in particolare, la contestazione rivolta all'autore del messaggio potrebbe avere il solo effetto positivo di limitare il danno, nel caso l'offensore in tutto o in parte ritrattasse).

politiche locali, che erano state diffuse tramite un forum sponsorizzato dal giornale del luogo.

¹⁴ Si tratta dunque di cause "principalmente simboliche", come rileva L. LIBSKY, *Silencing John Doe: Defamation & Discourse in Cyberspace*, in 49 *Duke L. J.* (2000), 860.

¹⁵ *John o Jane Doe, Roe*, e così via sono i nomi con i quali viene convenzional-

mente indicata la parte processuale non ancora identificata o che deve restare anonima.

¹⁶ Così nella sentenza *Dendrite International, Inc. v. Doe*, adottata nel 2001 dalla Appellate Division del New Jersey. Il caso riguardava i messaggi anonimi, pubblicati in un forum di Yahoo!, aventi ad oggetto i dirigenti di una compagnia, accusati fra l'altro di avere intenzione di venderla.

Ciò non di meno bisogna convenire che non è affatto peregrino cercare di evitare che, con il pretesto di una diffamazione, si usi il tribunale al solo scopo di identificare e colpire l'autore del messaggio, con l'effetto di scoraggiare ora e per sempre le denunce relative a fatti di interesse pubblico.

Il problema è talmente sentito, in Nordamerica, da aver condotto all'adozione, a livello statale, di apposite misure legislative. Queste si collocano nel più vasto filone delle leggi c.d. *anti-S.L.A.P.P.* (*Strategic Lawsuits Against Public Participation*), che sono dirette a proteggere i consumatori e i dipendenti delle grandi compagnie dalle azioni che queste intentano in modo sistematico contro di loro per scoraggiarne le azioni di critica e di protesta.

Alcuni Stati, e per prima la California, hanno invero ritenuto necessario ribadire che la libertà di pensiero deve poter essere esercitata senza timore di ritorsioni giudiziarie ingiustificate, quando i messaggi vengano espressi in un luogo aperto al pubblico o in un forum pubblico e riguardino questioni di pubblico interesse¹⁷.

Decisiva al riguardo è la precisazione, contenuta nella legge californiana, secondo la quale la pubblicità del forum non dipende dalla natura, pubblica o privata, del relativo diritto di proprietà (come avviene di regola nella giurisprudenza statunitense sulla libertà di pensiero): se così non fosse, l'immunità prevista dalla legge non sarebbe mai invocabile, dal momento che tutti o quasi tutti i luoghi di discussione, nel ciberspazio, appartengono a privati.

Ciò ha consentito ad una Corte di quello Stato di ritenere che la legge anti-slapp sia applicabile anche alle *chat room* e ai *message board* (o forum) di proprietà privata, a condizione che essi siano aperti al pubblico o ad una larga frazione della comunità interessata¹⁸.

4. L'ANONIMATO COME DIFESA DELLA PERSONA DA FORME DI CONTROLLO PERVASIVE.

Va aggiunto che in Internet tacere il proprio nome non costituisce per definizione una forma di abuso o più volgarmente di

¹⁷ La legge in esame garantisce a tutti il diritto di "dismiss at an early stage non-meritorious litigation meant to chill the valid exercise of constitutional rights of freedom of speech and petition in connection with a public issue". Cfr. al riguardo R. RICHARDS, *Privacy, Security, and Human Dignity in the Digital Age. Compulsory Process in Cyberspace: Rethinking Privacy in*

the Social Networking Age, in 36 *Harvard J. of Law and Public Policy* (2013), 539 ss.

¹⁸ Cfr. D. NUNZIATO, *The Death of the Public Forum in Cyberspace*, in 20 *Berkeley Tech. L. J.* (2005), 1115 ss., 1166 ss.

V. anche S. KILIAN, *In Defense of Anonymous Online Speech in Oklahoma*, in 47 *Tulsa L. Rev.* (2012), 721 ss.

vigliaccheria, come può invece ritenersi in altri media. L'anonimato funge infatti da indispensabile difesa rispetto alle maligne potenzialità offerte alla raccolta e all'incrocio dei dati dalla telematica. Ai dati personali che per motivi più o meno leciti sono già in circolazione è bene infatti non aggiungere informazioni visibili a tutti sulle proprie opinioni politiche o sindacali o sulla propria fede, se non sulla propria salute.

