medialaws

Rivista di diritto dei media
1/2017 settembre

ANNO 2017 - CODICE ISSN 2532-9146
Impaginazione a cura di Chiara Pavesi

MediaLaws - Rivista di diritto dei media è una rivista quadrimestrale telematica, ad accesso libero, che si propone di pubblicare saggi, note e commenti attinenti al diritto dell'informazione italiano, comparato ed europeo.

La rivista nasce per iniziativa di Oreste Pollicino, Giulio Enea Vigevani, Carlo Melzi d'Eril e Marco Bassini e raccoglie le riflessioni di studiosi, italiani e stranieri, di diritto dei media.

La rivista fa proprio il Code of Conduct and Best Practice Guidelines for Journal Editors elaborato dal COPE (Comittee on Publication Ethics).

La qualità e il rigore scientifici dei saggi della Rivista sono garantiti da una procedura di *double-blind peer review* affidata a un comitato di esperti per la valutazione individuato secondo criteri di competenza e rotazione e aggiornato ogni anno.

MediaLaws - Rivista di diritto dei media
Regolamento per la pubblicazione dei contributi

1. "MediaLaws – Rivista di diritto dei media" è una rivista telematica e ad accesso aperto che pubblica con cadenza quadrimestrale contributi attinenti al diritto dell'informazione.

2. Gli organi della rivista sono il Comitato di direzione, il Comitato scientifico e il Comitato degli esperti per la valutazione. L'elenco dei componenti del Comitato di direzione e del Comitato scientifico della rivista è pubblicato sul sito della stessa (www.medialaws.eu/rivista). Il Comitato degli esperti per la valutazione è sottoposto ad aggiornamento una volta l'anno.

3. La rivista si compone delle seguenti sezioni: "Saggi", "Note a sentenza" (suddivisa in "Sezione Europa", "Sezione Italia" e "Sezione straniera"), "Cronache" e "Recensioni e riletture". I singoli numeri potranno altresì ospitare, in via d'eccezione, contributi afferenti a sezioni diverse.

4. La sezione "Saggi" ospita contributi che trattano in maniera estesa e approfondita un tema di ricerca, con taglio critico e supporto bibliografico.

5. La sezione "Note a sentenza" ospita commenti alle novità giurisprudenziali provenienti dalle corti italiane, europee e straniere.

6. La sezione "Cronache" ospita commenti a questioni e novità giuridiche di attualità nella dimensione nazionale, europea e comparata.

7. La sezione "Recensioni e riletture" ospita commenti di opere rispettivamente di recente o più risalente pubblicazione.

8. La richiesta di pubblicazione di un contributo è inviata all'indirizzo di posta elettronica submissions@medialaws.eu, corredata dei dati, della qualifica e dei recapiti dell'autore, nonché della dichiarazione che il contributo sia esclusiva opera dell'autore e, nel caso in cui lo scritto sia già destinato a pubblicazione, l'indicazione della sede editoriale.

9. La direzione effettua un esame preliminare del contributo, verificando l'attinenza con i temi trattati dalla rivista e il rispetto dei requisiti minimi della pubblicazione.

10. In caso di esito positivo, la direzione procede ad assegnare il contributo alla sezione opportuna.

11. I saggi sono inviati alla valutazione, secondo il metodo del doppio cieco, di revisori scelti dall'elenco degli esperti per la valutazione della rivista secondo il criterio della competenza, della conoscenza linguistica e della rotazione. I revisori ricevono una scheda di valutazione, da consegnare compilata alla direzione entro il termine da essa indicato. Nel caso di tardiva o mancata consegna della scheda, la direzione si riserva la facoltà di scegliere un nuovo revisore. La direzione garantisce l'anonimato della valutazione.

12. La direzione comunica all'autore l'esito della valutazione.
Se entrambe sono positive, il contributo è pubblicato.
Se sono positive ma suggeriscono modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. La direzione si riserva la facoltà di sottoporre il contributo così come modificato a nuova valutazione, anche interna agli organi della rivista. Se solo una valutazione è positiva, con o senza modifiche, la direzione si riserva la facoltà di trasmettere il contributo a un terzo valutatore. Se entrambe le valutazioni sono negative, il contributo non viene pubblicato.

13. Per pubblicare il contributo, l'Autore deve inviare una versione definitiva corretta secondo le regole editoriali della rivista pubblicate sul sito della stessa, un abstract in lingua italiana e inglese e un elenco di cinque parole chiave. Il mancato rispetto dei criteri editoriali costituisce motivo di rigetto della proposta.

14. Le valutazioni vengono archiviate dalla direzione della rivista per almeno tre anni.

15. I contributi di autori di particolare autorevolezza possono essere pubblicati senza essere sottoposti alla procedura di valutazione, dandone notizia in nota a tali contributi.

Editoriale

Saggi
Sezione Monografica "*fake news*, pluralismo informativo e responsabilità in rete"

Note a sentenza
Sezione Europa
Corte di giustizia dell'Unione Europea

Note a sentenza
Sezione Europa

Corte europea dei diritti dell'uomo

Note a sentenza
Sezione Italia

Cronache

Editorial

Articles
Fake news, pluralism and ISP liability

Notes and comments
Europe
Court of Justice of the European Union

Notes and comments
Europe

EUROPEAN COURT OF HUMAN RIGHTS

Notes and comments
Italy

New legislation

Perché MediaLaws diventa (anche) una rivista scientifica?

Editoriale di
Oreste Pollicino
Giulio Enea Vigevani

Nel 2010 nasceva il blog medialaws.eu con un obiettivo: diventare il punto di riferimento per chiunque fosse interessato alle trasformazioni del diritto all'informazione alla prova del nuovo contesto tecnologico. Nel tempo, la piattaforma ha attratto contenuti di spessore giuridico sempre più significativo e, al contempo, il campo del diritto dei media si è sempre più esteso ed è andato acquisendo una sempre maggiore autonomia metodologica e disciplinare.

In questo contesto, è emersa quasi naturalmente l'esigenza di affiancare al blog una sede scientifica in cui potere approfondire le prospettive sempre più numerose discendenti dalle trasformazioni tecnologiche e giuridiche prima descritte. Su queste basi nasce "MediaLaws - Rivista di diritto dei media". Un *legal journal* geneticamente interdisciplinare, aperto ai diversi campi del sapere giuridico ma anche ai rapporti tra diritto ed altre scienze; geneticamente posizionato all'incrocio tra diritto interno e diritto sovranazionale, attento tanto alle grandi questioni teoriche di portata globale quanto a problemi concreti dibattuti quotidianamente nelle aule di giustizia. Tale duplice proiezione, internazionale e domestica, teorica e concreta, porta fisiologicamente la Rivista a rivolgersi in via privilegiata tanto agli studiosi sensibili ai rapporti.

Con queste premesse, la Rivista non cela l'ambizione di diventare uno dei punti di riferimento del dibattito scientifico legato al sempre più consolidato ambito disciplinare del diritto dei media. Con due tratti costitutivi. In primo luogo, l'obiettivo di dialogare con gli studiosi di altri ordinamenti: per questo l'inglese si affianca all'italiano quale lingua di lavoro. Infine, ed emblematicamente, la consapevolezza della centralità, ieri, oggi e domani, della libertà di espressione quale diritto dell'individuo e fondamento della democrazia pluralista.

Saggi
Articles

Sezione Monografica “*fake news*, pluralismo informativo e responsabilità in rete”
Fake News, Pluralism and ISP Liability

Primi appunti su *fake news* e dintorni.
Fake News: an Introduction to the Italian Debate

Marco Bassini
Assegnista di ricerca in Diritto costituzionale presso l'Università Commerciale "L. Bocconi"
Giulio Enea Vigevani
Professore associato di Diritto costituzionale presso l'Università degli Studi di Milano - Bicocca

Abstract

L'articolo affronta alcuni quesiti preliminari al fine di introdurre il dibattito in corso, in Italia, rispetto alla possibile adozione di misure speciali finalizzate al contrasto delle *fake news* in Internet. Il saggio muove dall'assunto secondo il quale il dibattito attuale e l'enfasi mediatica sul problema delle *fake news* derivino in larga parte da una non corretta ponderazione delle caratteristiche di novità diInternet, e dal convincimento che si debba a esso il propagarsi di un fenomeno già ampiamente diffuso nei media tradizionali. Muovendo da questo assunto, l'articolo evoca la necessità di una puntuale definizione delle categorie di contenuti che rientrano nell'ambito delle *fake news* ai fini di selezionare le tipologie di informazione non veritiera che, incidendo su un bene giuridico costituzionalmente protetto, meritano l'adozione di idonee misure di contrasto. Ciò chiarito, il saggio, sulla base di un'interpretazione liberale del diritto di espressione, evidenzia perplessità rispetto alle posizioni, sempre più diffuse, che salutano con favore il coinvolgimento attivo degli *Internet service provider* (tra cui i motori di ricerca e i *social network*) nell'attuazione di sistemi di filtraggio finalizzati alla rimozione delle notizie false da Internet.

The article aims at addressing some preliminary questions with a view to introducing the ongoing debate in Italy on the implementation of special legislative measures to contrast the spread of fake news on the Internet. The essay claims that said debate is to a large degree biased as result of an inherent overestimation of the evils and perils of the Internet. Fake news would constitute, indeed, a long-standing problem that has affected over the time traditional media too. Assuming that there is no qualified connection between the rise of the Internet and the spread of fake news, the article call for a more precise definition of fake news in order to determine which categories of false statements may affect constitutionally protected interests and those which are merely irrelevant. Once clarified that only some types of fake news should be subject to legal prohibition, the article, on the basis of a liberal interpretation of freedom of speech, criticizes the view that Internet service providers (including social network and search engine providers) may be actively involved in filtering systems with the purpose of removing fake news from the Internet.

Sommario

Internet
fake news
social network
responsabilità degli ISP
hate speech

1 Introduzione

Nell'ultimo anno, il dibattito tra gli studiosi del diritto dei media è stato quasi monopolizzato da un tema sino a poco prima ignoto: le *fake news*. Il confronto all'interno della comunità scientifica internazionale, per vero, è stato provocato – come sempre più spesso accade – da fattori prevalentemente esogeni, legati alla crescente esacerbazione del dibattito pubblico e alla sua emancipazione da una dialettica a carattere irenico, secondo quella dinamica di polarizzazione studiata da tempo da Cass Sunstein[1]. A determinare questo clima, in cui tanto l'accreditamento di *fake news* da parte del pubblico quanto le manifestazioni d'odio (*hate speech*) hanno conosciuto terreno fertile, ha senz'altro contribuito l'esplosione dell'utilizzo dei *social network* come mezzo di propaganda politica. Nonostante la "novità" dei mezzi tramite i quali l'odio *online* e le *fake news* penetrano nel dibattito pubblico, occorre peraltro interrogarsi se queste problematiche presentino dei caratteri del tutto innovativi o non sottendano, invece, sotto sembianze apparentemente nuove, tematiche già note anche in tempi meno tecnologici.

A fronte del propagarsi di un fenomeno che, nella sua declinazione attiva (ossia come "produttori") e passiva (ossia come "vittime") non ha risparmiato diversi suoi esponenti, la classe politica non è rimasta inerte. A livello nazionale*, inter alia,* è stata presentata una proposta di legge (il cosiddetto "DDL Gambaro")[2], da subito oggetto di forti critiche, che mira a responsabilizzare le piattaforme *online* per la diffusione di notizie false, esagerate, tendenziose o tendenti a turbare l'ordine pubblico, oltre a introdurre fattispecie di reato *ad hoc* per gli autori di tali notizie e per la diffusione di campagne d'odio. Tale disegno di legge non pare, invero, avere alcuna possibilità di completare l'iter parlamentare.

Ben di maggiore interesse – come vedremo – è il lavoro del Parlamento tedesco che ha condotto all'approvazione di una legge – anch'essa assai controversa – che regola i compiti e la responsabilità dei *social network*, specie in caso di *hate speech*[3].

Anche a livello di Unione europea, la questione del contrasto alle manifestazioni del pensiero illecite in rete si sta ponendo sempre più all'ordine del giorno. Di qualche interesse anche per il tema delle *fake news* è, da ultimo, la Comunicazione in materia di lotta ai contenuti illeciti *online*[4] che, nel settembre 2017, la Commissione europea ha trasmesso a Parlamento e Consiglio. Tale testo mira a valorizza il ruolo "proattivo" degli intermediari, sulla base del postulato che le piattaforme *online* debbono esercitare una maggiore responsabilità nel controllo dei contenuti. La Comunicazione prevede, infatti, una serie di linee-guida e principi per le piattaforme *online*, per intensificare la lotta contro i contenuti illegali in rete, in collaborazione con le autorità nazionali, gli Stati membri e gli altri soggetti interessati, specie in relazione ai reati di incitamento al terrorismo e di *hate speech*. In particolare, individua una serie strumenti comuni per prevenire, individuare rapidamente, rimuovere ed evitare la ricomparsa, attraverso la disattivazione dell'accesso, di contenuti illeciti. In questa prospettiva, agli operatori della rete è richiesto di attivarsi velocemente nella rimozione dei contenuti, in taluni casi anche solo dopo una segnalazione di soggetti privati.

Sul piano dottrinale, limitandoci all'Italia, il merito di aver inaugurato il dibattito sul tema del contrasto alle *fake news* deve essere forse attribuito a Giovanni Pitruzzella, che sulle pagine di due autorevoli quotidiani rifletteva sugli strumenti per garantire un'informazione corretta in rete[5]. Due i punti nodali della tesi dell'attuale Presidente dell'Antitrust: l'affermazione dell'estraneità delle *fake news* all'ambito di tutela della libertà di informazione e la proposta di misure di filtraggio da adottarsi o dagli *Internet service provider* che ospitano i contenuti caricati dagli utenti o da operatori autonomi e terzi, appositamente incaricati di liberare la rete dalle informazioni patentemente false.

La proposta di Pitruzzella, sviluppata ulteriormente in un volume scritto insieme a Oreste Pollicino e Stefano Quintarelli[6], ha suscitato reazioni polemiche, dettate in particolare dai dubbi circa la legittimità costituzionale e l'opportunità di un regime "speciale" per la manifestazione del pensiero

---

[*] Sebbene il presente scritto costituisca il frutto di riflessioni condivise degli autori, Giulio Enea Vigevani ha redatto i paragrafi 1-2-3 mentre Marco Bassini ha curato la stesura dei paragrafi 4-5-6. Il paragrafo 7 è da ascrivere congiuntamente agli autori.

[1] Da ultimo, C. Sunstein, *#Republic: Divided Democracy in the Age of Social Media,* Princeton, 2017.

[2] Senato della Repubblica, Disegno di legge n. 2688, "Disposizioni per prevenire la manipolazione dell'informazione *online*, garantire la trasparenza sul web e incentivare l'alfabetizzazione mediatica", presentato il 28 febbraio 2017.

[3] Legge per migliorare l'applicazione della legge sui *social network* (*Netzwerkdurchsetzungsgesetz* – NetzDG). Si v. la traduzione a cura di G. Giannone Codiglione, in *questa Rivista.*

[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms", 28 settembre 2017 COM(2017) 555 final.

[5] G. Pitruzzella, *Quel filtro necessario per le notizie false sul web,* in *Corriere della sera,* 2 gennaio 2017;
cfr. anche *Italy antitrust chief urges EU to help beat fake news,* in *Financial Times,* 30 dicembre 2016.

[6] G. Pitruzzella – O. Pollicino – S. Quintarelli, *Parole e potere*, Milano, 2017.

in rete[7]. Tali posizioni sottolineavano altresì la difficile compatibilità di ogni sistema di filtraggio sul web con la disciplina europea dei servizi Internet ed evocavano sovente la metafora del *marketplace of ideas*, coniata dalla giurisprudenza della Corte suprema statunitense per estendere la protezione del Primo Emendamento anche a manifestazioni di pensiero connotate da disvalore o prive di qualsiasi contributo per il dibattito pubblico[8].
Proprio l'invocazione di tale metafora a garanzia di una più ampia circolazione del pensiero in rete è discussa criticamente da Oreste Pollicino[9], che ne contesta la perdurante applicabilità a Internet, che costituirebbe un mercato non più *free,* ossia non più libero dal potere degli *over the top*. In questa prospettiva, si potrebbe giustificare una regolazione che possa ammettere ipotesi di interventi preventivi nei confronti delle *fake news*, senza tuttavia rendere i *provider* censori e giudici del vero e del falso.
Nel corso degli ultimi mesi il dibattito si è così arricchito grazie a diverse prese di posizione, alcune delle quali trovano spazio all'interno della sezione monografica di questo fascicolo (tra i molti, i saggi di Marco Cuniberti, Cesare Pinelli e Franco Pizzetti). Non è casuale che a esercitarsi su questo versante di ricerca siano stati, finora, soprattutto gli studiosi della Costituzione: a ben vedere, ogni riflessione incentrata sulla repressione del fenomeno delle *fake news*, così come, del resto, dei discorsi d'odio intercetta un tema che si colloca alle radici dello stato liberal-democratico e chiama in causa l'interpretazione dei principi costituzionali e, in specie, della libertà di espressione. Non sono estranee a questo discorso, peraltro, le concezioni relative al modello di democrazia ("aperta" o "militante"[10]) nonché forse anche la visione ottimistica o pessimistica in ordine alla capacità dei cittadini di sottoporre a giudizio critico i messaggi veicolati sulle nuove e vecchie piattaforme informative.
Anche per queste ragioni, i contributi presenti nella sezione monografica di questa rivista riflettono idee anche molto distanti. Questo scritto introduttivo mira, non senza un qualche sforzo speculativo, a rappresentare una prima riflessione critica rispetto ad alcune questioni che si appalesano come cruciali per determinare la compatibilità con il sistema costituzionale delle misure volte alla repressione del fenomeno delle *fake news*. Di qui, un elenco di interrogativi a cui si cercherà di dare una prima risposta: che cosa si intende per *fake news*? Quale differenza intercorre tra il fenomeno delle *fake news* e i discorsi d'odio (*hate speech*)? È possibile identificare con esattezza e in via generale un bene giuridico leso dalla mera diffusione delle notizie false? La disciplina sulla (ir)responsabilità degli *Internet service provider* merita di essere rivisitata alla luce del modello di business che in concreto rivestono i moderni operatori delle piattaforme di condivisione? O, al contrario, tale normativa deve essere preservata nei suoi caratteri essenziali, ancorché a significativa distanza (cronologica e "tecnologica") dalla sua adozione? E ancora: il paradigma costituzionale a tutela del pluralismo informativo è ancora valido nel nuovo ecosistema digitale dell'informazione?

2 Alcune premesse di carattere metodologico

Prima di affrontare il dibattito sulla liceità delle *fake news* e sull'opportunità per il legislatore - italiano ed europeo - di intervenire in questo terreno, pare utile muovere da un'osservazione preliminare, che riguarda lo statuto giuridico delle notizie "false" in sé considerate.
Invero, all'interno del testo della Costituzione e delle disposizioni, specialmente di diritto penale, dedicate all'esercizio della libertà di parola, non sembrano rinvenirsi indicazioni che depongano per una collocazione del falso nell'alveo del giuridicamente illecito. Paolo Barile, maestro anche del diritto dell'informazione, più di trent'anni fa sottolineava come «neppure la diffusione di notizie false può essere considerata illecita in sé e per sé»; infatti, «il "fine d'inganno" può essere illecito solo

[7] Tra le molte reazioni attraverso i media, cfr., C.A. Carnevale Maffé, *Neppure l'Autorità della Veridicità può fermare il mercato delle bufale,* in *Il Foglio,* 7 gennaio 2017; C. Melzi d'Eril – G.E. Vigevani, *Difesa giuridica dal socia-chiacchiericcio,* in www.ilsole24ore.it, 2 aprile 2017; C. Blengino, *Non si legifera sulla verità,* in www.ilpost.it, 9 gennaio 2017; M. Bassini, Fake news: *perché non è un lavoro da spazzini (del web),* in www.medialaws.eu, 16 marzo 2017. Sintetizza bene il dibattito e i profili economici e giuridici rilevanti A. Nicita, *È possibile il libero scambio nel mercato della verità?,* in *Il Foglio,* 15 gennaio 2017.
[8] Cfr. la celebre *dissenting opinion* di Justice Holmes in *Abrams v. United States* 250 U.S. 616 (1919).
[9] Si v. O. Pollicino, *Fake News, Internet and Metaphors (to be handled carefully),* in 9(1) *Italian Journal of Public Law* (2017), ripubblicato anche in questa *Rivista*.
[10] Tra i molti riferimenti, si v. K. Loewenstein, *Militant Democracy and Fundamental Rights*, in 31 *American Political Science Review* (1937), 417 ss.

in quanto costituisca il fulcro di un'attività illecita che contrasti con altri principi costituzionali»[11].
Nella medesima logica, anche le disposizioni incriminatrici vigenti che puniscono una condotta consistente nella circolazione di informazioni non veritiere, invero, non colpiscono tale comportamento in sé, ma lo ammantano di rilevanza penale nella misura in cui, per esempio, provochi allarme sociale o nocumento all'ordine pubblico. Analoga è la *ratio* che fa prevalere i diritti della personalità (onore, reputazione, identità personale, dignità) nel conflitto con il diritto di cronaca, qualora quanto narrato non corrisponda al vero.
Si ritiene, dunque, opportuno percorrere una scelta di metodo, ovvero l'adesione alla c.d. "teoria del bene giuridico costituzionalmente protetto", che reprime comportamenti illeciti in ragione dell'idoneità a pregiudicare un bene di rilievo costituzionale che l'ordinamento vuole tutelare. Già aderendo a questa posizione è possibile discostarsi da quelle ricostruzioni che assumono, al contrario, una concezione del falso come elemento in sé illecito e generativo di responsabilità in capo a chi lo dissemini: in questa direzione appare muoversi senza particolari freni il disegno di legge Gambaro a cui si è accennato.
Si deve, poi, svolgere un'ulteriore fondamentale premessa, che si lega all'osservazione dei mutamenti che si sono prodotti nell'ambito del settore dell'informazione.
L'evoluzione digitale ha provocato importanti trasformazioni, realizzando una disintermediazione rispetto agli operatori dell'informazione che, in precedenza, potevano vantare una sorta di oligopolio nella creazione e diffusione di notizie. Del resto, già in precedenza l'invenzione della stampa aveva allargato l'ambito dei soggetti in condizione di esercitare, con la scrittura, il proprio diritto di parola e fenomeni analoghi si sono verificati alla nascita di ogni ulteriore mezzo di comunicazione.
I nuovi media estendono ulteriormente la cerchia dei soggetti, addivenendo a un riconoscimento pressoché universalistico del «diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione», che induce a marginalizzare, almeno in parte, il ruolo degli operatori professionali dell'informazione cui era affidato, in precedenza, il controllo delle notizie (laddove per controllo si intende la produzione, l'accertamento, la verifica e tutte le attività complementari e collegate).
L'abbattimento dei costi e la relativa facilità con la quale chiunque può oggi attivare un sito Internet e condividerne i contenuti hanno determinato una apertura pressoché incondizionata, in cui ciascun utente, un tempo mero ricettore di informazioni, può divenirne oggi produttore, pur non disponendo del bagaglio di competenza e di esperienza che dovrebbe essere proprio di un giornalista professionista.
Queste trasformazioni sollecitano l'esigenza di riflettere sulla persistente attualità dei principi e delle regole di derivazione liberale ovvero sulla necessità di rivisitare alcuni punti fermi e consolidati per reagire allo sviluppo e alla diffusione sul web di un fenomeno profondamente diverso da quelli finora conosciuti.
In altri termini, occorre interrogarsi se le differenze tra media tradizionali e nuovi media siano così profonde da pretendere l'elaborazione non solo di nuove norme puntuali ma addirittura di nuovi paradigmi.
L'impressione è che, a discapito della recente attualità del dibattito sulle *fake news,* le radici del problema siano antiche[12] e che le questioni specifiche da affrontare non così nuove, a fronte di un mezzo (Internet) che esiste da venti anni e uno strumento (i *social network*) che conosce una diffusione decennale.

3 *Fake news*: un tentativo definitorio

Un altro fattore di cruciale importanza, per depurare il dibattito da possibili fraintendimenti, riguarda la definizione del perimetro delle *fake news*. Esistono infatti diversi tentativi di concettualizzazione di questa categoria, mediante l'astrazione di caratteristiche comuni che la rendono predica-

[11] P. Barile, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984, 229. Apparentemente "possibilista" rispetto al potere dello Stato di intervenire, punendo il «subiettivamente falso» (a differenza dell'obiettivamente erroneo), è invece la tesi di un altro grande studioso del Novecento, Carlo Esposito (*La libertà di manifestazione del pensiero nell'ordinamento italiano,* Milano, 1958, spec. 36-37), secondo cui tali affermazioni non rientrerebbero nell'ambito di applicazione della garanzia costituzionale della libertà di manifestazione del pensiero ma non sarebbero direttamente vietate. Ma, a ben vedere, lo stesso Autore precisa (nota 82) che, «poiché la Costituzione non statuisce né impone di statuire un generale obbligo di verità, ma si limita a garantire le sole manifestazioni veritiere, i divieti legislativi saranno giustificati solo in rapporto alle concrete finalità pratiche sommariamente elencate nel testo». Sarebbe così consentito, anche secondo l'impostazione del grande giurista napoletano, vietare e punire il falso, ma solo «in vantaggio della fede pubblica in generale, o di più individuati interessi di singoli o di collettività». Così, la stessa posizione di Esposito finisce con il condurre alla ricerca di un bene giuridico la cui protezione potrebbe giustificare la limitazione della sfera di esercizio della libertà di parola e per sconfessare l'assunto della rilevanza illecita per sé del falso.
[12] Non è casuale che il fenomeno delle "bufale" nell'ambito dell'attività informativa abbia impegnato i giuristi anche in tempi non sospetti : si v. S. Casillo – F. Di Trocchio – S. Sica, *Falsi giornalistici. Finti scoop e bufale quotidiane,* Napoli, 1997.

bile rispetto a un ambito più o meno ampio di contenuti veicolati sul web.
Riteniamo corretto muovere da un dato empirico, ossia la falsità delle notizie. Per *fake news* si dovrebbero intendere senz'altro le notizie false, le menzogne. Si tratta di un fenomeno che precede senz'altro lo sviluppo di Internet e delle nuove tecnologie, ma che da questi sviluppi ha derivato una più marcata rilevanza nel dibattito pubblico: nell'epoca della post-verità, infatti, non esistono più esperti di indiscussa autorevolezza (a prescindere dal rispettivo campo di competenza ed esperienza) e le emozioni, le pulsioni e i desideri, anche in conseguenza delle dinamiche di polarizzazione ben descritte da Cass Sunstein[13], finiscono per prevalere o comunque occupare un posto non meno importante dei meri fatti. In questo scenario, una possibile tassonomia delle *fake news* propone di distinguere tre categorie di contenuti[14].
La prima categoria comprende le falsità costruite ad arte da gruppi di potere, talvolta dagli stessi governi stranieri (specialmente di Stati la cui tenuta democratica pare vacillare). Queste notizie sono create e diffuse deliberatamente con l'obiettivo di modificare l'agenda pubblica, manipolando l'informazione e la formazione dell'opinione pubblica anche tramite il ricorso all'utilizzo di tecnologie sofisticate (compreso l'utilizzo di *account* coordinati o gestiti da robot che funzionano in base ad algoritmi): a riguardo di questa tipologia, il saggio di Franco Pizzetti[15] compreso in questa sezione monografica illustra dettagliatamente le modalità operazionali della disinformazione e le relative criticità connesse. Quale risposta rispetto a questa categoria di *fake news*? La reazione più opportuna appare la previsione di obblighi di trasparenza e di identificazione della fonte di provenienza, cui dovrebbe correlarsi la possibilità di isolare e segnalare le notizie generate artificialmente tramite robot. In quest'ottica, a essere colpita non è tanto la categoria delle *fake news* in quanto tali, bensì la fonte di produzione delle medesime, vale a dire gli *account* deliberatamente creati e funzionali alla diffusione di notizie false.
Una seconda categoria di un'ipotetica tassonomia comprende le notizie false o di dubbia autenticità che circolano in rete suffragate dalla condivisione tra utenti (la *vox populi*). Può trattarsi di innocuo chiacchiericcio ma anche di contenuti che inducono a comportamenti poco provveduti: l'esempio classico è dato dalla ricorrente affermazione secondo cui i vaccini andrebbero contrastati in quanto espressione del potere di mercato delle imprese farmaceutiche. Queste notizie non incontrano specifici divieti, almeno in via generale, nel mondo "della materia". Questione aperta è se le caratteristiche proprie di Internet debbano indurre a una diversa risposta e all'elaborazione di regole nuove, in ragione del maggior carattere diffusivo della rete[16]. Resta comunque che nella nostra organizzazione sociale, lo Stato fornisce l'istruzione, educa al senso critico e promette una informazione obiettiva attraverso il servizio pubblico e plurale attraverso il sistema dei media, cartaceo, audiovisivo e digitale. Se poi la profilassi delle malattie di un figlio viene attuata sulla base delle opinioni ascoltate in una piazza, reale o virtuale che sia, forse non tutte le responsabilità sono da attribuirsi alla rete…
Da ultimo, la terza categoria include tutte le notizie false che ledono interessi individuali o collettivi. In presenza di contenuti di questo tipo, dovrebbe essere agevole, percorrendo alcuni insegnamenti giurisprudenziali già corroborati, applicare alla rete le medesime regole che vietano la condotta *offline*. La vera sfida in questo contesto appare l'individuazione di opportune misure che consentano di conoscere chi è responsabile della diffusione delle notizie false, di qualificarlo agli occhi dell'opinione pubblica (come foriero di menzogne), di poter replicare alle falsità diffuse, di rimuoverle una volta accertata l'illiceità e di chiedere conto dei danni provocati.

4 Un problema sempre esistito

Agli albori di Internet, quando ancora si utilizzavano i modem 56 Kbps e la rete non aveva ancora pervaso ogni segmento della dimensione sociale e professionale degli individui, venne alla luce

[13] Cfr. anzitutto C. Sunstein, *The Law of Group Polarization,* 10(2) *Journal of Political Philosophy* (2002) 175 ss. e soprattutto, più recentemente, Id., *#Republic. Divided Democracy in the Age of Social Media*, cit. Secondo Sunstein, l'avvento delle cosiddette "cascate informative" avrebbe contributo a determinare una dinamica di radicalizzazione del dibattito pubblico in cui, anziché sottoporre le proprie posizioni a un ulteriore vaglio critico, ogni utente-consumatore di informazione agisce secondo un pregiudizio di conferma e tende a rafforzare le proprie convinzioni e ad accrescere la distanza rispetto alle posizioni avverse.
[14] Per un primo abbozzo di tale classificazione, cfr. C. Melzi d'Eril – G.E. Vigevani, *Difesa giuridica dal social-chiacchiericcio,* in www.ilsole24ore.it, 2 aprile 2017.
[15] F. Pizzetti, Fake news *e allarme sociale: responsabilità, non censura,* in *questa Rivista*.
[16] Interessanti notazioni, a questo proposito, sono state svolte da C. Sunstein, *Democracy and the problem of free speech,* New York, 1995, il quale si interroga sulla persistente tenuta dello standard di tutela della libertà di espressione, ancorato alla dottrina del *clear and present danger*, rispetto alle caratteristiche di Internet. Tale interrogativo si pone soprattutto in relazione alla capacità dei messaggi d'odio di suscitare approvazione e di presentare un'effettiva idoneità a indurre o incitare comportamenti violenti in ragione delle diverse modalità di diffusione e di penetrazione nelle comunità di utenti. Cfr. anche Id., *Does the Clear and Present Danger Test Survive Cost-Benefit Analysis?*, Harvard Law School – Harvard University, in *SSRN-Social Sciences Research Network,* novembre 2016.

un "servizio antibufale", che tuttora esiste e funziona. Ai tempi, questo servizio serviva perlopiù a sconfessare un uso improprio e che oggi definiremmo probabilmente scellerato per la *privacy*, della posta elettronica, eletto a veicolo di "catene di Sant'Antonio", richieste di aiuto per raccolte fondi o magici quanto improbabili effetti moltiplicatori della propria ricchezza o, se volete, molto più realisticamente, credulità.

Ai non pochi sprovveduti dediti a un utilizzo quasi ludico e certo disinvolto delle email, veniva così dischiuso l'orizzonte di una verità in cui nessuna sventura era destinata a colpire i temerari che avessero "bloccato" queste catene o in cui, per esempio, la richiesta di aiuto di rivelava falsa o tristemente inutile.

Non solo i "servizi antibufala" ma anche l'incremento della familiarità con il mezzo e la crescente alfabetizzazione digitale (cui purtroppo fa da contraltare un non altrettanto ingente tasso di alfabetismo funzionale) hanno permesso di superare, nei primi anni di diffusione di Internet, questo fenomeno.

Viene dunque da chiedersi se anche oggi, a fronte di una nuova ondata di "bufale", stavolta per il tramite diretto (anche) del web, lo sviluppo di una maggiore capacità di discernimento da parte degli utenti non prometta un eguale superamento del problema della circolazione di *fake news*.

In fondo il parallelismo sembra trovare conferma: mentre la circolazione delle prime "catene" era affidata a un uso incauto, pressoché elementare, della posta elettronica, la circolazione di notizie infondate si alimenta al giorno d'oggi del "web partecipativo", in cui non solo è possibile attivare canali o piattaforme di condivisione, che formalmente si presentano come siti di controinformazione ma rappresentano un ricettacolo di notizie del tutto approssimative, non veritiere o tendenziose, ma al contempo è dato agli utenti interagire attivamente con i contenuti, condividendoli, commentandoli e così contribuendo, in alcuni casi, anche a forme "virali" di circolazione.

Questa ipotesi ricostruttiva sembra confermare le parole di Mill[17], e confortare così l'idea che soltanto un apporto sempre più ampio di informazione consente di migliorare complessivamente la qualità dell'ecosistema informativo.

Questa chiave di lettura evoca del resto l'elaborazione della dottrina e della giurisprudenza statunitense in materia di libertà di espressione, e la metafora del *marketplace of ideas*, in cui la cartina di tornasole dell'autorevolezza dell'informazione è data dalla sua capacità intrinseca di suscitare un riscontro all'interno dell'opinione pubblica[18]. Sicché, in una visione squisitamente di stampo liberale, anche le notizie infondate, mendaci o comunque non verificate meriterebbero di circolare, in quanto la loro scarsa attendibilità sarebbe destinata a trovare conferma nella incapacità di fare presa sull'uditorio. Al contempo, proprio l'esistenza e la circolazione di informazioni di cattiva qualità, tendenziose o non verificate permetterebbe di esaltare il carattere qualificato dell'informazione professionale.

La possibilità di utilizzare questo impianto dogmatico sembra suffragata dall'atteggiamento della giurisprudenza della Corte suprema statunitense, che non ha modificato il suo tradizionale approccio garantista nell'ambito della casistica relativa a ipotesi di limitazione della libertà di espressione in rete, dalla sentenza *Reno v. ACLU* del 1997 in poi.

E, del resto, l'esistenza di un contesto policentrico, composto da più *gatekeepers* (non solo i siti informativi ma anche le piattaforme di condivisione come i *social network*), contribuisce in certa misura ad attenuare i potenziali effetti lesivi derivanti dalla circolazione di notizie infondate, *in primis* creando un contesto di concorrenzialità tra le fonti ma soprattutto rendendo sempre più plurale e pluralistico l'assetto degli attori coinvolti nel mercato dell'informazione, non più circoscritto a un novero di operatori qualificati, alla stregua di veri e propri intermediari, il cui ruolo di "oligarchi" dell'informazione avrebbe potenzialmente aggravato l'effetto di una potenziale condotta diffamatoria. In altri termini, lo scenario di un'informazione disintermediata, in cui talvolta gli utenti divengono creatori-fruitori, sembra attenuare gli effetti negativi connessi alla diffusione di notizie false o lesive di interessi rispetto all'epoca in cui la circolazione delle medesime era affidata a un gruppo più ristretto di soggetti che, spartendosi il mercato, intercettavano un pubblico più ampio rispetto a quello che i singoli *gatekeepers* possono oggi contare, sebben complessivamente più ampio.

Discorso diverso vale forse per l'*hate speech*, dove la maggiore diffusività del discorso dell'odio su Internet alimenta il concretizzarsi di un evento lesivo, in quanto suscitando approvazione il messaggio presenta una maggiore capacità di tradursi in un effetto incitativo o di istigazione alla

[17] Così J.S. Mill, *Saggio sulla libertà*, Londra, 1859, trad. it. di S. Magistretti, Milano, 2012, 71: «Anche se l'opinione repressa è un errore, può contenere, e molto spesso contiene, una parte di verità; e poiché l'opinione generale o prevalente su qualsiasi questione è raramente, o mai, l'intera verità, è soltanto mediante lo scontro tra opinioni opposte che il resto della verità ha una probabilità di emergere».

[18] Ancora oggi emblematica in tal senso è la celeberrima affermazione di Louis Brandeis nell'opinione concorrente alla sentenza della Corte suprema statunitense nel caso *Whitney v. California,* 274 U.S. 357 (1927), 377: «*If there be time to expose through discussion the falsehood and fallacies, to avert the evil by the processes of education, the remedy to be applied is more speech, not enforced silence*».

commissione di atti di violenza. In questo quadro, il test del *clear and present danger* coniato dalla giurisprudenza statunitense potrebbe forse iniziare a vacillare. Va tuttavia rimarcata la differenza tra le due fattispecie, ancorché correlate in alcune circostanze, e segnatamente laddove le campagne d'odio si nutrano anche della diffusione di notizie prive di fondamento. Se peraltro, a rigore, l'*hate speech* già rientra nel perimetro delle norme vigenti quando l'utilizzo di un linguaggio d'odio tracimi – come non infrequentemente accade – in condotte diffamatorie o ingiuriose, che attentano all'onore e alla reputazione degli individui, insidiandone in definitiva anche la dignità, nel caso delle *fake news* le coordinate del problema appaiono diverse, sol che si pensi, per esempio, al ruolo delle piattaforme *online*, che a fronte della conclamata natura illecita di determinati contenuti possono essere richiesti (e obbligati) di procedere alla relativa rimozione, senza timore, verosimilmente, di essere tacciati come censori privati[19] o comunque come titolari di una responsabilità di tipo editoriale nella selezione dei contenuti.
Appare però dominante, non tanto nelle trattazioni dei giuristi, quanto nei dibattiti a livello mediatico e politico[20], una tendenza a confondere i diversi piani in cui queste problematiche devono essere collocate.

5 Le indicazioni costituzionali

Da un punto di vista di diritto costituzionale, alcune ricostruzioni paiono sovraccaricare la portata della libertà di informazione del profilo cosiddetto "passivo", ossia del c.d. "diritto di essere informati"[21]. Posto che è opinabile che tale posizione giuridica integri concretamente un *diritto a* ricevere informazioni corrette o semmai una *libertà da* fattori di ostacolo alla ricezione di informazioni, si deve probabilmente rivisitare l'importanza di quest'ultima declinazione, che invero la nostra Costituzione non tutela espressamente, ancorché la giurisprudenza costituzionale ne abbia fatto riconoscimento[22]. È semmai la Convenzione europea dei diritti dell'uomo a enunciare questo profilo, ma non pare operazione lungimirante, almeno in questa situazione, importare un patrimonio concettuale e giuridico estraneo al dettato della Costituzione al fine di trarne indicazioni e conclusioni che riguardano per l'appunto l'ampiezza delle tutele costituzionali.
In quest'ottica, è stato affermato che la circolazione delle *fake news* frustrerebbe questo profilo passivo coincidente con il diritto a essere informati, inquinando il contenuto informativo e minando alle fondamenta il corretto orientamento dell'opinione pubblica, privandolo di un'informazione veritiera che possa costituire il nucleo e presupposto di ogni giudizio critico. Non sembra condivisibile l'assunto per cui, in definitiva, per poter godere della più ampia libertà di circolare (anche) sul web, un contenuto dovrebbe presentare i connotati sufficienti a soddisfare senza storture un'esigenza informativa[23]. Questo argomento, del resto, tralascia il fondamentale problema della definizione del concetto di "verità" e della difficoltà di esprimere valutazioni in termini di tipo assoluto, nell'alternativa non superabile tra vero e falso. A questo riguardo, il pluralismo informativo è esattamente l'ingrediente, come ricorda la giurisprudenza della Corte costituzionale, che ha consentito di ovviare alle dinamiche non sempre virtuose (in una prospettiva meramente concorrenziale) del *marketplace* dell'informazione. "Più informazione" e soprattutto "di più punti di vista" è sempre stata la ricetta da offrire rispetto, per esempio, al rischio del consolidamento di strutture oligopolistiche e politicamente sensibili.
All'idea che solo le informazioni che soddisfano un'esigenza informativa meritino circolazione, in quanto funzionali al diritto a essere informati, deve dunque opporsi la ricostruzione, ancora una volta, che vede nell'ecosistema dell'informazione un *marketplace* delle idee in cui la capacità di discernimento dell'utente conduce a sottoporre a un giudizio critico i contenuti informativi. E del

[19] Cfr. sul punto della cosiddetta "*collateral censorship*", soprattutto J. Balkin, *Free Speech and Hostile Environments,* in 99 *Columbia Law Review* (1999), 2295 ss.
[20] Si pensi al già richiamato DDL Gambaro, che oltre a prevedere sanzioni penali per la diffusione di notizie false, esagerate e tendenziose o atte a turbare l'ordine pubblico e per la diffusione di notizie false che possono destare pubblico allarme, fuorviare settori dell'opinione pubblica, introduce anche una disposizione *ad hoc* per il contrasto delle campagne d'odio e della campagne volte a minare il processo democratico, tradendo così l'assunto di una comunanza di *ratio* che invero non pare ravvisarsi tra i due problemi al centro del dibattito, ossia la diffusione di *fake news* e di discorsi d'odio.
[21] Per una panoramica generale sul ruolo dell'informazione nell'ordinamento italiano, cfr. C. Chiola, *L'informazione nella Costituzione,* Padova, 1973.
[22] A partire dalle sentt. 105/1972, 225/1974 e 94/1977, fino alle più "recenti" sentt. 157/1987 e 112/1993, maturate, al pari di molte altre, nell'ambito della copiosa giurisprudenza della Corte costituzionale sul regime di monopolio, prima, e oligopolio, poi, nel settore radiotelevisivo.
[23] Paiono quindi del tutto condivisibili le osservazioni espresse da A. Di Giovine, *I confini della libertà di manifestazione del pensiero,* Milano, 1988, 96, in merito alla non immediata rilevanza della dicotomia tra la concezione "funzionale" e quella "individualistica" della libertà di manifestazione del pensiero rispetto al rapporto tra libertà e repressione del diritto di parola: «Non sembra […] corretto contrapporre – in chiave esplicativa delle diverse soglie di tolleranza – la concezione c.d. funzionale della libertà di manifestazione del pensiero (che comporterebbe "che essa sia garantita solo nei limiti della sua utilità storicamente determinata") alla concezione individualistica (in base alla quale la libertà di manifestazione del pensiero sarebbe garantita, al contrario, "al singolo come tale indipendentemente dai vantaggi o dagli svantaggi che possono derivarne allo Stato"), considerandole quasi come sinonimi di concezione "autoritaria" e concezione "liberale" della libertà in questione».

resto, molta della cosiddetta "controinformazione" o delle *fake news* non sono immuni, talvolta, da caratterizzazioni di natura politica; accadde così spesse volte che a promuovere ricostruzioni di accadimenti non veritiere o interpretazioni preorientate siano personaggi che rivestono ruoli e responsabilità politiche. In questa direzione, è importante che le *fake news* possano egualmente e liberamente essere veicolate sul web, nella misura in cui contribuiscono a formare l'opinione critica dei cittadini ma anche degli altri competitori politici rispetto alle idee propagandate da partiti e movimenti. Più informazione, dunque, aiuta a dare risalto all'informazione di qualità e a smentire, tacendo "con i fatti" e non…"con i filtri", le notizie false o tendenziose.

6 Gli interventi sugli ISP

Infine, osserviamo che l'imposizione di forme di controllo (preventivo) da parte delle piattaforme rispetto ai contenuti da loro ospitati non possono agevolmente conciliarsi con l'attuale assetto. Tale incompatibilità non si pone soltanto con il paradigma normativo ma anche con lo stesso modello di business degli operatori, fondato anch'esso sull'estraneità dei *provider* rispetto ai contenuti immessi dai fruitori dei loro servizi. È questa una regola che riflette un equilibrio non insensibile a ragioni di ordine politico, in quanto addebitare agli *Internet service provider* una siffatta responsabilità priverebbe non solo la rete del suo carattere di tendenziale neutralità/libertà, instillando forme di pericolosa censura di matrice privata, ancorché nell'ottica di una prevenzione delle *fake news*, ma scoraggerebbe di molto l'iniziativa economica di questi operatori[24].
Lo stesso approccio tedesco (basato sul *follow the money*) appare problematico in quanto presuppone che la capacità di ottenere profitti da parte di una piattaforma significhi un suo maggiore coinvolgimento (o quantomeno l'esigibilità di una condotta attiva) nella rimozione di contenuti.
La nuova legge tedesca[25], in vigore dal 1 ottobre 2017, individua proprio nei *social network* il proprio campo di applicazione materiale e soggettivo, istituendo a carico dei relativi gestori una serie di obblighi che si collegano all'esistenza di contenuti asseritamente illeciti. Tali obblighi sono declinati su due distinti versanti: per un verso, hanno a oggetto la produzione di rapporti con i quali i gestori dei *social network* sono tenuti a documentare la gestione di contenuti illeciti oggetto di un ingente numero di segnalazioni (più di cento) nel corso dell'anno solare; per altro verso, concernono la gestione dei reclami relativi a contenuti illeciti, da svolgersi secondo una procedura efficace e trasparente. Su quest'ultimo fronte si prevede, in particolare, la rimozione o il blocco di contenuti da effettuarsi entro ventiquattro ore dalla ricezione di reclami se si tratta di contenuti "manifestamente illeciti" ed entro il termine di sette giorni se l'illiceità (non manifesta) del contenuto dipenda dalla falsità del contenuto o dalle circostanze di fatto. Il mancato adempimento a questi obblighi può comportare l'applicazione di ammende fino a 500.000 Euro e, nei casi più gravi, fino a un milione di Euro.
La legge, ancor prima della sua entrata in vigore, ha certamente comportato un cambiamento nella gestione dei contenuti da parte dei *social network*, specialmente nel periodo antecedente le elezioni politiche del 24 settembre 2017[26]. Il modello tedesco si incentra, sulla repressione, più che delle *fake news*, dei discorsi d'odio ma non manca di offrire uno spaccato delle problematiche che ogni eventuale misura di controllo sui contenuti determina rispetto alla fisionomia e al modello di business (nonché di responsabilità) dei gestori delle piattaforme.
Inoltre, la previsione *ope legis* di queste misure provocherebbe un pericoloso precedente, legittimando l'istituzione, figlia anche (non si può negare – il che peraltro non è carattere da riprovare, ma coessenziale alle attività dei legislatori) del contingente sentire rispetto all'esigenza di contrastare la diffusione di notizie false, di misure che, in un'ideale progressione verso il futuro, potrebbero prestarsi per la repressione di altri generi di contenuti.
Da ultimo, prima di entrare nel merito delle modalità attraverso le quali esigere un intervento da parte degli operatori sulle *fake news,* merita di essere svolta una riflessione di carattere generale sulle implicazioni e sulle ricadute della scelta di affidare a soggetti di natura privata funzioni che ridondano una rilevanza pubblicistica.
È bene richiamare, in proposito, la *dissenting opinion* dei giudici Sajo e Tsotsoria nella sentenza della Grande Camera della Corte europea nel caso *Delfi.* La Corte di Strasburgo ha giudicato non

[24] Sull'evoluzione del modello di responsabilità degli ISP nell'interpretazione giurisprudenziale della relativa disciplina offertane da corti nazionali ed europee, si rinvia a M. Bassini, *La rilettura giurisprudenziale della disciplina sulla responsabilità degli Internet service provider. Verso un modello di responsabilità 'complessa'?*, in *Federalismi.it*, 28 novembre 2015 e O. Pollicino, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli* Internet Service Provider, in *ConsultaOnline*, 2014.
[25] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG), n. 536/17, 30 giugno 2017.
[26] Cfr. anche F. Bertolino, *Germania, come sta funzionando la legge anti-fake news di Merkel*, in www.lettera43.it, 6 settembre 2017.

sproporzionata l'interferenza con l'art. 10 della CEDU derivata dalla condanna al risarcimento del danno provocato dalla non tempestiva rimozione da parte di un portale *online* di commenti di terzi di natura diffamatoria.