In altri termini, quando si parla in Internet non è soltanto il rischio di ritorsioni a richiedere l'anonimato (come è sempre avvenuto per gli altri mezzi di diffusione), ma anche il rischio di profilature e schedature tanto da parte dei poteri pubblici quanto ad opera di privati (datori di lavoro, avversari politici, potenziali stalker).

Questo problema è universalmente noto, ma è avvertito maggiormente in Europa¹⁹, dove più viva è la memoria dei regimi autoritari, e al massimo grado in Germania, a causa delle sistematiche violazioni della riservatezza che hanno interessato i suoi cittadini sino a tempi relativamente recenti. Non a caso è la legge tedesca (art. 13, comma 6 del *Telemediengesetz*) ad imporre ai *Provider* di consentire, per quanto possibile, l'accesso ad Internet in forma anonima. Non a caso, è la giurisprudenza del Tribunale costituzionale federale tedesco la più severa nei confronti delle misure di *data retention*.

Come è noto, il Tribunale nel 2010 ha dichiarato illegittime tutte le disposizioni che consentivano l'archiviazione indiscriminata dei dati di traffico²⁰; mentre nel 2012 da un lato ha ritenuto che l'identificazione degli indirizzi IP dinamici costituisca una limitazione del diritto fondamentale al segreto della corrispondenza, e dall'altro ha dichiarato illegittimo l'obbligo di far conoscere alle autorità i codici di accesso personali degli utenti²¹.

Il valore dell'anonimato sembra tuttavia perdere colpi negli ultimi tempi. Anche la sentenza da ultimo citata accetta invero la logica dell'emergenza, laddove — con riguardo alla legittimità del divieto di commercializzare carte telefoniche prepagate anonime — ritiene che la registrazione di nome, cognome e indirizzo, pur rappresentando un'incisione non indifferente nei diritti della persona, sia da ritenere tollerabile, finché rimanga “un'eccezione”²².

Nello stesso turno di tempo, la Corte d'appello di Amburgo ha ritenuto che l'accesso anonimo garantito dalla citata *Telemediengesetz*

¹⁹ V. nella dottrina italiana G. FINOCCHIARO, *Anonimato*, in *Dig. Disc. Priv.*, Aggiornamento, 2010, 16 ss.

²⁰ BVerfG, sentenza del 2 marzo 2010.

²¹ BVerfG, sentenza del 24 gennaio 2012, rispettivamente ai nn. 172 ss. e 184 ss. della motivazione.

²² *Ibidem*, n. 136 ss. della motivazione.

gesetz non può, ragionevolmente, comprendere i servizi che per loro natura sono esposti al pericolo di illegalità ²³.

In quest'ultimo caso si parlava dello scambio di file musicali, che sembrerebbe avere ben poco a che fare con la libertà di pensiero ²⁴; così come non si può applicare direttamente alla manifestazione del pensiero la giurisprudenza relativa al segreto della corrispondenza. È vero peraltro che se l'ordinamento tedesco consente l'accesso ad Internet in forma anonima (e sia pure a condizione che tale accesso non avvenga a mezzo di carte telefoniche prepagate), questa garanzia spiega necessariamente effetto su tutti gli utilizzi di Internet, e *in primis* sulla libertà di pensiero.

Sembra in definitiva che la protezione (e la promozione) di quest'ultima attraverso l'anonimato, se negli Stati Uniti trova linfa nel principio del *marketplace of ideas*, in Germania si radichi piuttosto nella suprema necessità di difendere le persone da forme di controllo pervasivo.

Se così non fosse, sarebbe difficile spiegare come mai la giurisprudenza tedesca abbia talvolta dato la precedenza alla manifestazione anonima del pensiero rispetto alla tutela di altri diritti che pure sono considerati fondamentali, come l'autodeterminazione informativa, l'onore e la reputazione. Il caso emblematico è rappresentato dalla pronuncia resa dalla Corte suprema federale in ordine all'attività del sito *spickmich.de*, dedicato alla valutazione dei docenti scolastici da parte dei loro alunni.