Ebbene, i due giudici contestano recisamente questa conclusione, ritenendo che la soluzione così prospettata rischi di generare come effetto l'incentivazione di forme di censura privata da parte degli operatori, nel solco di quella *collateral censorship* di cui bene ha parlato in un suo articolo Jack Balkin[27]. In estrema sintesi, se gli ISP fossero obbligati a rimuovere contenuti o comunque fossero considerati responsabili degli stessi, per riflesso condizionato potrebbero implementare strategie di censura privata nel timore di incorrere in sanzioni, il che produrrebbe verosimilmente un effetto al ribasso nella circolazione di informazioni sul web.

Quanto alle possibili modalità per applicare sistemi di filtraggio, si pongono almeno due alternative. E, tuttavia, le opzioni disponibili, per ammissione dello stesso Presidente dell'AGCM Giovanni Pitruzzella[28], che pure si è mostrato aperto a qualche forma di controllo da parte di operatori pubblici o privati sull'assunto che la libertà costituzionalmente tutelata di essere informati osterebbe alla circolazione di notizie false[29], presentano implicazioni critiche non banali.

Da un lato, vi sarebbe l'opzione di incaricare i fornitori di servizi Internet (come i gestori di motori di ricerca o di *social network*) di un controllo *ex ante*, a monte, sul contenuto delle notizie. Soluzione che però presupporrebbe l'esercizio da parte di questi soggetti di una vera e propria responsabilità editoriale, giacché a nessun algoritmo potrebbe affidarsi il compito di selezionare le notizie false nell'alveo delle informazioni processate. Questa circostanza priverebbe gli operatori Internet delle esenzioni di responsabilità per i contenuti trasmessi o memorizzati: una situazione di vantaggio sotto un profilo giuridico che giustifica da un punto di vista economico la redditività dei servizi offerti, senza la quale difficilmente i prestatori offrirebbero egualmente i propri servizi.

Questa proposta, se attuata, rischierebbe di ingenerare le stesse criticità che circondano l'implementazione della sentenza *Google Spain* sul diritto alla deindicizzazione dei dati personali dai motori di ricerca[30]: trasformerebbe, come si è osservato[31], gli operatori Internet in attori paracostituzionali; affiderebbe loro, un tendenziale arbitrio nella definizione dei criteri per la selezione delle notizie; graverebbe di un'ulteriore funzione soggetti che operano secondo un preciso modello di business.

Oltretutto, controvertendo della fondatezza di contenuti informativi, resterebbe un fortissimo spazio di discrezionalità, tale da poter insinuare la trasfigurazione della funzione di selezione in un'attività censoria o comunque svolta secondo un'impostazione "di tendenza" e "orientata". Il tutto in uno scenario assai diverso, idoneo a sovraccaricare ulteriormente il pregiudizio per l'interesse informativo: mentre in *Google Spain* a essere in questione era la rimozione (dai soli motori di ricerca) delle notizie ritenute non più di interesse pubblico, quindi risalenti nel tempo, nel caso delle *fake news* l'incisione riguarderebbe notizie tratte dall'attualità, anzi di cogente attualità, con un fortissimo potere discrezionale, quello di decidere della verità e della falsità delle notizie, concentrato nelle mani di un operatore privato.

Dall'altro lato, si argomenta che un'alternativa potrebbe prevedere tale onere di controllo in forma "istituzionale" da parte di società specializzate, terze rispetto ai fornitori di servizi Internet, Pitruzzella, in proposito, evoca il possibile intervento di istituzioni «terze e indipendenti che, sulla base di principi predefiniti, intervengano successivamente, su richiesta di parte e in tempi rapidi, per rimuovere dalla Rete quei contenuti che sono palesemente falsi o illegali o lesivi della dignità umana»[32]

E nondimeno, due appaiono le principali difficoltà cui questo modello di *governance* dell'informazione in rete potrebbe andare incontro.

---

[27] Cfr. ancora J. Balkin, *op. cit.*, ma soprattutto la *joint dissenting opinion* dei giudici Tsotsoria e Sajó nella pronuncia della Grande Camera CEDU, *Delfi c. Estonia*, ric. 64569/09 , punto 2: «*As Professor Balkin has demonstrated, the technological infrastructure behind digital communication is subject to less visible forms of control by private and public regulators, and the Court has just added another such form to this panoply. Governments may not always be directly censoring expression, but by putting pressure and imposing liability on those who control the technological infrastructure (ISPs, etc.), they create an environment in which collateral or private-party censorship is the inevitable result. Collateral censorship "occurs when the state holds one private party A liable for the speech of another private party B, and A has the power to block, censor, or otherwise control access to B's speech". Because A is liable for someone else's speech, A has strong incentives to over-censor, to limit access, and to deny B's ability to communicate using the platform that A controls. In effect, the fear of liability causes A to impose prior restraints on B's speech and to stifle even protected speech. What looks like a problem from the standpoint of free expression ... may look like an opportunity from the standpoint of governments that cannot easily locate anonymous speakers and want to ensure that harmful or illegal speech does not propagate*».

[28] Secondo Giovanni Pitruzzella, Internet si caratterizza per aver introdotto due innovazioni cruciali. La prima corrisponde all'affermazione di un sistema decentralizzato di produzione dell'informazione, che trasforma qualsiasi utente in potenziale creatore di informazione. La seconda coincide invece con la centralità del ruolo di soggetti come i motori di ricerca e i *social media* (veri e propri *gatekeepers* secondo il Presidente di AGCM) che collegano i produttori e i fruitori di informazione. Cfr. in dettaglio G. Pitruzzella, *Quel filtro necessario per le notizie false sul web*, cit. e *amplius* G. Pitruzzella – O. Pollicino – S. Quintarelli, *op. cit.*, 55 ss.

[29] Tale profilo della libertà di informazione, infatti, dovrebbe intendersi come garanzia di un'informazione corretta e veritiera, non *biased* o inquinata, in quanto si tradurrebbe nella pretesa dei fruitori di informazioni a non essere ingannati.

[30] CGUE, C-131/12, *Google Spain* (2014).

[31] Cfr. O. Pollicino, *Google rischia di "vestire" un ruolo paracostituzionale*, in www.ilsole24ore.it, 14 maggio 2014.

[32] G. Pitruzzella, *Quel filtro necessario per le notizie false sul web*, cit.

Per un verso, resterebbero intatte le criticità sopra segnalate rispetto all'ipotesi in cui il filtraggio sia svolto dagli stessi motori di ricerca o gestori di piattaforme *online*, con particolari motivi di preoccupazione legati alla trasparenza dell'attività svolta, trattandosi di soggetti investiti *ad hoc* di questa funzione.
Ma, per altro verso, il ricorso a questi soggetti istituzionali potrebbe generare problematiche del tutto peculiari rispetto alla scelta dell'intermediario, ai criteri potenzialmente diversi cui il rispettivo operato potrebbe informarsi, e perfino alla composizione di questi organismi. Alimentando, così, come è accaduto recentemente, ipotesi o ricostruzioni al limite del bizzarro, per indulgere in un eufemismo. Proposte sulle quali, per amore di scientificità, si ritiene opportuno non spendere alcun tempo[33].

7 Qualche bilancio

Quello delle *fake news* appare, allora, un tema antico, che non deriva davvero da Internet quanto dalla progressiva erosione delle situazioni di "oligopolio" nel mercato dell'informazione. Dietro le riflessioni sull'opportunità di introdurre misure che rispondano all'esigenza di depurare il web di notizie false sembra agitarsi, in realtà, un più generale atteggiamento di timore rispetto a una tecnologia nuova (ma non così nuova, dato che vanta almeno venti anni) verso la quale i consociati non sembrano possedere una del tutto piena padronanza. È una "paura del nuovo" che cela la difficoltà di decifrare fenomeni in cui la combinazione tra regola e tecnica, o per meglio dire tra regola tecnica e regola giuridica sfugge a una comprensione immediata.
Riflettendo sull'attualità ed emancipando la riflessione da una visione Internet-centrica, è possibile osservare come non siano mancati, nel passato, e non manchino tuttora esempi poco commendevoli in cui a farsi veicolo di notizie prive di fondamento, talvolta sapientemente manipolate per servire l'interesse di un pubblico selezionato, sono stati in realtà i mezzi di informazione tradizionali[34], e segnatamente quotidiani cartacei.
Dove ha però un senso immaginare tutele nuove? Forse rispetto alla manipolazione dell'informazione da parte di gruppi di potere che possono condizionare l'opinione pubblica tramite i nuovi mezzi: si pensi al dibattito sulle malattie portate dai migranti e sull'utilità dei vaccini, tra gli altri.
Si deve tuttavia elaborare se la miglior risposta a queste istanze provenga dalla definizione di nuove fattispecie oppure dalla promozione di nuovi obblighi. Quest'ultima appare una soluzione agevole da percorrere, per esempio ove si traduca nell'imporre ai *social network* obblighi di identificazione che permettano a terzi di verificare la provenienza e la fonte delle informazioni diffuse. Questo rimedio appare coerente, del resto, con la stessa fisionomia costituzionale della libertà di espressione, il cui esercizio è permesso "a volto scoperto".
Un'altra ipotesi da considerare potrebbe riguardare il rafforzamento del diritto di replica, di rettifica, e l'implementazione di meccanismi di segnalazione di notizie false che non siano "dall'alto" ma semmai scaturiscano, nella medesima ottica del *marketplace* di stampo liberale, dal confronto con gli utenti. In questa direzione procede da tempo, per esempio, Wikipedia, che ha dimostrato caratteri di trasparenza e *accountability* nella gestione della pubblicazione delle informazioni e di eventuali rettifiche o modifiche, pur essendo fondata esclusivamente su una dinamica di costruzione "dal basso" del sapere, secondo una logica di disintermediazione pura.
La via più opportuna da intraprendere sembra dunque quella della trasparenza, unita a un apporto sempre più ampio e pluralistico di informazione e scevra da qualsiasi logica paternalistica che consideri il falso in sé come un comportamento illecito, aprendosi alla prospettiva statunitense che intravede il vero test dell'autorevolezza nello scambio dialettico.
Una simile prospettiva di risoluzione del problema appare del resto l'opzione maggiormente compatibile con il sistema costituzionale, che incarna lo schema di una democrazia tollerante e una visione ottimistica su un esercizio consapevole dei diritti fondamentali proclamati dalla nostra Carta da parte del popolo, munito di adeguate capacità di discernimento. Ogni diversa opzione tradirebbe, al contrario, l'avvicinamento a un modello diverso, più simile alla cosiddetta democrazia protetta o militante, che si caratterizza per il timore diffuso di un abuso dei diritti oltre il limite costituzionalmente tollerato e per la conseguente risposta in chiave "etica" da parte dello Stato.

[33] Senza spendere nomi (ci sia concesso…), si vv. *"Una giuria popolare per le balle dei media": Beppe Grillo contro le bufale su giornali e tv, a difesa di Internet*, in *Huffington Post*, 3 gennaio 2017.
[34] L'esempio più recente deriva probabilmente dall'uso del titolo "Dopo la miseria portano le malattie" impiegato da un quotidiano nazionale con l'intento di collegare, senza nessuna argomentazione scientifica sull'esistenza di un nesso eziologico, la morte di una bambina per malaria con l'incremento dei flussi migratori registrati in Italia negli ultimi mesi.

Una prospettiva che, per il presente ma soprattutto per il futuro non sembra opportuno abbracciare e che, a ben vedere, sembra entrare in tensione con il paradigma di uno stato liberal-democratico. A volte, essere ottimisti, specie nelle congiunture meno favorevoli, non guasta.

Fake News, Internet and Metaphors (to be handled carefully)*

The metaphor of the free marketplace of ideas is frequently referred to as a crucial argument to support a liberal view of freedom of speech and contrast the enforcement of measures aimed at preventing fake news. This metaphor is subject to critical remarks for three different reasons.
First of all, whilst it may be the case that the problem of scarcity of technical resources does not affect the Internet, our attention and time continue to be scarce "products".
Secondly, it is reasonable to ask whether the marketplace of ideas metaphor is well suited to the scope (and limits) of protection for free speech under the European constitutionalism paradigm.
Thirdly, metaphorical language fits in very well with legal reasoning , but it should be handled properly (and with care).

Oreste Pollicino
Full Professor of Constitutional Law, Bocconi University

"The internet is a new free marketplace of ideas".

This is the preferred metaphor[1] of those who within scholarly and public debate take the view that the issue of fake news need not be addressed (and confronted) by public authorities (and public law). The main idea behind this thesis is that whereas in the world of atoms, as Justice Holmes wrote in 1919, the "best test of truth is the power of the thought to get itself accepted in the competition of the market"[2], this is even more true in the world of bits, as the internet is amplifying the free exchange of and competition between ideas and opinions. Consequently, according to the marketplace of ideas paradigm, if it is true that under the First Amendment there is "no such thing as a false idea"[3] in the material world, this is even truer in the digital word, thanks to the enhanced opportunity to express thoughts. In other words, public authorities should not have any role in dealing with the ever growing phenomena of fake news on the internet, because web users are (optimistically) supposed to have all the tools they need in order to select the most convincing ideas and true news, disregarding news that is not convincing or fake. This constitutes an expression of complete trust in the capacity for selfcorrection of the market for information.

Is there any alternative reading of the possible relationship between public powers, regulation, and truth on the internet? Or should public law decline to play any role in the matter? In order to try to answer to the questions mentioned above, it is necessary to take a step back: what is hidden behind the label fake news? A first tentative answer could include within the definition all information or news that shares a certain level of falsehood. Such information may be entirely made up or only partially false.

Obviously, as for the right to be forgotten saga and many other issues which are experiencing a second lease of life in the digital era, the debate surrounding fake news is not new to the age of the internet. It is "just" a question of the different degree of relevance and intrusiveness of this issue. It is evident that the global nature of the "new" technology, the fact that virtually every internet user is able to became an editor and to spread and (especially) share (even false) information and the corresponding much greater potential impact of falsehoods on the internet are exponentially amplifying the urgent need to verify the sources of information in the post-truth digital era.

The real challenge is how such a process of verification should be conducted

According to the champions of the free market of ideas metaphor, since by definition scarcity of resources is an analogue and not a digital limit, with the result that there is no need to protect pluralism of information on the internet, legal rules (and especially public law) should take a step back in the name of the alleged self-corrective capacity of the information market. Just as the economic market knows no test of product "validity" but allows demand to drive supply, relying on the market to distinguish between viable and shoddy products, the best way of dealing with the phenomenon of fake news in the information market is to secure the widest possible dissemination of all news, including news from contradictory and unreliable sources.

The thesis is not so convincing, in my opinion, for at least three reasons.

First of all, whilst it may be the case that the problem of scarcity of technical resources does not affect the internet, our attention and time continue to be scarce "products". In fact, while the amount of information available is growing, the 24 hours in the day cannot be extended. Against this background, when faced with this information overload the temptation for users will be to search for news, information and ideas that enhance their previous thoughts and preferences, leading to the process of group polarisation succinctly described by Cass Sunstein[4]. Put it differently, in the world of bits, much more than in the word of atoms, deliberation tends to move groups, and the individuals comprising them, towards a more extreme point in the direction indicated by their own predeliberation judgments. The result seems to be that, quite paradoxically, despite (or perhaps better, precisely due to) the unlimited amount of information on the internet, there is a less pluralistic exchange of different opinions than in traditional media where the scarcity of sources is still an issue.

Secondly, it is reasonable to ask whether the marketplace of ideas metaphor is well suited to the scope (and limits) of protection for free speech under the European constitutionalism paradigm.

First, as is well known, protection for freedom of expression in Europe is more limited than in the US. Regarding this issue it is sufficient to compare the wording of the First Amendment of the US

---

* Questo editoriale è stato pubblicato nel n. 1/2017 della Rivista Italian Journal of Public Law, che l'Autore ringrazia per la gentile concessione.

1 US Supreme Court, *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

2 Dissenting opinion of Justice Holmes in the US Supreme Court case *Abrams v. United States*, *Abrams v. United States*, 250 U.S. 616 (1919).

3 US Supreme Court, *Gertz v. Welch*, 418 U.S. 323 (1974).

4 C. Sunstein, *Republic.com*, Princeton, 2002.

Constitution with Article 10 of the European Convention on Human Rights. However, it is not simply a question of differences in scope, but also of difference in focus. Whilst the First Amendment addresses mainly the active dimension to the right to express freely one's own thoughts, Article 10 of the European Convention (but also Article 11 of the Charter of Fundamental Rights of the European Union) emphasises the passive dimension to the right to be pluralistically informed. In this respect, it could be argued that fake news is not constitutionally covered by the European vision of free speech. Or to put it differently, the European courts would find it very difficult to accept the view of the US Supreme Court according to which, as alluded to above, "Under the First Amendment there is no such thing as a false idea. However pernicious an opinion may seem, we depend for its correction not on the conscience of judges and juries but on the competition of other ideas"[5].
Thirdly, metaphorical language fits in very well with legal reasoning[6], but it should be handled properly (and with care).
Metaphor implies knowledge transfer across domains (from the Greek *meta pherein*, to "carry over"). This means that we have two relevant constitutive domains: the source domain and the target domain. The free market of ideas metaphor carries over from the source domain of economic activity to the target domain of speech a systematic set of entailments that supersedes the limitations of the older free speech model. In order to understand it fully, it is important not to forget the features of the source "market" domain when Holmes used the metaphor in 1919 and the US Supreme Court subsequently adapted it to the internet in 1997. Holmes wrote in a period of lasser faire Capitalism, in which the liberal state and market competition were at their zenith. If Holmes was sceptical about any external verification of the truth and removal of news proven to be false, the concept of a free market provided a meaningful alternative model for the notion that truth, just as economic wellbeing, could result from competition between (true and false) ideas and information. Similarly, when the US Supreme Court borrowed the metaphor, referring to the internet as the "new market place of ideas", the economic market of the web (during its period of genesis) was absolutely free and not in any way affected by dominant positions, not to speak of monopolies or oligopolies. Within this context, the metaphor of the free marketplace of ideas and the proposed test for the truth (competition in the absence of any public control) made perfect sense. By contrast, today the same metaphor seems to completely decontextualised given that the economic market, as the source domain from which the metaphor has been taken, is far from "free": as is well known in the DG Competition in Brussels and in every national competition authority, the internet is characterised by huge market failures which require not only ex post intervention but also ex ante, by public authorities. Against this background, if fake news is arguably the most significant and pervasive source of failure in the marketplace of ideas, one can surely not exclude the possibility of intervention by public authorities because, in contrast to the US Supreme Court's definition of the Internet as the "new free marketplace of ideas", the source domain of the digital relevant market is anything but a free market, being characterised by economic concentration and the strength of (a few) private operators.
Nobody is advocating for a "public tribunal of the true" or for enhancing the liability regime of new (and old) social platforms.
The only point should be quite clearly made is that metaphors (also) in digital law should be managed with care. Otherwise the concrete risk is, as it has been tried to prove above, to be lost in legal metaphors.

[5] US Supreme Court, *Gertz v. Welch*, 418 U.S. 323
[6] See from a US perspective, S.L. Winter, *A clearing in the forest. Law, life and Mind*, Chicago, 2001 and more than thirty years earlier, from a European perspective, A. Giuliani, *La nuova retorica e la logica del linguaggio normativo*, in *Rivista internazionale di filosofia del diritto*, XLVII, 1970, 374 ss.

Il contrasto alla disinformazione in rete tra logiche del mercato e (vecchie e nuove) velleità di controllo

The Fight Against Fake News Online Between Market Principles and (Old and New) Forms of Control

Marco Cuniberti
Professore associato di Diritto costituzionale presso l'Università degli Studi di Milano

Abstract

Il contributo affronta il problema della disinformazione in rete, e degli strumenti che possono essere messi in campo nel tentativo di arginare il fenomeno: premesse alcune notazioni fortemente critiche sull'atteggiamento dei media c.d. *mainstream* e del mondo politico, con particolare riguardo ad un recente disegno di legge e ad una risoluzione del Parlamento europeo in materia, e dopo aver espresso perplessità sul reiterato utilizzo, in questo ambito, della metafora del "*free marketplace of ideas*", l'autore si sofferma, in particolare, sul ruolo che in tale attività di contrasto può essere svolto dai grandi intermediari privati (in particolare motori di ricerca e *social network*), sulla necessità di mantenere la distinzione tra informazione professionale e semplice libertà di espressione e, infine, sulla necessità di ripensare la stessa nozione di pluralismo nel mondo della rete.

The article focuses on the problem of the spread of fake news on the Internet and the possible legal remedies to tackle it. Some critical remarks are brought forward with respect to the attitude of mainstream media and political actors. Particularly, the author explores some concerns regarding a bill introduced in the Italian Parliament and a resolution of the European Parliament. After having criticized the recurring reference to the metaphor of the free marketplace of ideas in this field, attention is paid to three factors, namely: the role that intermediaries (including social network and search engine providers) may play to contrast the spread of fake news, the crucial difference between professional information and "simple" exercise of freedom of speech, and the need to revisit the notion of pluralism in accordance with the characteristics of the Internet.

Sommario

Internet
disinformazione in rete
fake news
libertà di espressione
responsabilità degli ISP

1 Informazione, disinformazione, controinformazione tra "vecchi" e "nuovi" media.

A dispetto della perdurante convinzione che il tramonto del novecento abbia coinciso con la fine delle ideologie, il mondo contemporaneo è un mondo molto più ideologico di quanto non si sia portati a ritenere: e uno dei settori in cui questo approccio ideologico è più evidente e pervasivo è rappresentato dalla percezione delle nuove tecnologie e del loro impatto sulla società e sulla esistenza umana.

Accade così che, nel mondo di internet, ciò che (ideologicamente) viene rappresentato come la lotta tra progresso e reazione, o tra libertà e oppressione, in realtà sia solo la lotta tra (vecchi e nuovi) centri di potere e di interesse: così, ad esempio, la neutralità della rete, spesso invocata in nome e a garanzia della libertà degli utenti, è stata (e rimane) anche, e forse soprattutto, un'arma utilizzata nello scontro tra vecchi e nuovi monopolisti del mercato delle comunicazioni, tra i gestori delle infrastrutture e i c.d. "over the top" [1].

Anche il problema, oggi così dibattuto, della disinformazione in rete appare caratterizzato dalla stessa distorsione ideologica: per rendersene conto, è sufficiente chiedersi per quale motivo il tema sia diventato "virale" solo nel 2016, nonostante la presenza di massicce dosi di disinformazione in rete non rappresenti certo una novità [2].

Non si può fare a meno di notare, infatti, che il 2016 è stato contrassegnato da almeno due eventi (la c.d. Brexit e l'elezione di Donald Trump alla presidenza U.S.A.) che hanno mostrato, al di là di ogni dubbio, le crescenti difficoltà che i mass media tradizionali incontrano nel leggere, interpretare e comprendere le trasformazioni di larghe fasce dell'elettorato: non solo, ma i due eventi hanno anche definitivamente accertato le difficoltà che gli stessi mass media incontrano nell'orientare e nel condizionare le scelte degli elettori, dal momento che non è un mistero che, in entrambi i casi, le decisioni emerse dalle urne hanno frontalmente smentito le aspettative e i desiderata della stragrande maggioranza dei media c.d. "*mainstream*", dei loro esponenti di spicco e dei centri di interesse di cui questi sono espressione.

Tali vicende hanno quindi reso evidente, forse per la prima volta in modo così netto, che i grandi media tradizionali non hanno più il controllo della "opinione pubblica": più ancora, forse, hanno segnalato che la stessa "opinione pubblica", come ambiente (più o meno virtuale) costruito dai media c.d. mainstream e dai centri di potere e di interesse cui questi danno voce, non esiste più, e che al suo posto si viene delineando un universo disperso e frammentato che i media non sono più in grado di capire, strutturare e, soprattutto, orientare [3].

A fronte di ciò, la reazione del mondo che gravita attorno ai mass media tradizionali (o mainstream che dir si voglia), fatto salvo qualche sporadico spunto di riflessione e di autocritica, è principalmente consistita nello scatenare una feroce campagna di denuncia dei pericoli della disinformazione e della manipolazione in rete: una campagna, però, non solo un po' tardiva, posto che il problema non nasce certamente ora, ma anche leggermente sospetta, dal momento che tende a dimenticare e a far dimenticare le pesanti responsabilità che gli stessi media c.d. mainstream hanno avuto, nel recente passato e sino ad oggi, nella costruzione di gigantesche operazioni di disinformazione di massa [4].

Il carattere ideologico dell'attuale polemica contro la disinformazione in rete risiede appunto nella sua attitudine a dissimulare la vera natura dello scontro in atto: che non è tanto uno scontro tra informazione "buona" e "cattiva", tra informazione e disinformazione, quanto una guerra tra vecchi e nuovi media - e vecchi e nuovi centri di potere - per il controllo dell'opinione pubblica, scatenata dal fatto che, per la prima volta, la informazione e disinformazione on line sembrano più efficaci, nell'o-

---

[1] Se appena si prova ad andare oltre il mito della rete "stupida" che contrassegna la fase pionieristica di internet (cfr. L. Lessig, *The Future of Ideas* (2001), trad. it *Il futuro delle idee,* Milano, 2006, 42), infatti, il dogma secondo cui la rete non deve operare distinzioni tra contenuti e tra i relativi fornitori appare uno sbiadito relitto del passato, in una rete dominata da enormi e potentissimi intermediari (a cominciare da *social network* e motori di ricerca) il cui ruolo è decisivo nell'accrescere o comprimere la visibilità di determinati contenuti, sicché l'unico significato che il principio di neutralità conserva, nell'attuale scenario, è quello di una leva ideologica attraverso la quale i c.d. "*Over the Top*" (OTT), oggi i veri signori della rete, proteggono e consolidano il proprio dominio a scapito degli operatori di rete.

[2] Per una ricca rassegna al riguardo cfr. ad es. E. Morozov, *The Net Delusion. The Dark Side of Internet Freedom* (2011), trad. it. *L'ingenuità della rete. Il lato oscuro della libertà di internet,* Torino, 2011.

[3] Mutuando il titolo di un fortunato libro di E. Parisier (*The Filter Bubble. What The Internet Is Hiding From You* (2011), trad. it. *Il Filtro. Quello che Internet ci nasconde,* Milano, 2012), si ragiona infatti di una "*bubble democracy*", una "democrazia delle bolle" che avrebbe preso il posto della "democrazia del pubblico" segnata dalla centralità del *medium* radiotelevisivo, a partire dagli anni cinquanta, la quale a sua volta sarebbe succeduta alla democrazia dei partiti, caratterizzata dal predominio della stampa di opinione come strumento di formazione e orientamento dell'opinione pubblica (D. Palano, La bolla mortale della nuova democrazia, in Il Foglio, 1°maggio 2017).

[4] A cominciare da quella che a buona ragione si può definire "la madre di tutte le *fake news*", quella cioè riguardante le famigerate quanto fantomatiche "armi di distruzione di massa" di Saddam Hussein, addotte a pretesto per scatenare una guerra di aggressione che ha causato, secondo le stime più prudenti, alcune centinaia di migliaia di vittime, in larga parte civili, oltre alla perdurante destabilizzazione dell'Iraq.

rientare, condizionare e manipolare l'opinione pubblica, di quelle veicolate dai media tradizionali.
Tutto ciò, peraltro, non dovrebbe stupire e forse neppure allarmare più di tanto, se solo si considera che, a partire dalla sua nascita attorno al XVIII secolo, il concetto di "opinione pubblica" non designa una realtà esistente in natura, ma appunto, un complesso ecosistema, sensibile all'azione di una pluralità di fattori di ordine economico, sociale, giuridico e tecnologico, che chiaramente si evolve e si trasforma con l'evoluzione della società, della sua struttura economica e giuridica, e ovviamente degli strumenti tecnologici: sicché, se da un lato non è probabilmente mai esistita una sola, generica ed onnicomprensiva "opinione pubblica", ma una pluralità di "sfere pubbliche" in rapporto di costante tensione, competizione ed influenza reciproca, d'altro canto ogni trasformazione della struttura economica, giuridica e tecnologica della società, intervenuta dall'avvento della società industriale sino ad oggi, ha di volta in volta messo in crisi l'idea e l'immagine dominante della "opinione pubblica", imprimendo ad essa radicali trasformazioni [5].
Se è così, è possibile che ci si trovi di fronte a uno dei tanti momenti in cui, come più volte è accaduto dalle sue origini ad oggi, la nozione dominante di "opinione pubblica" è entrata in crisi, per poi ricomporsi e ristrutturarsi conformandosi alle evoluzioni del tessuto economico e tecnologico: ciò che invece può suscitare qualche preoccupazione in più è il fatto che alle scomposte, ma in fin dei conti comprensibili, reazioni che vengono da una parte del mondo dell'informazione si affianchino prese di posizione decisamente più inquietanti da parte del mondo politico.

2 Due recenti (ed inquietanti) risposte dal mondo politico.

Negli ultimi mesi, infatti, il problema della disinformazione on line ha attratto anche l'attenzione del mondo politico: un mondo che, sin dall'avvento di internet, non si è mai contraddistinto per lucidità e preveggenza nell'approccio ai temi della rete e alle nuove tecnologie, e che anche in questa occasione non è sembrato dar prova di particolare equilibrio e lungimiranza.
Due documenti meritano di essere, pur brevemente, analizzati, perché, al di là degli esiti pratici (auspicabilmente nulli) che sono destinati a produrre, testimoniano tutti i limiti culturali dell'approccio del potere politico a questo tipo di tematiche: si tratta del recente disegno di legge A.S. 2688, presentato al Senato della Repubblica il 7 febbraio 2017 e avente come prima firmataria la senatrice Adele Gambaro, e della risoluzione approvata dal Parlamento europeo il 23 novembre 2016, sulla comunicazione strategica dell'UE per contrastare la propaganda nei suoi confronti da parte di terzi.
Il disegno di legge A.S. 2688, recante «disposizioni per prevenire la manipolazione dell'informazione *online*, garantire la trasparenza sul web e incentivare l'alfabetizzazione mediatica», si propone di dare attuazione alle preoccupazioni espresse, tra l'altro, dall'Assemblea parlamentare del Consiglio d'Europa circa «il numero di campagne mediatiche *online* miranti a fuorviare settori dell'opinione pubblica, attraverso informazioni intenzionalmente tendenziose o false, l'istigazione all'odio contro singoli individui e anche attacchi personali, spesso in ambito politico, volti a minare il regolare svolgimento dei processi democratici»; con l'esplicito fine di contrastare il diffondersi dei «movimenti populisti», il disegno di legge si propone quindi, sulla scia di analoghe iniziative intraprese in Francia e Germania, di dare vita a forme di «collaborazione» tra il potere politico e i «colossi del web», finalizzata a mettere in atto un «costante monitoraggio» della rete al fine di rimuovere contenuti

[5] Fondamentale è ancora oggi il riferimento a J. Habermas, *Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellshaft* (1962), trad. it. *Storia e critica dell'opinione pubblica*, Roma-Bari, 2005: alla luce di queste peraltro risalenti notazioni, dovrebbe forse ridimensionarsi anche l'impatto devastante che viene ascritto alla c.d. "*bubble democracy*" (v. *supra,* n. 3): le "bolle", o "sfere" che dir si voglia, nella struttura dell'opinione pubblica, ci sono sempre state; quello che cambia è probabilmente il modo, e la velocità, con cui si formano e si dissolvono, e il fatto che, diversamente dal passato, appare difficile inquadrare simili fenomeni secondo dinamiche sociologiche classiche, e in particolare attraverso le lenti della nozione di classe.

«falsi, pedopornografici o violenti» [6].
Al di là dell'esplicito riferimento ai «movimenti populisti», che sembrerebbe tradire le finalità politiche di questa auspicata forma di controllo della rete, le maggiori perplessità che simili propositi suscitano attengono a due distinti profili.
In primo luogo, è evidente che un monitoraggio di tale estensione richiederebbe o l'utilizzo di strumenti informatici, di "filtri", insomma, basati sull'utilizzo di determinate parole chiave, oppure la collaborazione degli utenti attraverso appositi strumenti di "segnalazione" dei contenuti inappropriati: sono strumenti che già esistono per l'individuazione di contenuti pornografici o violenti, e che negli ultimi mesi, come vedremo tra poco, si è cercato di esportare anche sul terreno della lotta alle c.d. f*ake news*; sono però anche strumenti la cui efficacia suscita qualche dubbio, è che non è escluso possano portare alla eliminazione di contenuti del tutto inoffensivi.
In secondo luogo, ma in stretta correlazione con quanto appena osservato, è impressionante che si accomuni la semplice «falsità» ai «contenuti pedopornografici o violenti»: a prescindere dal fatto che non sempre la falsità di un contenuto, diversamente dal suo carattere pedopornografico o violento, è rilevabile ictu oculi, non pare corretto mettere sullo stesso piano comportamenti tra i quali dovrebbe quanto meno sussistere una differenza in termini di gravità e di pericolosità sociale.
L'idea di sanzionare la falsità della notizia in sé, indipendentemente da ogni profilo ulteriore di danno sociale, trova poi espressione pratica nell'art. 1 del disegno di legge, che introducendo l'art. 656 – bis del codice penale, punisce con l'ammenda fino a 5.000 euro, salvo che il fatto costituisca più grave reato, «chiunque pubblica o diffonde, attraverso piattaforme informatiche destinate alla pubblicazione o diffusione di informazione presso il pubblico, con mezzi prevalentemente elettronici o comunque telematici, notizie false, esagerate o tendenziose che riguardino dati o fatti manifestamente infondati o falsi».
A parte la difficoltà di giustificare razionalmente il diverso trattamento di chi divulghi tali notizie attraverso strumenti elettronici o informatici rispetto a chi faccia uso di strumenti differenti, ciò che colpisce è che l'illecito consiste nella mera falsità della notizia, senza che sia richiesto alcun ulteriore profilo di dannosità o pericolosità della condotta: ora, se è vero, come sostiene la nostra migliore dottrina, che l'art. 21 non copre la deliberata e consapevole diffusione di informazioni false [7], è anche vero, d'altra parte, che nel nostro ordinamento, la sola e semplice affermazione di un fatto falso, che non sia preordinata o idonea ad arrecare un danno ingiusto o un ingiusto svantaggio ad altri, potrà rilevare al più – se proveniente da un giornalista - sotto il profilo deontologico, ma non comporta normalmente né responsabilità civile né sanzioni penali; il falso in sé, in altri termini, non è manifestazione del pensiero, ma non è neppure reato, rientrando piuttosto in una zona di irrilevanza giuridica [8].
Con tale previsione il disegno di legge introduce quindi una novità rilevante, con l'ulteriore particolarità che tale novità non è estesa ad ogni forma di espressione, ma solo a quelle che si avvalgono di strumenti elettronici o telematici, e che la norma non si applica a chi eserciti professionalmente

[6] Si legge infatti nella presentazione del d.d.l.: «la libertà di espressione non può trasformarsi semplicemente in un sinonimo di totale mancanza di controllo, laddove controllo, nell'ambito dell'informazione, vuol dire fornire una notizia corretta a tutela degli utenti. È infatti sotto gli occhi di tutti il danno che può comportare, nell'era dell'informatizzazione, la diffusione di una notizia sbagliata e distorta. Peggio ancora se manipolata. Le notizie false, o *fake news* o bufale, ci sono sempre state, ma non sono mai circolate alla velocità di oggi. Per questo non è più rinviabile un dibattito serio in questo senso. Se l'informazione diventa disinformazione i mezzi di comunicazione di massa possono essere utilizzati a fini di propaganda con il rischio che notizie appositamente distorte vengano strumentalmente adoperate per influenzare l'opinione pubblica. Questo perché con il diffondersi dei *social media* il pericolo di contaminare internet con notizie inesatte e infondate o, peggio ancora, con opinioni che seppur legittime rischiano di apparire più come fatti conclamati che come idee, è in crescita esponenziale. […] È dunque importante disciplinare la vita *online* come la vita *offline*, che si parli di cyberbullismo o di divulgazione di notizie false, bisogna puntare ad usare gli strumenti già a disposizione nel nostro ordinamento giuridico spostando l'attenzione dal reale al virtuale perché gli attori sono sempre gli stessi: i cittadini che, come nella vita reale, hanno il diritto di essere tutelati anche in quella virtuale. Si tratta di un dibattito ormai in fase avanzata in tutte le democrazie occidentali che investe i colossi di internet, il cui impegno è rivolto alla ricerca di nuovi strumenti in grado di filtrare e garantire l'autenticità delle notizie. Di pari passo all'incremento dei consensi dei movimenti populisti nei Paesi occidentali è accresciuta la preoccupazione che le *fake news* possano essere diffuse e poi cavalcate a fini politici. La reazione di Francia e Germania è stata quasi immediata: oltre all'avvio di programmi specifici volti a verificare l'attendibilità delle notizie che circolano sul web, è emersa l'esigenza di intervenire sotto il profilo normativo per ottemperare alla duplice necessità di effettuare un costante monitoraggio dei contenuti presenti in rete, per poi procedere alla rimozione di quelli considerati falsi. In particolare, in Germania è stata presentata una proposta di legge che obbliga i *social media* ad eliminare i contenuti falsi entro 24 ore dalla loro individuazione. […] Bisogna avviare un simile percorso anche in Italia attingendo agli strumenti che già ci sono: le leggi contro le informazioni false, illegali e lesive della dignità personale, ripensandole per il web. Ciò consentirebbe ai colossi della rete l'uso di selettori *software* per rimuovere i contenuti falsi, pedopornografici o violenti».

[7] Per tutti, cfr. già C. Esposito, *La libertà di manifestazione del pensiero nell'ordinamento italiano,* Milano, 1958, 36, nonché più recentemente A. Pace, in A. Pace-M. Manetti, *La libertà di manifestazione del proprio pensiero* (commento all'Art. 21 Cost.), in *Commentario della Costituzione,* Bologna – Roma, 2006, 89.

[8] Per usare le parole di A. Pace, *La libertà,* cit., loc. cit., che a sua volta riprende il citato scritto di C. Esposito, il fatto che l'art. 21 non copra «i fatti soggettivamente falsi […] non significa che la manifestazione di tali fatti sarebbe vietata, ma […] che non è costituzionalmente protetta. Il legislatore è pertanto libero di disciplinare le manifestazioni di pensiero non corrispondenti alle proprie interiori persuasioni; e quindi vietarle e punirle purché ricorrano due condizioni: *a)*, che sia «raggiunta la prova della divergenza della espressione dall'interiore pensiero»; *b)* che tale divergenza possa danneggiare la pubblica fede ovvero pregiudicare interessi (giuridicamente protetti) dei singoli o della collettività».

l'attività giornalistica o editoriale [9]: con il che si giunge al paradosso per cui l'operatore professionale, sul quale sino ad oggi si ritiene incombano maggiori responsabilità in relazione al rispetto dei doveri deontologici, verrebbe a godere, all'opposto, di un trattamento di favore [10].

La pena aumenta, poi, arrivando a contemplare anche la misura detentiva, se le notizie false o esagerate sono tali da «destare pubblico allarme», o se si collegano ad una «attività tale da recare nocumento agli interessi pubblici o da fuorviare settori dell'opinione pubblica, anche attraverso campagne con l'utilizzo di piattaforme informatiche destinate alla diffusione *online*»; e le sanzioni aumentano ulteriormente, arrivando alla reclusione non inferiore a due anni e all'ammenda fino a 10.000 euro, per chi «si renda responsabile di campagne d'odio contro individui o di campagne volte a minare il processo democratico, anche a fini politici» [11].

Ora, al di là del fatto che taluni di questi comportamenti (come la pubblicazione di notizie false, esagerate o tendenziose, tali da turbare l'ordine pubblico, o lo svolgimento di campagne d'odio) sono già sanzionati da altre norme [12], e al di là della perplessità che suscita il recupero di categorie come quella di «disfattismo politico» [13], ciò che appare inaccettabile in simili disposizioni è l'assoluta vaghezza ed indeterminatezza di espressioni come «recare nocumento agli interessi pubblici» o «minare il processo democratico, anche a fini politici».

E' persino inutile evidenziare come la reviviscenza di simili categorie evochi periodi oscuri della nostra storia: ed è impressionante che, per cercare di giustificare simili compressioni alla luce del disposto dell'art. 21 della costituzione, nella relazione introduttiva addirittura si aggravi il danno, e, non trovando di meglio che rifarsi ad una sentenza della cassazione del 1956, si evochi, come limite alla libera manifestazione del pensiero, non solo il dovere del cittadino «di non destare pubblico allarme», ma anche quello «di non denigrare all'estero la propria patria con notizie false, esagerate e tendenziose sulle condizioni interne» e la «esigenza dello Stato, come persona giuridica di diritto internazionale, qualunque sia il suo ordinamento politico, di tutelare il suo credito e il suo prestigio all'estero e di difendersi dall'opera nociva dei suoi cittadini» [14].

Altre previsioni del disegno di legge, come quelle sugli obblighi di comunicazione e sulla rettifica, se pure esprimono esigenze degne di apprezzamento, appaiono formulate in maniera tale da creare dubbi sulla loro effettiva utilità [15] e da configurare un aggravio inutile e sproporzionato a carico dei gestori di siti e piattaforme [16]; altre, ancora, impongono obblighi di rimozione di contenuti, a seguito di semplici richieste di privati [17], che, oltre ad essere in contrasto con le previsioni della vigente disciplina nazionale e comunitaria [18], sembrano basarsi su un sostanziale travisamento dei principi affermati in materia di diritto all'oblio nella sentenza *Google Spain* della Corte di iustizia UE

[9] Prevede infatti il comma 3 dell'art. 1 del disegno di legge che «l'articolo 656-*bis* del codice penale, introdotto dal comma 1 del presente articolo, non si applica ai soggetti e ai prodotti di cui alla legge 8 febbraio 1948, n. 47, e di cui all'articolo 1, comma 3-*bis*, della legge 7 marzo 2001, n. 62».

[10] Nella presentazione del disegno di legge, si ritiene di giustificare tale esito paradossale osservando che, mentre «i mezzi di comunicazione a stampa, le emittenti radiotelevisive tradizionali e le testate giornalistiche *online* sono (…) editorialmente responsabili dei loro contenuti», invece, nel caso di «notizie diffuse sul web senza alcun criterio professionale […], chiunque […] può dire quello che vuole, per la più che legittima libertà di espressione»: con il che, evidentemente, si confondono indebitamente due piani (quello della assunzione della responsabilità e quello della definizione dell'illecito) che dovrebbero rimanere distinti.

[11] Così dispone l'art. 2 del disegno di legge che introduce l'art. 265 – *bis* e *ter* c. p.

[12] Ad esempio dall'art. 656 c. p., o dalle previsioni della l. 25 giugno 1993, n. 205.

[13] Non si può fare a meno di notare, infatti, che l'art. 265 c. p., subito dopo il quale l'art. 2 del disegno di legge va a collocare gli artt. 265 – *bis* e *ter* appena richiamati, è rubricato «disfattismo politico», è collocato tra i delitti contro la personalità internazionale dello stato ed è destinato ad applicarsi in tempo di guerra.

[14] Il riferimento è alla sentenza della Cassazione n. 2445 del 1956, citata nella presentazione del disegno di legge.

[15] Così, l'art. 3, al comma 1, prevede che quando si apre un sito web privato, un blog, un forum o comunque una qualsiasi piattaforma elettronica destinata alla pubblicazione o diffusione *online* di informazioni presso il pubblico, fermo restando il non assoggettamento agli obblighi di registrazione di cui all'art. 5 della legge 8 febbraio 1948, n. 47 e all'art. 1, comma 3-*bis*, lett. a), della legge 21 marzo 2001, n. 62, è necessario che l'amministratore del sito comunichi, entro quindici giorni dalla diffusione *online*, tramite posta elettronica certificata, al tribunale territorialmente competente, il proprio nome e cognome, il domicilio, il codice fiscale e l'indirizzo di posta elettronica certificata, oltre che il nome e l'URL della piattaforma elettronica: qui non si comprende perché tali obblighi di comunicazione debbano avere come destinatario il tribunale (che peraltro non è chiaro se e come dovrebbe verificare l'autenticità delle informazioni fornite), se non come un tentativo di effettuare un parallelo con la registrazione dei periodici; ma se, rispetto alla registrazione dei periodici, attribuire tale competenza al tribunale aveva un significato preciso (quello di evitare la possibilità di un diniego arbitrario o improprio di registrazione), qui, invece, trattandosi di semplice comunicazione, non si vede perché il destinatario debba essere il tribunale.

[16] E' il caso dell'art. 4 del disegno di legge che, nell'estendere a titolari di blog o forum l'obbligo di rettifica previsto per i periodici, utilizza la medesima formulazione dell'art. 8 della legge sulla stampa, stabilendo che l'amministratore del sito provveda alla pubblicazione delle dichiarazioni o delle rettifiche dei soggetti «di cui siano state pubblicate immagini o ai quali siano stati attribuiti fatti o atti o pensieri o affermazioni da essi ritenuti lesivi della loro reputazione o contrari a verità, purché le dichiarazioni o le rettifiche non abbiano contenuto suscettibile di incriminazione penale», e che la pubblicazione della rettifica sia effettuata entro due giorni dalla richiesta, con idonea collocazione e caratteristica grafica e sulla pagina principale della piattaforma, con la stessa evidenza riservata allo scritto che ha determinato la richiesta: al riguardo, se è chiaro che chiunque si senta offeso da un contenuto *on line* è libero di chiederne la rimozione e, qualora non venga effettuata, di avviare un'azione giudiziaria, è evidente che quello che qui si impone è qualcosa di più e di diverso, cioè un vero e proprio obbligo di rettifica cui va dato riscontro indipendentemente dalla verità o falsità oggettiva dell'informazione, essendo sufficiente che il richiedente «ritenga» che il contenuto pubblicato sia contrario a verità e che il testo della rettifica non sia «suscettibile di incriminazione penale»; valutazioni che possono certo essere richieste a un direttore responsabile, ma che ben possono travalicare le capacità e le competenze di un privato cittadino.

[17] Nella presentazione del disegno di legge, con un accostamento quanto meno azzardato, il privato che segnala un abuso è equiparato al c.d. *whistleblower*.

[18] Cfr. art. 7 del disegno di legge: secondo gli artt. 16 e 17 del d. lgs. 70/2003, che danno attuazione agli artt. 14 e 15 della direttiva 2000/31/CE, sul commercio elettronico, l'obbligo di rimuovere un contenuto scatta solo in presenza di un ordine dell'autorità, essendo insufficiente la semplice richiesta rivolta da un privato al gestore del sito.

e nella giurisprudenza interna [19], e soprattutto impongono ai gestori delle piattaforme un obbligo di continuo e costante monitoraggio dei contenuti pubblicati dagli utenti, anch'esso in frontale contrasto con i principi comunitari [20].

Al di là della palese irragionevolezza di talune disposizioni, della carente formulazione tecnica e della genericità che le contraddistinguono, ciò che colpisce nel disegno di legge ora esaminato è l'atteggiamento culturale che esprime, caratterizzato dal recupero di concetti che era lecito immaginare ormai desueti, e che si sperava, con l'avvento della costituzione repubblicana, fossero stati ormai relegati nella notte della storia, come quello che eleva la tutela del prestigio internazionale dello stato a limite della libertà di espressione, in un clima di "militarizzazione" dell'informazione: sotto questo aspetto, però, bisogna riconoscere che i Senatori proponenti il disegno di legge sono, se non altro, in buona compagnia, come è agevole riscontrare dall'esame dell'altro documento sopra richiamato, cioè la risoluzione approvata dal Parlamento europeo nel novembre dello scorso anno «sulla comunicazione strategica dell'UE per contrastare la propaganda nei suoi confronti da parte di terzi».

Si tratta di un documento che sembra catapultato nei giorni nostri direttamente dall'America del Senatore McCarthy: partendo dal presupposto che sia in atto un conflitto tra UE e Russia, e che nell'ambito di tale conflitto il governo russo utilizzi siti, blog, agenzie giornalistiche e altri media anche in lingue UE per sostenere le ragioni della Russia e per "screditare" le istituzioni UE [21], la risoluzione evoca apertamente la categoria della guerra, parla di minacce per «la sovranità, l'indipendenza politica, la sicurezza dei cittadini e l'integrità territoriale degli Stati membri dell'UE» [22], e finisce col mettere sullo stesso piano tali attività russe con la propaganda dell'ISIS/Daesh [23], per concludersi con un generico invito agli stati a «vigilare» sulle azioni di disinformazione e di propaganda promosse dalla Russia, e con l'auspicio di una stretta collaborazione tra UE e NATO in questa azione di contrasto [24]:

Per fortuna (o forse per pudore), la risoluzione è molto generica sugli strumenti che occorrerebbe mettere in capo per contrastare la "disinformazione" russa (peraltro esplicitamente raffigurata come un attacco militare, e addirittura paragonata alla propaganda di una organizzazione terroristica volta al reclutamento di terroristi): quello che colpisce, però, al di là della vaghezza sulle misure auspicate, è il tono a dir poco enfatico ed allarmistico (minacce all'integrità territoriale, alla pace, alla sicurezza dei cittadini) che viene riferito a quelle che di fatto rappresenterebbero semplici attività di propaganda di un governo straniero.