A differenza dei colleghi francesi che hanno dichiarato illecita tale attività, rinvenendovi un trattamento di dati personali svolto senza il consenso degli interessati ²⁵, il *Bundesgerichtshof* ha ritenuto che le qualità o i difetti di ciascun docente siano materia di pubblico interesse, e che l'anonimato dal quale sono coperte le valutazioni sia indispensabile al fine di permettere tanto agli studenti quanto ai loro genitori di scambiarsi senza timore informazioni relative a tale materia ²⁶. La richiesta della parte attrice di venire a conoscenza della identità di coloro che l'avevano giudicata negativamente, onde poterli denunciare per trattamento illecito dei propri dati personali, è stata respinta.

²³ OLG Hamburg, sentenza del 14 marzo 2012 (c.d. *Rapidshare II*).

²⁴ Si deve tuttavia ricordare che ad avviso di una Corte statunitense (Southern District of New York, *Sony Music Entertainment Inc. v. Does 1-40*, 26 luglio 2004) il fatto di scaricare e di scambiare file coperti da copyright rappresenta una forma di manifestazione del pensiero, ed in quanto tale è dotata di una sia pur minima protezione costituzionale (che non comprende peraltro l'anonimato dell'agente).

²⁵ Con una ordinanza del 3 marzo

2008, il *Tribunal de grande instance* di Parigi ha ordinato al sito *note2be.com* di cessare l'uso e il trattamento dei dati nominativi dei professori che erano oggetto di valutazione da parte dei propri studenti. In virtù dell'art. 7 della legge "*Informatique et liberté*", il trattamento dei dati nominativi richiede il consenso della persona interessata, a meno che il responsabile del sito non persegua un interesse legittimo e non contrario ai diritti e agli interessi della persona in questione.

²⁶ BGH, sentenza del 23 giugno 2009.

Ciò che più importa, essa è stata respinta sulla base della lapidaria affermazione secondo la quale “l’anonimato è immanente a Internet”²⁷.

5. ALCUNE PROVVISORIE CONCLUSIONI.

Alla luce delle riflessioni or ora svolte si può formulare una prima conclusione: la Rete non può essere parificata agli altri mezzi, nei quali l’anonimato è immediato sinonimo di clandestinità, *id est* illegalità — la quale a sua volta può ritenersi giustificata soltanto come forma di resistenza nei confronti di un regime autoritario —.

In particolare, sembra ultroneo ritenere che siccome l’art. 21 Cost. protegge soltanto il pensiero autenticamente proprio, il parlante sia anche obbligato ad identificarsi esplicitamente, per poter fruire della tutela costituzionale²⁸. In altri termini, se è vero che il pensiero soggettivamente falso può essere vietato dal legislatore, ciò non vale a mio avviso per il pensiero espresso in forma anonima, perché esso non costituisce di per sé una frode.

Sembra peraltro inesatta anche la tesi opposta, secondo la quale la scelta di diffondere il pensiero in forma anonima atterrebbe alla libertà di formulare il contenuto del messaggio — in quanto scelta di dire o di tacere alcunché — e godrebbe pertanto del massimo livello di protezione costituzionale²⁹. In contrario si deve osservare che altro è il contenuto del messaggio (protetto, a meno che non sia subbiettivamente falso), altro è l’anonimato dell’autore, che deve essere garantito ma anche temperato con la necessità di individuare i responsabili di eventuali illeciti³⁰.

Il giusto equilibrio tra le esigenze costituzionali in giuoco non può tuttavia essere individuato se non attingendo ad una piena consapevolezza delle peculiarità che presenta la manifestazione del pensiero in Rete. Se da un lato è necessario respingere il tabù che pone la Rete fuori dal raggio di azione del legislatore, dall’altro è pure indispensabile verificare se le categorie tradizionalmente usate nel campo dei media siano adeguate alla realtà del ciberspazio.

Si tratta di un processo di apprendimento lento e complesso, che richiede una profonda conoscenza dei fenomeni internettiani e insieme una grande capacità di spogliarsi delle *idées reçues*.

²⁷ *Ibidem*, parte II, lett. cc) n. 6 della motivazione: “Die anonyme Nutzung ist dem Internet immanent”.