E' probabilmente vero che il governo russo utilizza in modo molto spregiudicato e raffinato gli strumenti offerti dalle nuove tecnologie per sostenere i propri interessi e difendere le proprie politiche [25]: ma è anche lecito chiedersi chi non ha utilizzato, e tuttora non utilizza, simili strumenti

[19] È il caso dell'art. 5, che al comma 1, stabilisce la possibilità di chiedere la rimozione dal web di contenuti diffamatori o di dati e informazioni personali trattati violando la normativa vigente: si tratta di una disposizione che da un lato è inutile, da momento che la possibilità di chiedere la rimozione di simili contenuti è già prevista dall'ordinamento, dall'altro viene motivata invocando impropriamente la sentenza *Google Spain*, che come è noto non parla affatto di "rimozione", ma solo di eliminazione del *link* riferito ad uno specifico contenuto dall'elenco dei risultati di una ricerca.

[20] Cfr. ancora, da un lato, l'art. 7 del disegno di legge, dall'altro l'art. 17 del d. lgs. 70/2003, e l'art. 15 della direttiva 2000/31/CE sul commercio elettronico: sulla incompatibilità col diritto UE dell'imposizione ai *provider* di sistemi di filtraggio automatico dei contenuti illeciti v. anche CGUE, C-70/10, *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (2010) .

[21] Tali strumenti sono individuati nella risoluzione in modo multiforme: talora ci si riferisce a specifici siti, agenzie di stampa e canali televisivi, come «gruppi di riflessione e fondazioni speciali (ad esempio *Russkiy Mir*), enti speciali (*Rossotrudnichestvo*), stazioni televisive multilingue (ad esempio RT), presunte agenzie di informazione e servizi multimediali (ad esempio *Sputnik*)», ma non mancano riferimenti molto più vaghi e generici, come quello a «gruppi sociali e religiosi transfrontalieri (in quanto il regime vuole presentarsi come l'unico difensore dei valori tradizionali cristiani), nonché *social media* e *troll* della rete». Tale congerie di strumenti sarebbe utilizzata dal governo russo «per sfidare i valori democratici, dividere l'Europa, raccogliere sostegno interno e creare una percezione di fallimento degli Stati nel vicinato orientale dell›UE», ma non manca il riferimento al sostegno diretto del Cremlino a «partiti politici e altre organizzazioni all›interno dell›UE», sostegno che avrebbe lo scopo di «minare la coesione politica».

[22] Premesso che «la guerra dell'informazione è un fenomeno storico antico quanto la guerra stessa»; che «la guerra dell'informazione mirata, che è stata ampiamente sfruttata ai tempi della Guerra fredda, da allora forma parte integrante della guerra ibrida moderna, una combinazione di misure militari e non, di natura palese o occulta, impiegate per destabilizzare la situazione politica, economica e sociale di un paese sotto attacco, senza una formale dichiarazione di guerra, ed è rivolta non solo ai partner dell'UE, ma anche alla stessa UE, alle sue istituzioni, a tutti gli Stati membri e ai cittadini, indipendentemente dalla cittadinanza e dalla religione»; che «con l'annessione della Crimea alla Russia e la guerra ibrida condotta da quest'ultima nel Donbass, il Cremlino ha esacerbato il confronto con l'UE»; che «il Cremlino ha intensificato la sua propaganda attribuendo un ruolo di maggior rilievo alla Russia nel contesto dei media europei, per creare nell'opinione pubblica europea il supporto politico a favore dell'intervento russo e compromettere la coerenza della politica estera del CUE», se ne trae la conclusione che «le tecnologie belliche dell'informazione e delle comunicazioni sono state impiegate per legittimare azioni che rappresentano una minaccia per la sovranità, l'indipendenza politica, la sicurezza dei cittadini e l'integrità territoriale degli Stati membri dell'UE».

[23] Si afferma infatti nella risoluzione che, al pari del governo russo, anche «l'ISIS/Daesh, Al-Qaeda e vari altri gruppi terroristici violenti jihadisti utilizzano sistematicamente strategie di comunicazione e di propaganda diretta, sia *offline* che *online*, nel quadro delle motivazioni addotte per giustificare le loro azioni contro l'UE e i suoi Stati membri nonché contro i valori europei», oltre che «allo scopo di incoraggiare il reclutamento di giovani europei».

[24] La risoluzione evidenzia infatti che «a seguito della dichiarazione del vertice NATO di Strasburgo/Kehl, che ha sottolineato la crescente importanza per la NATO di comunicare in maniera adeguata, tempestiva, accurata e reattiva in merito all'evoluzione dei suoi ruoli, dei suoi obiettivi e delle sue missioni, nel 2014 è stato istituito in Lettonia il Centro di eccellenza delle comunicazioni strategiche della NATO (NATO StratCom COE), il quale è stato positivamente accolto dalla dichiarazione del vertice NATO in Galles», e si conclude affermando l'esigenza di «cooperare strettamente con la NATO» (e in particolare con tale «Centro di eccellenza») al fine di sviluppare strumenti di contrasto alla propaganda russa.

[25] Una efficace descrizione dell'utilizzo propagandistico dei nuovi media da parte del governo russo si può trovare, ad esempio, in E. Morozov, *L'ingenuità della rete,* cit.

di influenza, a cominciare dai governi "democratici" dei paesi membri della NATO [26]; ed è anche lecito chiedersi se la risposta corretta, di fronte al ricorso a tali strumenti, sia questa sorta di "militarizzazione" del conflitto mediatico, che non può che mettere a repentaglio proprio quei valori di pluralismo, tolleranza e libertà di cui tanto ci piace ergerci a difensori.
Non si può non segnalare, infatti, il rischio, insito in un simile approccio, di etichettare qualsiasi voce dissenziente rispetto alle narrazioni fornite dai media c.d. mainstream di situazioni come la crisi ucraina o la guerra civile siriana, o qualsiasi voce metta in discussione la versione ufficiale dei rapporti tra UE e Russia fatta propria dal Parlamento europeo, o che affermi la necessità o l'opportunità, per singoli stati membri dell'UE, di intrattenere relazioni più distese con la Russia [27], come propaganda al soldo del Cremlino, secondo schemi che rimandano agli anni più bui della c.d. guerra fredda.
Appare quanto meno inquietante che un documento del genere non sia emerso dagli archivi di qualche agenzia di intelligence, ma sia stato discusso ed approvato (sia pure in modo fortunatamente non unanime) dalla più importante istituzione rappresentativa dell'UE: che addirittura il Parlamento europeo si spinga ad evocare in modo così plateale l'esigenza di una vera e propria militarizzazione dell'informazione, giungendo a legittimare, ed anzi ad auspicare, da parte di UE e NATO, gli stessi comportamenti che vengono stigmatizzati se a porli in essere è il governo russo, testimonia di un certo quale imbarbarimento e di una regressione autoritaria dell'Unione, destinata a non portare nulla di buono.

3 Gli strumenti giuridici per il contrasto alla disinformazione *online*.

Se, come si è visto, i confusi e maldestri tentativi di risposta della politica assumono tratti talora persino inquietanti, ciò non significa che il problema della disinformazione on line non esista: e a preoccupare non è tanto, diversamente da quanto si afferma nella relazione al disegno di legge presentato al Senato, la velocità con cui le c.d. "bufale on line" si diffondono, quanto piuttosto l'estrema frammentazione dell'audience, la sua tendenza ad articolarsi in ristrette comunità di utenti, in cui le informazioni sono condivise tra soggetti che spesso hanno già in partenza relazioni di vicinanza o amicizia. Ciò rende più problematico contrastare la diffusione di informazioni erronee rispetto a quanto accada con i mass media tradizionali, in cui le c.d. *fake news* possono essere più agevolmente individuate e smentite, e contribuisce ad accrescere l'effetto di "polarizzazione" già magistralmente individuato e descritto, oltre un quindicennio fa, da Cass Sunstein [28].
Se la diagnosi è chiara, non altrettanto può dirsi degli strumenti giuridici attraverso cui si dovrebbe porre rimedio al problema, e del ruolo che, nel contrasto a tali fenomeni, dovrebbe essere svolto da autorità pubbliche e poteri privati, a cominciare dai c.d. "colossi del web".

3.1 Il ruolo dei "colossi del web".

La prima domanda che ci si può porre riguarda la praticabilità di forme di monitoraggio dei contenuti circolanti in rete, da realizzare con la collaborazione degli stessi fornitori di servizi web, a cominciare da motori di ricerca e piattaforme social: e in effetti, da qualche tempo, gli stessi c.d. "colossi del web", superato l'iniziale rifiuto di qualsiasi forma di coinvolgimento o di responsabilizzazione rispetto all'utilizzo dei loro servizi da parte degli utenti, hanno iniziato a valutare la possibilità di attivare forme di controllo, affidate ora a filtri automatici, ora alle segnalazioni degli utenti, con l'ausilio di appositi nuclei di "giornalisti – sentinella" o di soggetti esterni specializzati nell'attività di

[26] Oltre alla già richiamata vicenda delle "armi di distruzione di massa" di Saddam Hussein, non pare un segreto che i governi dei paesi NATO, a cominciare dagli USA, hanno fatto largo uso di strumenti di comunicazione di massa e di *media* digitali per influire sulle vicende politiche di altri paesi, a cominciare dal nord Africa e dal medio Oriente, per non parlare del sostegno più o meno dichiarato a movimenti di opposizione al fine di favorire il c.d. *regime change*.
[27] Si veda ad es. il passaggio in cui la risoluzione «sottolinea che la strategia di informazione del Cremlino è complementare alla sua politica tesa a rafforzare le relazioni bilaterali, la cooperazione economica e progetti comuni con singoli Stati membri dell'UE, allo scopo di indebolire la coesione e le politiche dell'UE».
[28] C. Sunstein, *Republic.com* (2002), trad. it. *Republic.com. Cittadini informati o consumatori di informazioni?*, Bologna, 2003.

"*fact checking*" [29].
Sul punto, non si può che richiamare quanto si è già osservato con riferimento alla previsione di obblighi di monitoraggio nel disegno di legge presentato al Senato: la quantità di informazioni circolanti sulla rete, e soprattutto il carattere estremamente frammentato degli spazi di discussione e dei canali attraverso cui le informazioni circolano, rendono estremamente difficoltoso e aleatorio l'assolvimento di un simile compito, se affidato esclusivamente a risorse umane, laddove l'affidarsi a meccanismi automatici pare quanto meno velleitario, nel momento in cui si tratti di discernere il vero dal falso.
Il monitoraggio della rete è, insomma, una attività estremamente onerosa e, per forze di cose, parziale, sicché l'imposizione di un obbligo in tal senso, oltre che allo stato incompatibile, come si è detto, col diritto UE, appare in ogni caso difficilmente configurabile: un simile obbligo, tra l'altro, sortirebbe anche l'effetto di rafforzare ulteriormente la posizione dominante, se non propriamente monopolistica, di cui taluni di questi soggetti già godono, ponendo una ulteriore barriera, in aggiunta alle molte già esistenti, all'ingresso nel mercato di nuovi eventuali competitori.
Del resto, l'imposizione di un obbligo giuridico di rimuovere le informazioni individuate come "false" pone dei problemi non solo di ordine pratico (come individuare e riconoscere una informazione falsa) ma anche di ordine strettamente giuridico: come pure si è accennato, infatti, se da un lato è opinione condivisa che la libertà di espressione non copra la deliberata diffusione di informazioni false, dall'altro si ritiene generalmente che il dire il falso non possa considerarsi automaticamente un illecito in sé, almeno sino a quando non rechi nocumento a beni o diritti tutelati dall'ordinamento; e non si comprende per quale ragione un'affermazione falsa dovrebbe avere un diverso trattamento a seconda che sia diffusa attraverso la rete oppure attraverso altri mezzi di comunicazione.
Se quindi appare difficile – e, probabilmente, anche del tutto inopportuno - configurare un obbligo giuridico in tal senso, è innegabile che nulla impedisce ai c.d. "colossi del web", se lo ritengono opportuno, di attivare strumenti di monitoraggio dei contenuti che gli utenti veicolano in rete: e infatti, come si è accennato, alcuni dei grandi operatori "over the top" si stanno già attivando in tal senso.
Si tratta di iniziative motivate anche, se non essenzialmente, da ragioni di mercato: attivando e pubblicizzando simili strumenti, tali soggetti da un lato difendono e consolidano il loro capitale reputazionale, dall'altro rafforzano la loro posizione dominante, dal momento che – è lecito supporre – ben pochi aspiranti concorrenti sarebbero in grado di offrire simili prestazioni aggiuntive.
E tuttavia, proprio il fatto che i c.d. "colossi del web" siano liberi di introdurre e implementare simili forme di monitoraggio dovrebbe suscitare qualche interrogativo: entro che limiti un soggetto che svolga simili attività può poi pretendere di andare esente da responsabilità per l'eventuale utilizzo illecito dei propri servizi da parte degli utenti? E ancora, in presenza di operatori – come *social network* e motori di ricerca – che stanno sul mercato in una posizione di monopolio o di quasi monopolio, sino a che punto si può accettare che la decisione di rimuovere un contenuto – o di renderne particolarmente difficile il reperimento, il che in definitiva non è poi molto diverso - non possa essere messa in discussione e contestata da parte del soggetto che quel contenuto ha inizialmente pubblicato in rete?
Qui si rivela in tutta evidenza come la disciplina della responsabilità degli ISP contenuta nella direttiva 2000/31/CE sia decisamente datata, e pensata per applicarsi a figure molto differenti da quelle dei c.d. O.T.T. che attualmente dominano la scena: la posizione di chi pubblica contenuti on line è, infatti, del tutto carente di tutele giuridiche di fronte alla decisione di un *social network* o di un motore di ricerca di eliminare o di rendere inaccessibili quei contenuti, nonostante una simile decisione possa tradursi, di fatto, nella loro scomparsa dal mondo del web; parallelamente, l'assunto,

[29] Per limitarsi ai due soggetti più noti ed influenti, Google e Facebook, basti ricordare che nell'aprile 2017 Google ha annunciato l'estensione anche al motore di ricerca di una forma di *fact checking*, già sperimentata su *Google news*, frutto da un lato delle segnalazioni delle utenti (attraverso dispositivi che permettono agli utenti di segnalare contenuti "inappropriati" o offensivi) dall'altro del lavoro dei c.d. "valutatori della qualità della ricerca". Tale attività può mettere capo a due possibili esiti: l'inserimento nei risultati della ricerca, di un *link* a siti che si occupano di *fact checking* (siti che non sono collegati a Google, ma sono costituiti da media ed editori "certificati", che devono però adeguarsi agli standard sviluppati dal *Reporters Lab* della *Duke University* e da *Jigsaw*, la sezione di Google che si occupa di soluzioni tecnologiche), in modo da consentire agli utenti di valutare autonomamente l'attendibilità dell'informazione, oppure (soluzione che lascia più perplessi, per la maggiore opacità che la contraddistingue) la modifica dell'algoritmo di ricerca tendente a diminuire la visibilità dei contenuti ritenuti non affidabili o "autorevoli" (sulle due soluzioni v., rispettivamente, le segnalazioni pubblicate sul sito di Google da Justin Kosslyn (*Product Manager* di *Jigsaw*) e Cong Yu (*Research Scientist* di *Google Research*) sotto il titolo "L'etichetta Fact Check da oggi disponibile in tutti i paesi nella ricerca Google e in Google News" e da Ben Gomes, col titolo "Un aggiornamento sui miglioramenti della qualità della ricerca" . Quanto a *Facebook*, da alcuni mesi, dopo le polemiche relative al presunto ruolo dei *social media* nell'incrementare la diffusione di *fake news* in occasione delle ultime elezioni presidenziali americane, essa implementa un sistema di *fact checking* che utilizza le segnalazioni dei lettori e l'attività di verificatori esterni, e che culmina nell'apposizione di un avviso che segnala che il contenuto è controverso (v. A. Jamieson-O. Solon, Facebook to begin flagging fake news in response to mounting criticism, in *The Guardian,* 15 dicembre 2016: sulle criticità di tale sistema, prima tra tutte il fatto che l'apposizione di simili "etichette" rischia di generare un effetto opposto, incentivando gli utenti alla condivisione delle notizie marchiate come controverse, v. peraltro quanto riporta S. Levin, Facebook promised to tackle fake news. But the evidence shows it's not working, in *The Guardian*, 16 maggio 2017. Una articolata riflessione sugli strumenti utilizzabili per contrastare la disinformazione *on line* si rinviene, infine, anche nel documento diffuso in rete da Mark Zuckerberg nel febbraio 2017 sotto il titolo "Building Global Community".

pacifico, secondo cui l'ISP non può essere gravato di obblighi di controllo rispetto al materiale che gli utenti veicolano in rete attraverso i suoi servizi, non può far dimenticare il fatto che, tuttavia, tale controllo può, comunque, essere svolto, e che in tal caso la pretesa del provider di essere considerato un mero intermediario neutrale entra, inevitabilmente, in crisi [30].

Ciò premesso, posto che, allo stato, nulla impedisce (e probabilmente nulla impedirà anche in futuro) ai c.d. "colossi del web" di esercitare forme di controllo sulle informazioni veicolate attraverso i loro servizi, l'approccio che pare più accettabile è quello consistente nell'incentivare, ove possibile, forme di controllo "morbido" che puntino, fuori dai casi di contenuti palesemente osceni o violenti o raccapriccianti, non tanto a rimuovere i contenuti considerati inattendibili o inappropriati, quanto piuttosto a segnalare al lettore che determinati contenuti sono controversi, sono oggetto di discussione, o che l'attendibilità di determinate informazioni è oggetto di contestazione [31].

Un simile risultato sembra potersi raggiungere, nell'attuale contesto, solo attraverso l'attivazione di strumenti di soft power, promuovendo protocolli di intesa con i grandi intermediari della rete o incentivando forme di autoregolamentazione da parte degli stessi: fermo restando comunque che, indipendentemente dall'attivazione di simili forme di dialogo più o meno virtuoso tra le autorità di controllo e regolazione e i grandi colossi privati e multinazionali del web, pare molto difficile ricondurre l'azione di tali autorità ad un quadro di regole cogenti, sicché nulla potrà impedire che, dietro lo schermo della lotta alle *fake news*, questi soggetti si rendano protagonisti di forme di controllo, tanto più pervasive ed insidiose quanto poco trasparenti.

3.2. Qualche considerazione a proposito del c.d. "*free marketplace of ideas*".

Come si è detto, l'assunzione da parte dei c.d. "colossi del web" di compiti di monitoraggio e controllo, se da un lato non dovrebbe essere (come allo stato non è) oggetto di imposizione legislativa, d'altro canto potrebbe essere in qualche modo incentivata dalle stesse logiche del mercato, in quanto rispondente alla loro esigenza di difendere la propria reputazione commerciale: e questo induce a chiedersi se l'approccio più corretto non sia, in definitiva, proprio quello di affidarsi puramente e semplicemente alle logiche e alle dinamiche del mercato.

Il frequente e risalente richiamo al c.d. "free marketplace of ideas" sembra, però, da maneggiare con cautela, perché pare afflitto da una ambiguità di fondo: da un lato, infatti, con tale espressione si vuole evocare, del tutto condivisibilmente, il principio secondo cui la disinformazione e la diffusione di opinioni discriminatorie o offensive dovrebbero essere contrastate, almeno nella normalità dei casi, non già attraverso l'uso della forza pubblica, ma attraverso le armi della critica e della discussione, in un contesto in cui l'affermazione o la sconfitta di una tesi dovrebbero dipendere solo dalla sua solidità e quindi dalla sua capacità di prevalere sulle tesi contrastanti; dall'altro, però, non si può evitare di sfuggire al potenziale evocativo insito nel riferimento al "mercato", che sembra assumere un significato ulteriore nel contesto di una società dominata dall'ideologia neoliberale, che vede nel "mercato", il principio ordinatore fondamentale della società e di ogni aspetto della vita umana.

In questo senso il riferimento al "free marketplace of ideas" rischia di sottendere la equiparazione delle idee e delle notizie a merci, e dell'utente dell'informazione (ovvero del cittadino) al consumatore, e quindi evocare una soluzione in cui il semplice gioco della concorrenza sia in grado di fare emergere, come per virtù magiche, le idee "buone" a discapito delle "cattive": ma ci sono almeno due buoni ordini di ragioni che suggeriscono di accostarsi con cautela a questo tipo di approccio.

Il primo ordine di ragioni è connesso alla impossibilità di identificare l'utente dell'informazione, nella sua dimensione di cittadino, con il (presunto) protagonista del mercato concorrenziale, ovvero con il consumatore: impossibilità che discende non solo e non tanto dalla considerazione (che

[30] Al riguardo, spunti interessanti, e in qualche misura in controtendenza rispetto all'esclusione di responsabilità affermata dal diritto UE, si possono rinvenire nella sentenza della Corte EDU *Delfi c. Estonia,* del 10 ottobre 2013, su cui v. G. E. Vigevani, *La responsabilità civile dei siti per gli scritti anonimi*, in *Forum di Quaderni costituzionali* (*www.forumcostituzionale.it),* 4 febbraio 2014.

[31] Secondo lo schema utilizzato da Wikipedia, e consistente nel segnalare che determinate voci sono incomplete, o non indicano le fonti o indicano fonti insufficienti o non verificabili, e che come si è visto (*supra,* n. 29) è oggetto di sperimentazione anche da parte di *Google* e *Facebook*: per inciso, l'idea che solo contenuti osceni o violenti o raccapriccianti possano essere oggetto di rimozione appare sorprendentemente in linea, *mutatis mutandis,* con lo spirito dell'art. 21 della costituzione, nel momento in cui isola il concetto di «buon costume» come atto a legittimare più incisive forme di restrizione alla libertà di espressione: a riprova del fatto che, al netto di un impianto che può apparire anacronistico, l'art. 21 Cost. è ancora un punto di riferimento utile e significativo anche in un contesto tecnologico e sociale profondamente mutato (in questo senso sia consentito rinviare a M. Cuniberti, *Disciplina della stampa e dell'attività giornalistica e informazione in rete,* in M. Cuniberti (a cura di), *Nuove tecnologie e libertà della comunicazione,* Milano, 2008, 207 ss., 235 ss. in particolare; *contra,* nel senso della necessità di una revisione delle previsioni costituzionali in materia di informazione e di comunicazione, v. invece M. Orofino, *La libertà di espressione tra Costituzione e Carte europee dei diritti,* Torino, 2014.

potrebbe legittimamente apparire un po' paternalistica e moraleggiante, e quasi confinante con una visione "funzionalistica") secondo cui in una democrazia il compito dell'informazione dovrebbe essere quello di formare "cittadini informati" in grado di assumere decisioni consapevoli [32], ma prima e soprattutto da una differenza, verrebbe da dire ontologica e strutturale, tra le due categorie, che consiste nel fatto che le scelte operate dal consumatore, se sbagliate o non adeguatamente ponderate, si ripercuotono, nei loro effetti negativi, essenzialmente sul consumatore stesso, laddove, al contrario, le scelte che il cittadino è chiamato ad assumere nel momento in cui esercita i propri diritti politici esplicano i loro effetti sull'intera collettività, su chi le ha condivise e su chi vi si è opposto.

Ma vi è una ragione ancora più profonda che suggerisce di diffidare della integrale sottoposizione del mondo dell'informazione alle logiche del mercato: la possibilità, per il consumatore, di scegliere il prodotto migliore, e quindi l'attitudine del mercato ad operare come strumento di selezione dei prodotti più affidabili, è tanto maggiore quanto più ricche e affidabili sono le informazioni in possesso del consumatore, che gli consentono di operare una scelta pienamente consapevole; ma se il"prodotto" che si tratta di scegliere è l'informazione stessa, allora è evidente che la stessa idea di un "mercato dell'informazione" rappresenta niente più che un circolo vizioso, un vero e proprio corto circuito logico.

Le considerazioni appena svolte appaiono ancora più inquietanti se ci si sofferma a riflettere sulla possibilità di applicare al "mercato delle notizie" e delle "idee" le tecniche del c.d. behavioural advertising, o del c.d. direct marketing, che consentono di guidare l'utente, nella ricerca del prodotto più adatto alle proprie esigenze, sulla base di una approfondita conoscenza dei suoi gusti, delle sue preferenze e inclinazioni, dei suoi interessi e bisogni più o meno indotti [33].

Tale possibilità è, ovviamente, decuplicata dalle infinite possibilità di profilazione dell'utente offerte dalla rete, con l'ulteriore aggravante che la gestione dei c.d. big data richiede risorse ingenti che sono inevitabilmente nella disponibilità di pochi: in questo contesto, insomma, non solo l'informazione è degradata a merce, ma la mercificazione riguarda e colpisce le stesse informazioni sulla base delle quali l'utente viene profilato, e in definitiva ciò che consente la ricostruzione digitale della sua personalità.

Insomma, se l'immagine dello stato come una sorta di grande fratello, e di un "ministero della verità" intento a scandagliare la rete per depurarla dalle *fake news* evoca, a ragione, una buona dose di inquietudine, neppure sembra pienamente rassicurante la prospettiva di affidarsi serenamente al "mercato" e alla presunta capacità del "consumatore" di operare una sorta di darwiniana "selezione naturale" dell'informazione in rete.

3.3. Il ruolo dell'informazione professionale.

Accanto al tema del ruolo svolto dai c.d. "colossi del web", vi è poi il problema, anch'esso di non agevole soluzione, di individuare un qualche affidabile criterio per distinguere tra informazione professionale e mera libertà di manifestazione del pensiero in rete: tale distinzione, lungi dal vedere affievolita la sua importanza, dovrebbe acquistare un ruolo ancora più decisivo, in un contesto in cui l'attività di informazione professionale e la libera espressione di opinioni e idee convivono spesso fianco a fianco, veicolate dalle medesime piattaforme distributive.

Per quanto complicata possa risultare, infatti, la distinzione tra informazione professionale e semplice libertà di espressione rimane cruciale, in primo luogo per la tutela dell'affidamento del cittadino nella correttezza e nell'affidabilità dell'informazione, e, in secondo luogo, per una ragione più strettamente giuridica, dal momento che all'esercizio in forma professionale dell'attività di informazione si collegano diversi obblighi e responsabilità, così come differenti prerogative.

Per comprendere la delicatezza del tema è sufficiente pensare al problema, di perdurante attualità, della protezione delle fonti: secondo quanto emerge dalla giurisprudenza della Corte europea dei diritti dell'uomo e degli organi del Consiglio d'Europa, la possibilità di invocare il diritto – dovere

[32] Visione che sembra caratterizzare l'approccio di C. Sunstein, *Republic.com,* cit.

[33] Sul crescente utilizzo di tali strumenti nelle campagne presidenziali americane, a cominciare dalle quelle democratiche del 2018 e del 2012 per arrivare a quella che ha portato alla presidenza Donad Trump, si veda ad es. quanto afferma Alexander Nix, amministratore delegato della *Cambridge Analytica* e consulente di Donald Trump in occasione delle elezioni presidenziali del 2016, in un'intervista pubblicata su *La Stampa* l'8 settembre 2016 sotto il titolo "*Nix, il cervello della campagna elettorale di Trump: "Grazie ai big data sappiamo cosa vogliono i cittadini*": «nel 2008 abbiamo visto come la campagna dei Democratici abbia fatto ampio uso dei dati digitali per identificare e persuadere gli elettori, soprattutto con i *social media*. Questo è stato un fattore centrale nel cambiamento degli equilibri anche perché i Repubblicani erano rimasti indietro nell'uso delle tecnologie, mentre in passato erano stati all'avanguardia. Ora si è verificato un nuovo sorpasso in questo campo da parte repubblicana, con grandi investimenti e la mobilitazione di ingenti risorse».

della protezione delle fonti non è riconosciuta a chiunque eserciti la libertà di espressione in rete, ma rimane prerogativa di chi eserciti comunque un'attività di tipo professionale, o connessa all'esercizio professionale dell'informazione [34].

Tale delimitazione appare complessivamente ragionevole (a condizione di non attribuire rilievo decisivo e assorbente al possesso di una specifica qualifica legale) [35], se si considera la delicatezza degli interessi coinvolti in tale problematica, e che spesso motivano la richiesta della fonte di mantenere l'anonimato, sicché appare più che comprensibile che la prerogativa possa essere invocata da soggetti in possesso delle competenze tecniche e della sensibilità deontologica necessarie per verificare l'attendibilità della fonte e, conseguentemente, l'attendibilità e l'interesse sociale della notizia e gli eventuali argomenti contrari alla sua diffusione, per assumere riguardo alla pubblicazione una decisione informata e consapevole e quindi per assumersi anche le relative responsabilità.

E' quindi da salutare con favore, nonostante alcune perplessità sul metodo utilizzato e sui possibili esiti [36], l'orientamento espresso dalla sentenza delle Sezioni unite della Cassazione del luglio 2015, che, nell'estendere, sulla base di una interpretazione "evolutiva" della nozione di "stampa", la disciplina di favore dettata dall'art. 21 Cost. in materia di sequestro alle testate giornalistiche on line, ha comunque ritenuto di precisare che tale estensione non riguarda ogni attività di manifestazione del pensiero svolta in rete, ma solo quella che presenti, appunto, i crismi della "professionalità" [37]: la disciplina in materia di sequestro della stampa, in quanto disciplina di privilegio rispetto alla disciplina generale del sequestro preventivo di cui all'art. 321 c.p.p., può essere applicata solo a fronte di un'attività caratterizzata da diverse e più stringenti forme di responsabilità.

Se l'esigenza di distinguere tra informazione professionale e semplice libertà di espressione non viene meno, ed anzi addirittura sembra rafforzarsi nel nuovo sistema mediatico, è certo però che si tratta di una distinzione tutt'altro che semplice, a cominciare dal problema di individuare il soggetto o i soggetti abilitati a tracciare la linea di demarcazione tra i due ambiti: ci si può chiedere, al riguardo, se la distinzione debba essere affidata a regole di diritto pubblico riferite ai soggetti (nella forma di una abilitazione professionale) o al prodotto (nella forma della registrazione del sito), o se ci si debba piuttosto basare semplicemente sulla "autorevolezza", vera o presunta, della fonte, sul riconoscimento reciproco dei colleghi e su quello del pubblico.

Certo, per molti aspetti l'ideale sarebbe che la distinzione fosse affidata alla capacità di discernimento del pubblico o, al più, all'autogoverno spontaneo della categoria, senza l'ausilio di strumenti pubblicistici, e che quindi la riconoscibilità della informazione professionale fosse demandata alla "autorevolezza" della fonte: e tuttavia, il ricorso al generico concetto di "autorevolezza" di una determinata fonte rischia di essere viziato dagli stessi meccanismi di persuasione più o meno occulta e di manipolazione che, come si è detto, viziano il ricorso al "mercato" come strumento di selezione della "buona" informazione, a cui si aggiunge l'evidente tendenza dei media c.d. mainstream a legittimarsi a vicenda, conferendosi reciproche patenti di credibilità e autorevolezza [38].

Non solo, ma l'affidarsi esclusivamente a meccanismi informali basati sulla "autorevolezza", sul riconoscimento reciproco o, al limite, sull'autoregolamentazione, non può comunque risultare sufficiente e appagante, perché, come si è detto, la possibilità di distinguere e riconoscere l'informazione professionale è essenziale non solo per fornire all'utente un criterio di orientamento nell'approccio all'informazione on line, ma anche per delimitare i contorni di uno specifico regime giuridico, che a norme di favore (come quelle in tema di sequestro o di protezione delle fonti) affianca anche specifici obblighi e responsabilità (come le regole in materia di trasparenza sulla proprietà, sul finanziamento e sulla gestione, la presenza e gli obblighi di controllo del direttore, gli obblighi di natura deontologica).

---

[34] Il principio è desumibile dal complesso della ormai copiosa giurisprudenza della Corte EDU in materia di protezione delle fonti (per tutti v. le sentenze *Goodwin c. Regno Unito* del 17 marzo 1996, *De Haes e Gijsels c. Belgio* del 24 febbraio 1997, *Sanoma Uitgevers B. V. c. Olanda* del 14 settembre 2010), ed è affermato espressamente nella raccomandazione n. R(2000)7 del Comitato dei Ministri del Consiglio d'Europa adottata l'8 marzo 2000, e confermato nella raccomandazione 1950 (2011) dell'Assemblea parlamentare del Consiglio d'Europa (cfr. il *considerando* n. 15).

[35] Rimangono pertanto in piedi tutte le perplessità (espresse, ad esempio, da G.E. Vigevani, *La protezione del segreto del giornalista al tempo di internet*, in *Costituzionalismo.it*, 2/2011) sull'attuale formulazione dell'art. 200 c.p.c. che circoscrive la possibilità di invocare la protezione delle fonti ai soli giornalisti professionisti, come definiti dalla legge professionale n. 69 del 1963.

[36] Per cui v. ad es. C. Melzi d'Eril, Contrordine compagni: le Sezioni Unite estendono le garanzie costituzionali previste per il sequestro degli stampati alle testate on-line registrate, in Diritto penale contemporaneo, 9 marzo 2016.

[37] Si tratta della sentenza delle Sezioni Unite penali n. 31022 del 17 luglio 2015; il principio è confermato anche da Cass. pen., Sez. V, 24 marzo 2016, n. 12536, su cui v. S. Vimercati, la Cassazione conferma l'inestensibilità ai blog delle garanzie costituzionali previste per gli stampati in tema di sequestro, in Diritto penale contemporaneo, 26 ottobre 2016.

[38] Questa forma di autolegittimazione di parte del mondo giornalistico è particolarmente evidente se si guarda ai programmi di informazione e di approfondimento politico delle c.d. televisioni "generaliste", caratterizzati dalla costante e ripetuta presenza, in veste per lo più di commentatori e "opinionisti", di un gruppo molto ristretto di giornalisti, per lo più della carta stampata, che si alternano con impressionante continuità circolando da una trasmissione all'altra: il fatto che in tale gruppo siano rappresentati diversi orientamenti politici nulla toglie alla autoreferenzialità di cui simili prassi sono evidente espressione.

D'altro canto, però, la selezione ad opera delle autorità pubbliche di ciò che può ritenersi informazione professionale incontra crescenti difficoltà e rischia di prestarsi ad applicazioni arbitrarie, come dimostrano le incertezze che contraddistinguono anche la già citata sentenza delle Sezioni Unite del 2015, che, nel momento in cui si tratta di precisare quali siano i requisiti (ontologico/strutturale, da un lato, funzionale/teleologico dall'altro) che distinguerebbero i due ambiti, non riesce a individuare criteri distintivi immuni da rischi di equivoci e incertezza, ed anzi sembra addirittura tentata di ripiegare sui discutibilissimi criteri («periodicità regolare» ed esistenza di «una testata, costituente elemento identificativo del prodotto») già individuati dalla legge n. 62 del 2001 per circoscrivere l'obbligo di registrazione del «prodotto editoriale» diffuso attraverso reti telematiche [39].
E in effetti, se non vi è dubbio che la versione on line di un grande organo di informazione e, all'opposto, la pagina facebook o il blog amatoriale di un privato cittadino siano prodotti completamente diversi, è peraltro innegabile che tra questi due estremi si estende una vasta zona grigia: come classificare, ad esempio, e a quale disciplina sottoporre un blog organizzato professionalmente, che utilizza una vera e propria redazione e raggiunge milioni di lettori? O una piattaforma che organizza e diffonde contenuti generati dagli utenti? O, ancora, un blog tenuto da un singolo giornalista, ma collegato ad una vera e propria testata giornalistica? D'altro canto, pur senza voler sopravvalutare il c.d. citizen journalism, appaiono sempre più evidenti anche i limiti dell'esclusivo riferimento alla legge professionale come strumento per qualificare l'operatore dell'informazione.
La risposta a tali problemi non può però consistere, come sembra fare il disegno di legge A.S. 2688 in precedenza esaminato, nell'attribuire alla diffusione di informazioni e notizie in rete in forma non professionale (ovvero, nel linguaggio utilizzato dal disegno di legge, attraverso siti diversi dalle testate registrate) inediti obblighi aggiuntivi, che tendono ad assimilarne la posizione a quella delle testate giornalistiche registrate, se non addirittura a renderla più gravosa: se infatti, da un lato, si può comprendere che la semplice registrazione della testata, o la presenza nella redazione o direzione di giornalisti iscritti all'albo, possano non essere più ritenute, oggi, elementi decisivi e dirimenti al fine di distinguere l'informazione professionale ed esercitata in forma di impresa dalla semplice libertà di espressione in rete, è d'altra parte anche evidente che il problema non si risolve facendo d'ogni erba un fascio e eliminando, di fatto, la distinzione tra i due ambiti.
Si tratta invece di rinvenire nuovi criteri distintivi, adatti ai nuovi mezzi attraverso cui si veicola l'informazione in rete, senza indulgere in facili semplificazioni o nell'illusione che basti coniare un nuovo termine o una nuova definizione legislativa: in questo senso, non pare ci sia molto da attendersi da un legislatore che sino ad oggi si è mostrato, se non del tutto sprovveduto, quanto meno mosso da logiche contingenti e spesso strumentali, e sprovvisto di una visione organica [40]; sicché non resta che auspicare che, attraverso l'opera congiunta degli operatori del settore e della giurisprudenza, si possa comunque pervenire, prima o poi, alla individuazione di uno statuto dell'informazione professionale che definisca chi è il "giornalista" dell'era digitale, come lo si riconosce, che caratteristiche e che tipo di formazione debba avere, attraverso quali strutture svolga la sua attività.
Si tratta di un compito immane, che non solo non si risolve con un tratto di penna o coniando una nuova definizione legislativa, ma che probabilmente neppure può più risolversi sul piano esclusivamente nazionale, dal momento che il sistema dell'informazione è globale e che in esso operano attori (singoli giornalisti o imprese) che è difficile vincolare al rispetto di regole con efficacia territorialmente limitata.
Si tratta, infine, di una sfida che coinvolge anche, da un lato, il tema della formazione del giornalista e dell'accesso alla professione, dall'altro quello del suo inquadramento professionale, della sua posizione contrattuale e delle sue condizioni materiali ed economiche di lavoro; pare difficile, infatti, pretendere rigore e autonomia di giudizio da soggetti che, nella stragrande maggioranza dei casi, lavorano in condizioni di precarietà, con retribuzioni al limite della sussistenza e totalmente sottoposti alle pressioni economiche dei datori di lavoro.

[39] Su tale controversa (ed emblematica) vicenda sia consentito rinviare a M. Cuniberti, *Disciplina della stampa e dell'attività giornalistica e informazione in rete,* cit., 215 ss.
[40] Come dimostra, ancora una volta, il citato disegno di legge A.S. 2688, che non trova di meglio, per individuare i soggetti gravati dai nuovi obblighi e dalle nuove responsabilità, che coniare un nuovo termine («piattaforma digitale che distribuisce contenuti informativi») il cui significato e la cui estensione rimangono incerti, e che rischia di generare gli stessi problemi interpretativi che in passato hanno contraddistinto altre nozioni (a cominciare da quella di «prodotto editoriale» nella legge 62/2001) altrettanto disinvoltamente disegnate dal legislatore.

3.4. La necessità di ripensare il concetto di pluralismo.

Tutto il discorso sin qui svolto pone, in conclusione, il problema di ripensare la stessa nozione di pluralismo con la quale sinora ci si è confrontati [41]: la semplice presenza, all'interno del sistema dell'informazione, di una molteplicità di contenuti differenti, espressione di differenti orientamenti culturali e politici, è oggi del tutto insufficiente, in un contesto in cui la disponibilità di una quantità enorme di dati e di informazioni rende indispensabile definire attraverso quali percorsi l'informazione viene veicolata e ciascun singolo utente viene a contatto con i contenuti presenti in rete; sicché, il problema centrale del pluralismo, oggi, non è più tanto dare uno spazio a tutti (posto che lo spazio è quasi illimitato), quanto fare in modo che ciascun soggetto venga concretamente a contatto con una pluralità di opinioni diverse [42].

Il problema, insomma, non è tanto la presenza della disinformazione (che c'è sempre stata, e spesso è stata anche veicolata dai mass media tradizionali), quanto il fatto che la disinformazione si diffonde in un mondo frammentato e polarizzato, in cui non trova contraddittorio, sicché si moltiplicano i rischi di manipolazione dell'utente: si tratta, quindi, di chiedersi attraverso quali strumenti si possa incrementare il contraddittorio in rete.

A questo proposito, occorrerebbe cominciare con l'interrogarsi sui criteri con cui si organizza la ricerca e l'accesso alle informazioni on line, e che, semplificando all'estremo, possono essere ridotti a due modelli opposti: quello che premia e privilegia i siti considerati più rilevanti secondo criteri che potremmo definire "oggettivi" (a cominciare dal numero di link in ingresso), e quello che valorizza, invece, le preferenze del singolo utente ricavate dalle sue precedenti ricerche e esperienze in rete [43].

Se non vi è dubbio che entrambi i criteri appaiono radicalmente inadatti a definire uno scenario autenticamente pluralista, è però tutt'altro che chiaro quali possano essere le alternative: le differenti soluzioni ipotizzabili, infatti, appaiono tutte più o meno viziate ora da un approccio eccessivamente "paternalistico", ora da insanabili contraddizioni interne [44].

Sicché, in attesa che qualcuno scopra l'algoritmo perfetto, che riesca a tenere insieme libertà di scelta dell'utente e pluralismo, una prospettiva forse meno ambiziosa ma sicuramente praticabile potrebbe essere quella di investire sulla preparazione dell'utente, di fornire cioè all'utente gli strumenti culturali e tecnici adeguati per verificare l'attendibilità di una notizia: le c.d. "bufale on line", infatti, sono per lo più riconoscibili, con un minimo di pazienza e di attenzione, da un utente avvertito e consapevole.

Nello scenario del sistema dei media che si va delineando, allora, il vero compito di "servizio pubblico", molto più che quello di garantire il "pluralismo" come sinora lo si è inteso (cioè come spartizione di spazi a vantaggio di alcune realtà politiche o sociali previamente selezionate e definite) dovrebbe essere quello di fornire strumenti critici per l'approccio e l'utilizzo della rete, in primo

[41] Ovviamente l'attuazione del principio del pluralismo nel contesto digitale pone una quantità enorme di problemi ulteriori, su cui non è possibile in questa sede soffermarsi, e per cui si rinvia a F. Donati, *Il principio del pluralismo delle fonti informative a tempo di internet,* in *Diritto e Società* 2013, 663 ss., a O. Pollicino, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider,* in *Consulta on line,* 10 febbraio 2014, e da ultimo a V. Pampanin, *Tutela del pluralismo informativo e regolazione economica nel mercato convergente della comunicazione,* in G. Avanzini-G. Matucci (a cura di), *L'informazione e le sue regole. Libertà, pluralismo e trasparenza,* Napoli, 2016, 163 ss.; più in generale, per un bilancio, non particolarmente roseo, sull'attuazione del principio nel sistema italiano dei media v. M. Manetti, Pluralismo dell'informazione e libertà di scelta, in *Rivista AIC*, 1/2012.

[42] Si tratta, peraltro, di un problema che esce dai confini di internet in senso stretto, per coinvolgere anche i *media* tradizionali, il cui utilizzo è sempre più contaminato e mediato dalle logiche della rete: si v., ad esempio, con riferimento al tema dell'informazione e della comunicazione politica, quanto osserva l'AGCOM nella sua indagine del 2015 su "*Il consumo di informazione e la comunicazione politica in campagna elettorale*" (reperibile sul sito dell'Autorità), circa il fatto che, se la televisione rimane ancora il mezzo più influente nel determinare le scelte politiche dei cittadini, sempre più incisivo e decisivo appare il ruolo dei *social network* nell'indirizzare gli utenti verso la visione di determinati contenuti. E in effetti il sistema dei *media* dell'era digitale appare sempre più come un sistema «ibrido» (per riprendere il termine utilizzato da A. Chadwick, *The Hybrid Media System: Politics and Power*, New York 2013), caratterizzato non solo dalla coesistenza, ma anche e soprattutto dalla integrazione e compenetrazione tra piattaforme differenti.

[43] Cfr. P. Costa, *Motori di ricerca e* social media*: i nuovi filtri nell'ecosistema dell'informazione online e il potere oscuro degli algoritmi,* in G. Avanzini-G. Matucci (a cura di), *L'informazione e le sue regole,* cit., 252 ss., 262 ss. in particolare.

[44] Ad esempio la soluzione (prospettata da C. Sunstein, *Republic.com*, cit., 197 ss.) consistente nell'imporre obblighi che si potrebbero definire di "pluralismo interno", come quello relativo all'inserimento, nelle pagine web, di *link* a siti di diverso orientamento; o quella (suggerita da E. Pariser, *Il filtro,* cit., che prevede l'adozione di sistemi di filtraggio che espongano le persone ad argomenti che esulano dalla loro normale esperienza. Simili soluzioni, da un lato, e a meno di fare affidamento esclusivamente sulla buona volontà dei privati, postulerebbero l'imposizione di obblighi estremamente invasivi a carico dei fornitori di servizi e/o di contenuti in rete, finendo con il comprimere significativamente la loro libertà e col rendere più difficoltosa, se non impossibile, la loro attività (oltre a rafforzare, come è effetto prevedibile di misure simili, le posizioni dominanti esistenti): ma, soprattutto, queste proposte, oltre a sottendere un atteggiamento un po' paternalistico nei riguardi dell'utente, considerato incapace di operare scelte autonome, rivelano anche un considerevole schematismo, nel momento in cui danno per scontato che sia sempre agevole rinvenire i contenuti "nuovi" ed "inediti" con cui l'utente dovrebbe essere messo in contatto, mentre in realtà anche tale operazione richiede scelte complesse, che verrebbero demandate o all'autorità pubblica (con la conseguente compressione della libertà degli operatori) o agli operatori stessi (con il conseguente rischio di ulteriori manipolazioni ed errori, oltre a quello derivante dalla necessità di intensificare il monitoraggio sulle abitudini di navigazione dell'utente: in questo senso cfr. E. Morozov, *Internet non salverà il mondo*, cit., 332).). Insomma, anche l'individuazione dei contenuti "nuovi" o "inusuali" relativamente al singolo utente è operazione che implica scelte, espressione di opzioni a loro volta ideologiche: si v. ad es. quanto argomenta Mark Zuckerberg, nel suo intervento del febbraio 2017 già citato (*supra,* n. 29), secondo cui, per evitare l'eccesso di "polarizzazione", non si dovrebbero tanto mettere a confronto tesi contrapposte, quanto e soprattutto privilegiare i siti che tendono ad offrire una gamma di punti di vista il più possibile variegata e completa; il che, però, può anche essere letto come l'intenzione di emarginare tutti i siti portatori di posizioni "estreme" per privilegiare le fonti "moderate" e asseritamente "obiettive".

luogo come strumento informativo.
In questo senso sembrerebbero muovere, effettivamente, alcune previsioni del citato disegno di legge A.S. 2688, che fanno riferimento ad iniziative di «alfabetizzazione mediatica» e a forme di «sostegno ai progetti di sensibilizzazione e ai programmi di formazione volti a promuovere l'uso critico dei media *online*» [45]: ma, al di là delle perplessità sugli strumenti con cui tali obiettivi si vorrebbero conseguire [46], si tratta comunque di previsioni che rischiano seriamente di rimanere confinate nel limbo delle buone intenzioni, se appena si considera che l'educare il pubblico all'utilizzo consapevole della rete, non diversamente dal formare bravi giornalisti, comporta costi non indifferenti.
É quindi lecito chiedersi, al di là dei proclami altisonanti e degli ambiziosi progetti (tutti da realizzare, immancabilmente, «senza oneri aggiuntivi per la finanza pubblica») [47], se realmente lo stato, oggi, abbia intenzione di investire in questo ambito, o se non sia più consono allo spirito dei tempi il lasciare operare indisturbate le logiche del "mercato", prendendo atto che l'informazione (e, forse, anche il suo "consumatore") non è altro, ormai, che una merce come tante.