²⁸ Nel senso criticato M. BETZU, *Anonimato e responsabilità in Internet*, in *costituzionalismo.it*, 6 ottobre 2011.

²⁹ Così la sentenza *McIntyre* della Corte Suprema (citata *supra* alla nota 10).

³⁰ Così, ipotizzando forme di “anonimato protetto” P. COSTANZO, *Profili costituzionali di Internet*, in E. TOSI (a cura di), *I problemi giuridici di Internet*, I vol., III ed., Milano 2003, 77 ss.; A. PAPA, *op. cit.*, 86 ss.

Rileggendo le sentenze or ora sommariamente ricordate è facile, ad esempio, avere l'impressione che la tutela dell'onore e della reputazione in Internet sia destinata a seguire strade particolarmente ardue. In effetti negli Stati Uniti — dopo l'adozione del test che rende più difficile l'identificazione dell'autore di una presunta diffamazione — qualcuno ha già sottolineato il pericolo che si crei una fattispecie speciale di diffamazione in Rete, ben più difficile da punire di quella ordinaria o generale ³¹.

I giudici che si sono occupati di questi casi hanno tuttavia considerato alcune circostanze che rendono l'offesa diffusa in Internet quantitativamente, se non qualitativamente, diversa da quella manifestata attraverso altri mezzi.

In primo luogo, si è dato risalto alla possibilità dell'interessato di reagire immediatamente all'offesa, intervenendo nello stesso forum ³²; ma in realtà chiunque può incalzare l'autore del presunto messaggio lesivo, contestandone le affermazioni o chiedendo spiegazioni. La Rete consente dunque l'immediato e illimitato esercizio del diritto di rettifica, che tante resistenze trova comunemente nello spazio limitato del quale godono gli altri mezzi, e consente anzi di instaurare non solo un contraddittorio, ma un vero e proprio dibattito pubblico sul merito delle presunte offese. Ciò limita grandemente la dannosità di queste ultime, oltre a renderle strumento o occasione di informazione.

In secondo luogo, si è ritenuto che alcune offese non possono essere prese alla lettera, perché in Rete lo stile espressivo è più rilassato o perché certe parolacce fanno parte del gergo giovanile ³³. Si tocca qui la delicata questione della forma, che nella Rete riguarda la discriminazione non solo verso gli incolti, in generale, ma anche verso varie sub-culture cui non è forse corretto negare il diritto di cittadinanza.

Infine, la considerazione che sembra prevalere, espressa o inespressa, su tutte le altre si basa sulla scarsa affidabilità e/o autorevolezza del mezzo prescelto. Chi frequenta la Rete sa, o dovrebbe sapere, che i messaggi anonimi ivi diffusi possono essere esagerati, se non inventati, capziosi e fraudolenti; e che dietro il *nickname* si può nascondere qualcuno interessato a danneggiare la reputazione altrui. La valutazione normalmente rilasciata agli intermediari dell'informazione spetta oggi ai destinatari del messaggio, che possiamo supporre capaci di discernimento.

Se tutte queste considerazioni fossero condivisibili — ma non è

³¹ Cfr. M. VOGEL, *Unmasking "John Doe" Defendants: The Case Against Excessive Hand-Wringing over Legal Standards*, in 83 *Oregon L. R.* (2004), 795 ss.

³² Corte Suprema del Delaware, *Doe v. Cahill* (2005), cit.

³³ Corte d'Appello della California, *Krinsky v. Doe 6* (2008), sui commenti piuttosto pesanti rivolti ai dirigenti di una compagnia.

detto che lo siano — l'anonimato in Rete potrebbe forse risultare meno pericoloso di quanto appaia.

Abstract

The essay deals with the growing request for a ban on anonymous online messages, as a tool of wanton defamation towards people and firms. The tentative answer is that anonymity on the Net should be protected even in countries where free speech is fully guaranteed.

Two constitutional arguments, embraced by tribunals in the United States and in Europe, play in favour of this solution. The first one is the need for information in a democracy, in particular for the kind of information that would expose the whistleblower to retaliation. The second one is the need to protect personal information and data, that could be misused by the Government or by wrongdoers.