[45] Cfr. art. 6, comma 1, lett. *a)* del d.d.l. cit.
[46] Strumenti individuati, dalle successive lett. *b)* e *c)* del citato art. 6, nella realizzazione «nelle scuole secondarie di primo e di secondo grado» di iniziative «per sostenere la formazione alla professione di giornalista», e nella possibilità di effettuar periodi di *stage* presso testate giornalistiche *online*: è persino inutile sottolineare infatti che, da un lato, la scuola secondaria non sembra il luogo più idoneo per formare alla professione di giornalista, e, dall'altro, che è quanto meno improbabile che gli *stage* presso le testate giornalistiche possano svolgere un ruolo significativo, se solo si hanno presenti le enormi difficoltà che l'aspirante giornalista incontra nello svolgimento del periodo di tirocinio; ma soprattutto, il disegno di legge sembra confondere due piani che dovrebbero restare distinti, e cioè quello della formazione del "lettore", da un lato, e del "giornalista", dall'altro, col rischio di non fare bene né l'una né l'altra cosa
[47] Come, ad es., dispone espressamente proprio l'art. 6 del d.d. l. da ultimo citato.

"Postverità", verità e libertà di manifestazione del pensiero*

"Post-Truth", Truth and Freedom of Expression

Cesare Pinelli
Professore ordinario di Istituzioni di diritto pubblico
presso La Sapienza - Università di Roma

Abstract

L'articolo affronta dal punto di vista giuridico la questione della sistematica distorsione della verità dei fatti alla quale si presta il web. Allo scopo, dopo aver esaminato il problema con riguardo a una accezione di verità riferita ai singoli destinatari delle informazioni, l'Autore si diffonde sull'accezione più generale di verità come obiettivo di un dibattito libero secondo la nota metafora del "*free marketplace of ideas*", confrontandola con i problemi posti al riguardo dalla comunicazione via web.

The article addresses from a legal standpoint the problem of misrepresentation of the truth through the Internet. To this end, once explored the notion of truth in connection to the individual recipients of information, the paper focuses on the more general problem of defining truth as the ultimate objective of a free debate reflecting the well-known metaphor of the "free marketplace of ideas". This speculation is then considered against the background of the current issues raised by the use of digital technologies.

Sommario

libertà di espressione
informazione
fake news
Internet
social network

1 I termini del problema.

La nostra sarebbe l'epoca della "postverità", l'epoca in cui la verità non conterebbe dunque più nulla: il rischio di disinformazione deliberata in ogni ambito della vita individuale e collettiva, si dice, aumenterebbe in misura esponenziale attraverso Internet e in particolare i *social networks*, a livello di grandi masse di popolazione. Questo è quanto leggiamo sempre più spesso sui quotidiani. Bisogna aggiungere, anche se lo si legge meno di frequente, che i Big Data a disposizione di società come Google fanno gola a tanti che agiscono nella sfera economica e politica, e che la loro disponibilità e il loro uso costituiscono un fattore di devastante distorsione tanto del mercato quanto delle competizioni elettorali: abbiamo cominciato a vederlo nelle campagne presidenziali americane, ma il rischio è molto più vicino a noi di quanto si creda[1].

Diffido di qualsiasi definizione generale della nostra o di altre epoche, specie quando, come nel caso della "postverità", inclina verso l'apocalittico. Ma in quel racconto c'è di sicuro qualcosa di razionalmente accertabile, e su cui potrò concentrarmi anche per i limiti delle mie conoscenze in materia.

Anzitutto la creazione di informazioni false presentate come vere (c.d. *fake news*), sia con la manipolazione informativa, ossia con l'uso di notizie vere ma con alterazioni e omissioni per indurre il destinatario a trarre implicazioni fuorvianti, va distinta dalla propaganda. Anch'essa mira a influire su opinioni, atteggiamenti, emozioni e comportamenti di uno o più settori della società avvalendosi della disinformazione. Tuttavia la propaganda oltre ad essere assoggettata a regole proprie e ad essere addirittura espressamente consentita dalla Costituzione ove si tratti di una forma di espressione della libertà di religione (art. 19), si svolge comunque in un contesto ben determinato, che consente al destinatario di avvertirne i possibili effetti: tale è ad esempio la propaganda di un prodotto di mercato, o di un partito o di un candidato in campagna elettorale. La diffusione massiccia, incontrollata e istantanea di notizie deliberatamente falsificate o manipolate va invece ben oltre la propaganda.

Essa si distingue pure, d'altra parte, dalla suggestione o dalla persuasione occulta di cui si cominciò a parlare mezzo secolo fa, in un libro rimasto famoso, come "aggressione all'inconscio"[2], e le cui tracce giuridiche sono ora rinvenibili nel divieto di pubblicità subliminale. Nel nostro caso stiamo parlando di informazioni di cui è agevolmente possibile provare la falsità, e che connotano corrispondentemente il concetto di manipolazione, che può ricorrere anche nel caso della suggestione.

Ma perché è proprio la rete a consentirle? Non basta dire che le nostre società sono caratterizzate da debolezze cognitive molto estese: la tendenza ad accedere e diffondere informazioni senza valutarle criticamente, la refrattarietà all'approfondimento, la sindrome da deficit di attenzione. Altri mezzi di comunicazione, a partire dalla televisione, favoriscono infatti l'accettazione passiva di un'informazione più ancora della rete, che richiede un comportamento comunque più interattivo da parte del destinatario.

La differenza sta altrove. I giornalisti che operano coi mezzi informativi tradizionali debbono sottostare alle regole sul diritto di cronaca, a pena di incorrere nelle sanzioni di volta in volta previste dalla legge. Inoltre, fanno parte di una comunità di professionisti che in Italia è addirittura istituzionalizzata in un ordine professionale, ed esercitano la loro attività alle dipendenze di un'impresa editoriale, per cui diffondere notizie deliberatamente falsificate o manipolate può provocare loro gravi danni reputazionali. Infine, il singolo che si ritenga leso per la falsità dei fatti attribuitigli è titolare del diritto di rettifica.

Nelle comunicazioni in rete non vi è nulla di tutto questo, e nello stesso tempo è consentito l'anonimato. Il singolo, ma anche i partiti e i candidati alle elezioni o i governi, sono indifesi di fronte alle notizie false o manipolate diffuse in rete, soprattutto perché queste possono esservi immesse senza che se ne possa identificare l'autore.

Le conseguenze sono ovunque drammatiche, come dimostrano tanti episodi individuali (fino a suicidi di giovani colpiti da calunnie diffuse in rete nei loro confronti) o relativi alla vita politica (fino ai sospetti di risultati elettorali inquinati da notizie false relative a taluni candidati, distorsioni del dibattito pubblico, delle competizioni elettorali e delle decisioni politiche, compresa la politica estera e militare dei singoli Stati). Si pensi, solo per parlare degli Stati Uniti, al ventottenne che entrò sparando in una pizzeria di Washington, convinto da informazioni diffuse su siti web che vi

* L'articolo trae spunto dalla relazione svolta al Corso di Dottorato in Diritto pubblico del Dipartimento di Scienze giuridiche dell'Università Sapienza di Roma, 20 giugno 2017.

1 Cfr. G. Da Empoli, *La rabbia e l'algoritmo. Il grillismo preso sul serio*, Padova, 2017, 14 ss.

2 V. Packard, *I persuasori occulti* (1958), Torino, 1989.

si nascondesse un centro di sfruttamento della prostituzione minorile gestito da Hillary Clinton, allora candidata alla Presidenza. Ma anche alle storie di Barack Obama nato all'estero e quindi ineleggibile, o del cambiamento climatico come «una bufala ordita dai cinesi per danneggiare l'industria americana», o di immigrati arabi nel New Jersey che festeggiavano la distruzione delle Torri Gemelle l'11 settembre 2001[3]. È ancora più recente lo scontro su "chi mente" fra il Presidente Trump e l'ex Direttore dell'FBI Comey, scontro che trae origine dalla mancata incriminazione di Hillary Clinton per sue *email* scoperte dall'FBI e proseguito da Trump a colpi di tweet.
La campagna contro i vaccini ha fatto come è noto molti proseliti in Italia proprio attraverso la rete, ed ora ci troviamo con un tasso di bambini ammalati a causa delle mancate vaccinazioni inferiore a quello ritenuto accettabile dall'Organizzazione Mondiale della Sanità, che ha costretto il governo a correre ai ripari, peraltro non senza contestazioni di un numero consistente di famiglie.
Gli esempi dovrebbero bastare a far capire la portata deflagrante delle falsificazioni che circolano via web.

2 La verità dei fatti come limite alla libera manifestazione del pensiero e la circolazione delle notizie in rete.

Nel nostro ordinamento la libertà di manifestazione del pensiero incontra il limite della "verità" dei fatti in riferimento al diritto di cronaca dei giornalisti e a condizioni ben determinate. Fu il cd. "decalogo dei giornalisti", fissato da due sentenze della Corte di cassazione del 1984 e mai da allora smentite, a stabilire che il diritto di cronaca dovesse rispettare, oltre l'utilità sociale o all'interesse pubblico dell'informazione fornita e alla forma "civile" dell'esposizione e della valutazione dei fatti, la verità oggettiva o putativa dei fatti (dunque quantomeno comprovata da una seria verifica delle fonti delle notizie), condizione che la giurisprudenza ritiene rispettata fino a quando si possa dimostrare la buona fede del cronista[4].
Nelle ipotesi di ingiuria (art. 594 c.p.) e diffamazione (art. 595 c.p.), l'art. 596 c.p. contempla poi, nei limiti e nei termini ivi previsti, l'*exceptio veritatis* circa l'attribuzione di un fatto determinato alla persona offesa. È vero che l'indirizzo giurisprudenziale secondo cui la diffamazione via *social network* non sarebbe punibile per mancanza dell'elemento essenziale della "comunicazione con più persone" richiesto dall'art. 595 c.p., trattandosi di ambiente virtualmente "chiuso" rispetto ad un sito web[5], è stato ampiamente superato, sia con l'argomento che un pubblico indeterminato può ricevere le informazioni lasciate in un determinato momento sul sito grazie al *tagging*, che consente di copiare messaggi e foto pubblicati in bacheca e nel profilo altrui oppure email e conversazioni in chat[6], sia in base all'orientamento della Cassazione secondo cui l'uso di una bacheca *Facebook"*consente a gruppi di soggetti di valorizzare il profilo del rapporto interpersonale allargato ad un numero indeterminato di aderenti al fine di una costante socializzazione[7]. Tuttavia, lo stesso argomento utilizzato per applicare le norme penali all'offesa *online* dimostra che questa può rivelarsi più gravosa e persistente di ogni altra, dal momento che la diffusione in rete non incontra limiti[8].
Quindi, da una parte siamo in presenza di un vuoto di tutela nei confronti di grossolane distorsioni di fatti diffuse sulla rete che non abbiano a che vedere con l'ingiuria o con la diffamazione, e dall'altra rimane l'impressione che le offese punibili così diffuse ricevano una garanzia non proporzionata alla loro gravità.

[3] Riportato in F. Rampini, *La postverità ti fa male, lo sai*, in *L'Espresso*, 22 dicembre 2016, 66.
[4] A. Pace, *Art. 21,* in A. Pace–M. Manetti, *Rapporti civili. La libertà di manifestazione del proprio pensiero*, in *Commentario della Costituzione*, Bologna-Roma, 2006, 334.
[5] Trib. Gela, 23 novembre 2011, n. 550.
[6] Trib. Monza, sez. civ. IV, 2 marzo 2010, n. 770; Trib. Teramo, sez. Giulianova, 16 gennaio 2012; Trib. Livorno, Ufficio G.I.P. 2 ottobre 2012, n. 38912.
[7] Cass. Pen., sez. V, 14 novembre 2016, n. 4873. V. già nello stesso senso Cass. Civ., sez. III, 20 dicembre 2007, n. 26964 e Cass. Pen., sez. I, 22 gennaio 2014, n. 16712.
[8] C. Parodi, *I reati di ingiuria e diffamazione a mezzo internet*, in *Corr. Giur*., 2000, 882.

3 La verità come risultato del confronto nel "libero mercato delle idee" e la circolazione delle notizie in rete.

Nel diritto costituzionale contemporaneo, la verità non è prospettata solo quale limite giudizialmente accertabile in una specifica fattispecie alla libertà di manifestazione del pensiero, ma anche come obiettivo ultimo del confronto fra tutte le opinioni, comprese le più eterodosse. In questo caso, ambedue i termini vengono declinati diversamente. L'espressione del pensiero viene qui riguardata non nel suo contenuto informativo ma appunto quale opinione su un certo fatto, e la verità è corrispondentemente riferita non a un certo fatto bensì all'esito di un processo necessariamente intersoggettivo

L'archetipo di questa versione si può rinvenire nella metafora del *free marketplace of ideas* coniata in una opinione dissenziente del Justice Holmes, il quale, riprendendo in sede giurisprudenziale il motivo che aveva guidato Milton e Mill nella loro battaglia contro la censura, osservò:

> «Che si persegua taluno per le opinioni espresse mi sembra perfettamente logico. Chi non ha dubbi circa le premesse da cui parte o le proprie capacità e desidera un certo risultato con tutto il cuore, esprime naturalmente i propri desideri in termini di legge, e spazza via ogni opposizione. Consentire l'opposizione mediante la parola è un po' considerare la parola impotente, come quella di chi affermasse che ha fatto quadrare il cerchio, o non avere effettivamente a cuore il risultato o dubitare sia delle proprie premesse o delle proprie capacità. Ma una volta constatato che il tempo ha avuto ragione di molte fedi battagliere, possiamo giungere a credere, più di quanto crediamo nei principi fondamentali della nostra condotta, che il bene supremo è meglio raggiunto attraverso il libero commercio delle idee, che la prova migliore della verità è la capacità del pensiero di farsi accettare nella competizione del mercato e che la verità è l'unica base sulla quale i nostri desideri possono essere sicuramente realizzati. Questa, in ogni caso, è la teoria accolta dalla nostra Costituzione. La quale, come tutta la vita, è un esperimento. Ogni anno, se non ogni giorno, dobbiamo scommettere la nostra salvezza su qualche previsione fondata su conoscenze imperfette. Finché tale esperimento fa parte del sistema, penso che dobbiamo costantemente vigilare contro il tentativo d'impedire l'espressione delle opinioni che detestiamo e consideriamo esiziali, tranne che minaccino d'interferire così da vicino con i leciti e urgenti fini del diritto da rendere necessario un riparo immediato per la salvezza del Paese»[9].

Molto più tardi questa impostazione sarà ripresa, pur con sfumature differenti, dalla Corte Europea dei diritti dell'uomo, allorché riterrà che la libertà di espressione di cui all'art. 10 CEDU «*vaut non seulement pour les "informations" ou "idées" accueillies avec faveur ou considérées comme inoffensives ou indifférentes, mais aussi pour celles qui heurtent, choquent ou inquiétent l'État ou une fraction quelconque de la population. Ainsi le veulent le pluralisme, la tolérance et l'esprit d'ouverture sans lesquels il n'est pas de "société démocratiqué"*»[10].

Abbiamo così accennato a un indirizzo che al di là e al di qua dell'Atlantico ha contrassegnato a lungo il modo di intendere il rapporto fra libertà di pensiero e verità, e più largamente fra diritti di libertà e democrazia. Esso ha certamente incontrato obiezioni di ordine teorico. Ma non è di esse che merita parlare qui, bensì degli enormi ostacoli di ordine pratico al libero corso del "mercato delle idee" che insorgono grazie alla propagazione in rete di false dicerie. Le quali non sono affatto smontabili come se si trattasse di una merce contraffatta, ma esibiscono una particolare resistenza alla confutazione.

Secondo Cass Sunstein, che riporta al riguardo una serie di esperimenti condotti fra gruppi di persone, tale resistenza può dipendere da due ordini principali di fattori. Il primo è quello che chiama "le cascate informative", basate sul fatto che, «nel momento in cui un certo numero di persone pare credere a una diceria, anche altre vi prestano fede, benché abbiano buoni motivi per ritenerla falsa. La maggior parte delle dicerie riguarda argomenti sui quali non si dispone di conoscenze personali o dirette, per cui ci si rimette alla massa»: e su Internet «le cascate informative sono all'ordine del giorno, e anche quando riguardano dicerie prive di fondamento influenzano fortemente le nostre convinzioni e il nostro comportamento. Basta considerare che i video di You Tube conquistano un numero molto maggiore di spettatori se si viene a sapere che ne hanno già attratto molti – un chiaro esempio di cascata»[11]. Il secondo fattore di resistenza delle dicerie, non necessariamente alternativo al primo, consisterebbe nella "polarizzazione nei gruppi", e si può esemplificare con la dimostrabile circostanza che dopo una discussione i partecipanti tendono più di prima a prote-

[9] O.W. Holmes, *Abrams v. United States*, 10 novembre 1910, 250 US 616, 624, in Id., *Opinioni dissenzienti*, Milano, 1975, 105.
[10] Corte CEDU, *Handyside c. Royaume-Uni*, ric. 5493/72 (1976).
[11] C.R. Sunstein, *Voci, gossip e false dicerie. Come si diffondono, perché ci crediamo come possiamo difenderci*, Milano, 2010, spec. 29 e 32.

stare contro un comportamento che pare loro scorretto, o che chi individualmente ritenga che sia stata commessa un'ingiustizia ne sarà ancor più convinto al termine della discussione[12].
Sostiene Sunstein che gli stessi processi che creano le false credenze possono renderle resistenti alla correzione, a causa della biased assimilation, che induce le persone ad elaborare le informazioni ricevute, che in ogni caso non è un processo neutrale, in funzione delle proprie inclinazioni e preferenze. In condizioni simili la correzione di dicerie false può addirittura rafforzarle: quando si tentò di dimostrare la falsità dell'affermazione dell'amministrazione Bush che l'Iraq disponeva di armi di distruzione di massa, ci fu semplicemente un rafforzamento delle convinzioni precedenti, sia dei liberal che dei conservatori. Quanto più invece le convinzioni precedenti sono deboli, come nel caso delle dicerie su Obama nel 2008, tanto più diventa facile smontarle[13].
Tutto ciò, prosegue Sunstein, non basterebbe a «negare del tutto l'esistenza di un "libero mercato delle idee". Bisogna però riconoscere che a volte questo peculiare mercato funziona male»: funziona male soprattutto nell'era dei blogger e di YouTube, dove «le vostre affermazioni non solo possono essere conservate per sempre, ma anche così attentamente monitorate che una qualsiasi, tolta dal contesto, può essere presentata come rappresentativa del tutto, o come indizio di qualcosa di oscuro o di allarmante»[14].

4 I rimedi e le obiezioni ai rimedi.

In definitiva, per come è attualmente regolata, la circolazione delle notizie in rete consente una distorsione dei fatti che presenta rischi consistenti sia per la tenuta di certi diritti individuali (all'onore o all'immagine) sia per la possibilità di mantenere integri i circuiti di formazione delle opinioni su cui si basa ogni consultazione democratica.
I rimedi che sono stati proposti dipendono dai giudizi di partenza sul fenomeno e dalla fiducia nella capacità dei sistemi di comunicazione in rete di autoregolarsi. Se si presuppone che «[i]l nuovo regime digitale ha un evidente tratto democratico sia da lato dei produttori sia dal lato delle audience», per il fatto di moltiplicare gli accessi e gli strumenti cognitivi, e si riconosce però che esso riduce «il tasso di responsabilità del sistema», il raggio dei rimedi ne risulta corrispondentemente ridotto a «criteri interni in grado di circoscrivere l'anonimato e di rendere chiari e pubblici i principi ispiratori degli algoritmi»[15].
A questo primo gruppo di rimedi si possono ricondurre tutti i tentativi dei responsabili di Google e Facebook, alcuni dei quali peraltro già attuati o in corso di attuazione, di autoregolare l'uso delle informazioni, in particolare con la sottrazione di introiti pubblicitari alle «pagine web che travisano, nascondono o espongono scorrettamente le informazioni su chi pubblica notizie, i contenuti dell'informazione o l'intento primario del sito, oppure con ricorso ad algoritmi che scoraggiano la diffusione di informazioni false»[16]. L'autoregolazione, soprattutto se perseguita dagli stessi responsabili dei motori di ricerca, presuppone evidentemente la fiducia nella loro capacità di evitare la distorsione dei fatti determinata da questi circuiti di comunicazione. Essa presenta il vantaggio di poter operare a livello globale, vista la diffusione a quella scala delle grandi compagnie, ma anche almeno un'incognita abbastanza evidente. Mi riferisco alla scarsa trasparenza e perfino alla difficoltà di comprendere l'efficacia dei rimedi così introdotti: fino a che punto «il ricorso ad algoritmi che scoraggiano la diffusione di informazioni false» risulterà efficace se la stragrande maggioranza degli utenti ignora il funzionamento stesso degli algoritmi? Costoro dovrebbero evidentemente fidarsi di ciò che i titolari dei motori di ricerca sostengono di aver fatto per rimuovere le pagine che distorcono le informazioni.
In senso opposto si muovono i rimedi che richiedono un intervento regolativo dei pubblici poteri. Mi limito a segnalarne due. In base al primo, gli Stati membri dell'Unione europea dovrebbero istituire Autorità indipendenti, coordinate da un'Autorità centrale istituita dall'Unione in base allo schema dell'Antitrust, allo scopo di rimuovere dai siti le notizie false ('*fake news*') e imporre sanzioni a quanti le abbiano diffuse[17]. Un secondo rimedio, ispirato al modello del Digital Millennium Copyright Act, consiste nel riconoscere a chiunque un diritto di segnalare e rimuovere dai siti web le calunnie e le

12 *Ivi*, 45-46.
13 *Ivi*, 54 ss.
14 *Ivi*, spec. 58 e 73.
15 A. Pilati, *Il regime digitale è democratico. Sono gli algoritmi che devono essere chiari*, in *Il Foglio*, 7-8 gennaio 2017, 4.
16 Cfr. M. Gaggi, *Facebook e Google. Battaglia per salvare la verità*, in *Corriere della Sera*, 16 novembre 2016, 11.
17 G. Pitruzzella, Intervista a *Financial Times*, 30 dicembre 2016.

informazioni false con correlativo obbligo dei gestori di rimuoverle[18].
Questo genere di rimedi presenta l'indubbio vantaggio di togliere dalle mani dei gestori il potere di regolazione. Il vantaggio è indubbio, dal momento che i rimedi proposti riflettono la sana diffidenza del costituzionalismo liberale verso l'accentramento eccessivo del potere: come si può ad esempio escludere, in assenza di un qualsiasi controllo esterno, che i gestori sacrificheranno i costi reputazionali alle risorse pubblicitarie? E perché, prima ancora, costoro dovrebbero essere giudici esclusivi di un simile apprezzamento? Ritorniamo alla questione del "libero mercato delle idee", o meglio ai limiti di una metafora che assimila troppo rapidamente le idee alle mele o alle automobili.
Sfortunatamente, le soluzioni che puntano all'intervento pubblico presentano però esattamente non solo il vantaggio ma anche lo svantaggio opposto a quello dei sostenitori dell'autoregolazione. Come risulta dalle proposte che ho riportato, l'intervento pubblico si trova pur sempre circoscritto a una dimensione nazionale o sovranazionale. L'ipotesi di una disciplina internazionale, la sola che combacerebbe con il livello globale della circolazione delle notizie in rete, è estremamente ardua, scontrandosi subito con l'ipotesi di uno o più Stati *free rider*.

5 Per un approccio graduale e comprensivo.

Nulla da fare dunque? Dobbiamo rassegnarci alla libera circolazione in rete delle false dicerie? Sarebbe una conclusione eccessiva, cui può giungere solo chi presupponga che esista una bacchetta magica per estirpare improvvisamente questo male. Se invece adottiamo un approccio graduale e comprensivo, la conclusione può essere diversa.
Un approccio graduale, intanto. La previsione del divieto dell'anonimato, fissata da Stati o da grandi organizzazioni sovranazionali come l'Unione europea, sarebbe per esempio già un grosso passo avanti. Ci saranno ancora siti dove circoleranno notizie o opinioni avvolte dall'anonimato, d'accordo; ma dovranno vedersela con costi reputazionali crescenti. È solo un esempio, che peraltro ha a che vedere col problema più urgente, cui altri se ne potrebbero aggiungere puntando sulla diffusione di black lists di siti inaffidabili da parte di Autorità indipendenti, preferibilmente le Autorità garanti delle comunicazioni.
Ma raccomanderei soprattutto un approccio comprensivo. Il fatto è che, perlomeno nei Paesi che siamo soliti denominare democrazie costituzionali, la grande diffusione della rete è caduta in una fase storica di massima sfiducia per la politica democratica e di crescente diffidenza per le conquiste della scienza. La sfiducia per la politica, oltretutto, dipende anche da una politica che ha abbandonato la ricerca delle soluzioni di problemi reali per rivestirsi di "un linguaggio delle intenzioni" che sostituisce ai compromessi pratici un mondo parallelo dove ci sono solo il bene e il male[19]. Né si può escludere che proprio questa peculiare distorsione dei fatti abbia contribuito a innescare una spirale di sfiducia, e poi di rabbia, nei confronti dei politici, in cui la circolazione di notizie false può trovare più facilmente credito. Nello stesso tempo cresce il sospetto per la scienza. Man mano che diminuisce la possibilità per ciascuno di noi di dominare le conoscenze scientifiche, tendiamo non a fidarci ma a diffidare degli esperti, anche perché, grazie alle superficiali acquisizioni raggiunte attraverso i media e la rete, noi stessi ci crediamo esperti, come dimostrano le distorsioni di cui l'opinione pubblica è stata vittima a proposito degli OGM e delle biotecnologie[20].
Se è vero che la grande diffusione di notizie fuori controllo sulla rete coincide con una punta di massimo discredito per la politica da una parte e per la scienza dall'altra, possiamo ancora meravigliarci della grande fortuna delle notizie false? Eppure molto dipenderà pur sempre da tutti noi. Ecco perché, anche se la circolazione di notizie false produrrà ancora danni irreversibili a singole competizioni elettorali come ai diritti di singoli cittadini, non possiamo permetterci di concludere che le nostre democrazie e i nostri diritti ne saranno definitivamente inquinati.

[18] C.R. Sunstein, *Voci, gossip e false dicerie*, cit., 88.
[19] P. Rosanvallon, *Le bon gouvernement*, Paris, 2015, 351.
[20] G. Bronner, *La democrazia dei creduloni*, Roma, 2016.

Fake news e allarme sociale: responsabilità, non censura*

Fake News and Social Alarm: Responsibility Does not Mean Censorship

fake news
responsabilità degli ISP
Internet
censura
algoritmi

Francesco Pizzetti
Professore ordinario di Diritto costituzionale, Università degli Studi di Torino

* Relazione introduttiva presentata al XXXII Convegno dell'Osservatorio "Giordano dell'Amore" sul tema " Fake news e allarme sociale: responsabilità, non censura", Milano, 5 maggio 2017.

1 Il tema di questo Convegno si incentra sulle *fake news* e sull'allarme sociale che esse ingenerano. Occorre dunque definire preliminarmente cosa si intenda per *fake news*.
Si tratta di una questione che non è possibile risolvere facendo riferimento a definizioni semplici e sufficientemente condivise del significato di questo termine.
Si può però dire che rientrano in questa categoria le notizie che riguardano fatti o vicende false, in quanto mai accadute, o false perché riferiscono di vicende realmente accadute in modo da indurre in errore di valutazione o di comprensione chi ne venga a conoscenza.
Qui sorge subito una prima questione di particolare importanza: per qualificare una notizia come *fake* è sufficiente che essa sia "falsa" o racconti in modo "falso" o "deformante" fatti realmente accaduti, o occorre invece che a questi elementi in qualche modo "oggettivi" si aggiungano anche elementi "soggettivi" quali la finalità perseguita e la consapevolezza della falsità della notizia o del modo con il quale essa è data?
Secondo la maggior parte dei commentatori e degli studiosi, a definire le *fake news* non concorrono però soltanto questi elementi perché una notizia sia considerata un *fake* occorre anche verificare non solo la finalità per la quale essa è diffusa e la conoscenza della falsità da parte di chi la dà o la diffonde, ma anche che essa sia diffusa per una finalità consapevolmente perseguita.
Questo aspetto complica molto la definizione di cosa si debba intendere per *fake news* perché introduce nella nozione non solo l'elemento soggettivo della consapevolezza della "falsità della notizia", ma anche quello della intenzionalità della sua diffusione, legata a una finalità specifica.
Il principio di finalità applicato al concetto di *fake news* è però estremamente sfuggente. I fini perseguiti da chi, consapevolmente, diffonde notizie false in quanto riferite a fatti mai accaduti, o false in quanto riferite a fatti accaduti ma rappresentati in modo falso o fuorviante, possono essere i più diversi e i più distanti tra loro.
Vi sono *fake* diffuse per pubblicizzare un prodotto commerciale; per aumentare il numero degli ascoltatori di una trasmissione televisiva o dei lettori di un giornale o degli utenti di un social; per aumentare il numero dei contatti tra utenti e la piattaforma che contiene l'informazione. Diffondere *fake news* o non impedirne la circolazione può essere utilissimo allo scopo di aumentare le vendite di beni o servizi di ampliare lo share dei media o di aumentare il numero degli *account* di un social, al fine di innalzare il valore commerciale del mezzo col quale la notizia è diffusa. Allo stesso modo non si può ignorare che i *social* stessi hanno interesse a diffondere *fake news* quando queste, per il loro contenuto, incentivano la curiosità degli utenti e si prestano a esser ridiffuse in modo massiccio. In questo caso, infatti, i *social* traggono un profitto dal numero di clic che l'accesso alla notizia produce e che si trasforma in un accrescimento del valore degli spazi pubblicitari oltre che nell'accumulo di un numero sempre crescente di dati, preziosissimi in tempi di Big data.
Diverso invece il quadro in cui si collocano le *fake news* che hanno la finalità di orientare la informazione politica o scientifica. Le *fake news* che intervengono nel dibattito politico o nei processi decisionali derivanti hanno lo scopo di modificare le opinioni politiche degli utenti, al fine di incrementare il consenso di chi si sostiene o di diminuire quello di chi si contrasta. Le *fake news* in materie scientifiche hanno in linea generale lo scopo di orientare le convinzioni dei cittadini circa la affidabilità della informazione scientifica nei settori più diversi della conoscenza. Le false comunicazioni scientifiche possono andare, infatti, dai farmaci e dalle cure relative alla salute fino alle tematiche ambientali, senza dimenticare le notizie e i "racconti" orientati a ridefinire la conoscenza del passato, come accade nel caso dei negazionisti o a spingere a visioni distopiche del futuro.
La stessa costante ricostruzione della storia, già paventata nel famoso libro di Orwell 1984, è resa oggi ancora più facile proprio dal fenomeno delle *fake news* che, a tal fine, sono ampiamente utilizzate.
Il termine *fake news* fa dunque riferimento a uno spettro amplissimo di fenomeni che assumono valore e significato diverso a seconda della finalità che ne orienta l'uso.

2 Il significato di questo neologismo è inoltre molto diverso da altri due concetti che negli ultimi tempi, anch'essi espressi con termini altrettanto nuovi, lo accompagnano spesso nelle discussioni sui media e nel dibattito pubblico.
Intendo riferirmi al neologismo "*post truth*" e al controverso concetto di "*alternative facts*".
Anche in questo caso siamo in presenza di termini che cercano di cogliere aspetti nuovi della realtà in cui viviamo, legati in particolare all'ecosistema costituito dai media e dalla diffusione delle notizie on line.
Come tutti sappiamo, "*post truth*" è stata scelta come la parola dell'anno 2016 dall'Oxford Dictionary, che ne ha dato una definizione precisa. Si tratta di una definizione, che ha più un valore

"concettuale" che "descrittivo", in quanto esprime il significato che l'aggettivo ha per i redattori del dizionario, mentre di norma i dizionari definiscono il significato che le parole hanno nel linguaggio utilizzato dalla comunità linguistica di riferimento.
Si tratta comunque di un aggettivo finalizzato ad esprimere una caratteristica del sostantivo al quale si accompagna. Esso si riferisce o denota circostanze rispetto alle quali i fatti oggettivi influenzano l'opinione pubblica non per ciò che essi sono ma per il modo col quale vengono raccontati («*relating to or denoting circumstances in wich objective facts are less influential in shaping public opinion than appeals to emotion and personal belief*»).
In questo senso l'espressione "*post truth politics*" è utilizzata per indicare quella comunicazione politica che, riferita o meno che sia a fatti realmente accaduti e a idee correttamente rappresentate, è data in modo da suscitare emozioni in chi l'ascolta.
L'obbiettivo è quindi di suscitare una partecipazione emotiva all'evento descritto o al messaggio politico che ne è oggetto.
Nel caso della c.d. *post truth*, la finalità del messaggio dato è dunque quella di stimolare o provocare emozioni (e credenze) e dunque una adesione di carattere più emotivo che razionale.
In questo senso nulla vieta che una *fake news* sia anche "*post truth*", come accade quanto la notizia falsa punti più sull'emotività che sulla razionalità di quanti ne vengano a conoscenza.
Un altro neologismo che spesso è accomunato a *fake news* è "*alternative facts*", un termine per ora ancor più incerto nel suo significato, usato in modo plateale dalla consigliera del Presidente Trump Kellyanne Conway durante una conferenza stampa il 22 gennaio 2017.
Il significato di questa espressione, secondo la stessa Conway, starebbe sostanzialmente ad indicare affermazioni o notizie relative a fatti accaduti che presentano una visione della realtà propria di chi la esprime anche se diversa da come gli stessi fatti sono stati visti e raccontati dalla maggioranza dei media o da fonti istituzionali specificamente competenti. Un po' come le diverse stime normalmente date da organizzatori e autorità di polizia circa il numero dei partecipanti a una manifestazione di massa.
L'uso dell'espressione "*alternative facts*", nella misura in cui legittima informazioni relative a fatti accaduti non corrispondenti alla verità oggettiva, è stata fortemente contestata da un gruppo cinquanta importanti giuristi americani aderenti al Distrisct of Columbia Bar Association's Rule of Professional Conduct, che il 23 febbraio 2017 hanno presentato un ricorso contro Conway per violazione del Codice etico, in quanto giurista titolare di pubblico incarico.
Tuttavia, in attesa di vedere se questa espressione sia o no destinata a radicarsi, è chiaro che essa rappresenta sostanzialmente una sottospecie di particolare interesse delle *fake news*.
Diverso è invece il discorso rispetto a un altro termine, anche questo frequentemente utilizzato con riguardo alle *fake news*. Il riferimento è al c.d. "*hate speech*", ovvero ai "discorsi di odio".
L'hate specch, infatti, ha una definizione specifica ed è stato oggetto di numerosi interventi normativi, sia a livello di Unione Europea che di CEDU, così come da parte degli ordinamenti giuridici di numerosi Stati.
Per *hate speech* si intendono, secondo il Consiglio di Europa (ma analoghe sono le definizioni degli altri ordinamenti) «tutte le forme di espressione miranti a diffondere, fomentare, promuovere o giustificare l'odio razziale, la xenofobia, l'antisemitismo o altre forme di odio fondate sull'intolleranza. Tra cui l'intolleranza espressa sotto forma di nazionalismo aggressivo e di etnocentrismo, la discriminazione e l'ostilità nei confronti delle minoranze, dei migranti e delle persone di origine immigrata» (Consiglio di Europa, Comitato dei Ministri).
All'interno dell'Unione Europea l'*hate speech* è stato definito illegale fin dalla Decisione quadro 2008/913/JHA del 28 novembre 2008 ed è su questa base che la stessa Unione Europea ha concordato il 31 Maggio 2016 con Facebook, Microsoft, Twitter e YOU Tube, nell'ambito dell'Internet Forum, il *"Code of Conduct on illegal online hate speech*".
Il concetto di *hate speech* è dunque precisamente determinato e giuridicamente regolato e perciò diverso da a quello assai più generico e sfuggente di *fake news*.
Nulla vieta che una *fake news* possa, per il suo contenuto, coincidere anche con l'*hate speech* e, se diffusa on line, ricadere nell'ambito del Codice di condotta appena citato.
Tuttavia concettualmente *fake news* e *hate speech* sono termini diversi che fanno riferimento a aspetti differenti della diffusione di notizie con riferimento al loro contenuto.
Va inoltre sottolineato che tutti i termini qui usati, *fake news*, *post truth*, *alternative facts*, *hate speech*, hanno almeno due cose in comune.
La prima è di far riferimento in generale alla diffusione di notizie o opinioni relative a fatti, o ideologie, o modi di vedere la realtà e di descriverla.
La seconda che nessuno di essi è di per sé limitato all'uso di Internet o alla comunicazione on line.

Al contrario tutti si applicano anche al sistema dei media e dei mezzi di diffusione del pensiero. Inoltre in genere riguardano aspetti dell'informazione che confinano con la libertà di opinione e comportano problemi non semplici di armonizzazione tra la libertà di manifestazione del pensiero, o per gli americani la "*freedom of speech*", e la violazione del diritto dei cittadini ad essere informati correttamente nel quadro di un diritto di informazione costituzionalmente garantito non solo come un diritto in sé ma anche, e soprattutto, come un diritto funzionale

3 Fermo restando quanto appena detto, sarebbe assurdo negare che tutti questi termini, e i fenomeni ai quali si riferiscono, hanno assunto un valore specifico nel tempo attuale in virtù del sistema dei media, da un lato, e della diffusione delle notizie on line, dall'altro.
L'incrocio tra media tradizionali e diffusione delle notizie on line, così come l'incrocio fra *fake news* e *hate speech*, dà vita a quello che *Mediamatters for America* ha definito nel suo noto paper "*Misinforme of the Year: the Ecosystem of Fake News and the "Alt-Right*", come un vero e proprio Ecosistema. Ancor più interessante su questo piano il contributo di Kate Starbird, "*Information Wars: A Window into the Alternative Media Ecosystem*", pubblicato in medium.com.
Pur essendo di estrema importanza ed efficacia, l'uso coordinato di media tradizionali e/o della informazione on line al fine della diffusione delle *fake news*, tuttavia non vi è dubbio che il vero habitat o bordo di cultura del tema che stiamo affrontando è quello della informazione on line.
Del resto la *Standford Graduate School of Education* il 22 novembre 2016 ha reso noto che una indagine condotta su 7.804 studenti in 12 Stati degli USA dimostra che la capacità dei giovani americani, anche delle *high school*, di valutare la credibilità delle notizie diffuse in rete è bassa. Infatti il 30% degli intervistati tra una notizia data da un sito "vero" e quella data da un *fake* website, ovviamente simile nell'aspetto al vero, preferiscono credere al sito falso.
Insomma, non vi è dubbio che l'interesse maggiore in materia di *fake news* va dedicato alla diffusione di questo tipo di notizie sulla rete.

4 L'aspetto principale della pericolosità delle *fake news* diffuse in rete e tramite i *social* consiste nel fatto che nella realtà on line ha preso piede un fenomeno inaspettato anche se molto prevedibile: quello della c.d. "informazione fai da te", in virtù della quale gli utenti dei *social* si informano l'uno con l'altro, attraverso una sorta di catena elettronica di S. Antonio potenzialmente pressoché infinita. E' facilissimo, inserendosi in queste "catene", magari usando tag che le identificano, diffondere informazioni false che però, specialmente dalle persone meno informate sono credute vere e originate o ritrasmesse da utenti reali della rete.
Questo compromette in modo decisivo la possibilità di sostenere, come spesso si è fatto, che la rete è in grado di autocorreggersi grazie alla Crowdwisdom, in virtù della quale le notizie infondate o di scarsa credibilità sono espulse dagli stessi utenti che rinunciano a ridiffonderle.
E' molto difficile credere che la crowdwisdom possa davvero funzionare quando si tratta di distinguere notizie fondate o credibili da *fake news* volutamente fatte circolare da chi è interessato a diffonderle. Occorre tenere presente che la maggior parte delle *fake news* che si diffondono in modo ampio, e talvolta persino virale, sulla rete sono originate non da *account* corrispondenti a esseri umani, anche se magari in modo anonimo, ma da *account* coordinati e gestiti da robot operanti secondo algoritmi appositamente definiti. E' evidente che questo fenomeno, proprio per la sua pervasività (guidata anche da un uso sapiente dei Big data e del Data analysis) rende difficilissimo per gli utenti normali distinguere fra notizie false o falsamente riportate e notizie corrette, anche se diffuse attraverso il sistema della "informazione fai da te".
Per questo non si può far conto soltanto sulla *crowdwisdom* per combattere in modo efficace il fenomeno delle *fake news* on line.
Per comprendere meglio questi aspetti e, in generale, il fenomeno delle *fake news* on line, è necessario però richiamare all'attenzione su alcuni aspetti della rete e dei *social* che è indispensabile avere presenti.
Questo comporta anche alcune precisazioni terminologiche che rispondono ad aspetti essenziali dei molti e diversi modi che caratterizzano la diffusione delle informazioni in rete e, di conseguenza, il fenomeno delle *fake news*.

5 Premesso che Internet gli strumenti di manipolazione della rete e, più specificamente, dei *social* sono numerosi e molteplici, è innanzitutto importante distinguere le *fake news* dai "*fake account*" e dai "*fake website*".
Mentre *fake news* è un termine che riguarda la notizia e il suo contenuto, *fake account* riguarda invece l'esistenza in rete di *account* anonimi, dei quali cioè il titolare non è noto, o usa una identità falsa. In molti casi, poi, l'*account* utilizzato corrisponde a persone realmente esistenti, dei quali è stata rubata l'identità.
Facebook ha dichiarato che nel 2016 un numero, non elevato ma significativo, di falsi *account* erano stati originati utilizzando mail rubate attraverso attività di hackeraggio.
Il fenomeno dei *fake account* è già molto pericoloso quando resta nascosta o è fasulla solo l'identità personale di chi lo gestisce. In questi casi, infatti, è quasi sempre impossibile al normale utente conoscere chi sia la fonte della eventuale *fake news* o comunque chi realmente abbia diffuso in rete una notizia diffusa in rete della quale si voglia controllare la fonte.
Il fenomeno diventa però infinitamente più pericoloso quando i *fake account* siano originati e gestiti da robot o, come si usa dire, bot in rete.
In questo caso infatti è possibile che la medesima *fake news* sia veicolata a un numero elevatissimo di persone, utilizzando anche un numero molto significativo di *account*. Non solo: è possibile organizzare dialoghi a intreccio fra *fake account* gestiti dal medesimo robot e *account* gestiti da identità effettivamente riconducibile a utenti reali della rete o, meglio, del social.
Ancora: va tenuto presente che in un sistema ormai dominato dalla tecnica dei Big Data e dal Data analysis è possibile anche inviare, tramite robot opportunamente gestiti con algoritmi dedicati, messaggi diversi a gruppi di utenti differenti e individuati sulla base di specifiche caratteristiche.
E' possibile di conseguenza moltiplicare e differenziare le *fake news* in modo che, pur mantenendo il medesimo potere di influenzare e confondere il dibattito pubblico, i messaggi raggiungano gli utenti in modo mirato e adeguato alle loro caratteristiche, opinioni e capacità di comprensione.
In questo modo le *fake news* aumentano enormemente di potenza e di efficacia e sono più difficilmente riconoscibili dai singoli utenti reali proprio perché sono "tarate" in modo da essere particolarmente adeguate alla loro mentalità e alle loro opinioni.
Ovviamente si tratta comunque di tecniche sofisticate e costose, che possono essere utilizzate solo da organizzazioni dotate di mezzi adeguati e per finalità che ne giustifichino l'impiego.

6 In questa fase della rete, il fenomeno appare riguardare essenzialmente la politica, come ha dimostrato la campagna elettorale di Trump, non a caso supportata dall'organizzazione estremamente sofisticata di Stephen Bannon e dei tre centri da lui gestiti (primo fra i quali la nota organizzazione Breibart).
E' noto però che già ora, e ancora più avverrà in futuro, tecniche analoghe sono impiegate anche a fini commerciali.
La tecnologia dei Big Data e della Data analysis consente infatti alle imprese di lanciare messaggi mirati ai consumatori, in un rovesciamento epocale del rapporto tra offerta e domanda. Grazie a queste tecnologie l'offerta può essere pensata e presentata in modo da incontrare esattamente la domanda anche di gruppi specifici di consumatori, dei quali si conoscono a priori tendenze, bisogni, desideri.
In ogni caso allo stato attuale è certamente vero che il legame fra *fake news*, falsi *account* e *account* gestiti da robot guidati da algoritmi molto sofisticati, è alla base del rapporto tra *fake news* e politica.
Un rapporto che spesso è orientato al discredito dell'avversario, accusato frequentemente di comportamenti del tutto falsi o le cui opinioni e atteggiamenti sono "raccontati" in modo da tornare a suo danno.
Non mancano però le *fake news* fatte girare in rete per favorire il candidato che si vuole rafforzare. In questo caso si tratta di notizie false nel contenuto, o false nel modo di raccontare fatti realmente accaduti, che vengono però presentate in modo da suscitare passioni e emozioni favorevoli al candidato.
E' qui che il fenomeno delle *fake news* si incrocia in modo rilevante con quello dell'informazione *post truth*. E' possibile inoltre che un uso sofisticato delle *fake news* a favore di un candidato possa consistere anche in narrazioni di fatti mai accaduti o, ancor meglio, di fatti accaduti ma presentati in modo da suscitare condivisione col racconto che di essi fa il candidato che si vuol sostenere, secondo l'impostazione che è alla base della tanto controversa teoria dell'*alternative facts*.
E' evidente a tutti che le tecniche, qui molto approssimativamente descritte, sono estremamente

insidiose e dannosissime per il dibattito democratico.
Esse infatti alterano la formazione dell'opinione pubblica non solo perché è falso o falsamente rappresentato il contenuto della notizia, ma anche perché è diffuso in modo da rendere impossibile alle persone comuni di conoscere la reale fonte della notizia e quindi poterne mettere in dubbio la veridicità, o comunque valutarne obiettivi e ideologia di riferimento. Inoltre esse hanno esplicitamente la finalità di incidere sul dibattito pubblico al fine di condizionare l'opinione e i comportamenti dei cittadini e degli elettori.

7 La rete e in particolare i social, che sono l'ambiente di elezione di questi fenomeni, dilatano infatti oltre ogni precedente dimensione gli effetti delle *fake news*, cambiando profondamente il dibattito pubblico.
Lo stesso padre del web, Tim Berners-Lee, in una lettera aperta in occasione del 28° anniversario della sua invenzione, ha lanciato un altissimo grido di allarme sull'uso dei servizi web per diffondere *fake news* che contengono falsità che vanno oltre la verità, secondo modalità che ingenerano odio e in alcuni casi lo propagano in modo da soffocare ogni sentimento di amore, inteso ovviamente come senso di convivenza comunitaria.
Quello che è certo, comunque, è che, come si è già detto, la maggior parte delle notizie che si diffondono in rete in modo virale sono *fake news* o notizie ispirate alla volontà di stupire e attrarre l'attenzione per la loro stranezza e anomalia. Ma quello che conta di più è sapere che ciò che ne rende virale la diffusione non è tanto il loro contenuto, quanto il fatto che molto spesso sono ridiffuse attraverso robot, la cui azione è talvolta ispirata a scopi politici ma molto spesso anche soltanto al fine di moltiplicare gli accessi alla notizia, i famosi clic che si trasformano per i *social* e i motori di ricerca in preziosi indicatori di valore e in fonti altrettanto preziose di pubblicità.
Inoltre il moltiplicarsi di accessi alla rete e alle piattaforme *social* è essenziale anche per alimentare banche dati da utilizzare con le tecniche Big data, sia che lo si voglia fare a scopi politici che a scopi commerciali.
Del resto, secondo una recente indagine, circa il 50 per cento delle notizie diffuse in rete sono originate da robot piuttosto che da accessi di utenti reali, titolari di specifici *account*.
Il valore commerciale degli accessi, sia sotto il profilo della frequenza di uso dei *social* che della raccolta di dati su chi clicca spiega bene anche la resistenza che per parecchio tempo ha caratterizzato gli IT Companies nel combattere questi fenomeni. Resistenza che sta venendo meno in modo sempre più accelerato negli ultimi due anni, proprio a seguito dell'eccessivo diffondersi sia dei discorsi di odio che delle *fake news*.

8 Al quadro sin qui delineato merita aggiungere altri due fenomeni particolarmente importanti in rete, che sono strettamente connessi alla diffusione delle *fake news*.
Il primo, importantissimo, riguarda i c.d. *website fake*. Si tratta di siti che deliberatamente diffondono notizie false rispetto al contenuto o al modo col quale questo è presentato, sia per finalità politiche, o finanziarie, o commerciali, o comunque di inquinamento del dibattito scientifico e storico.
Essi possono essere di due tipi.
Un primo tipo, rispetto al quale è discutibile se il termine *fake website* sia corretto, riguarda siti deliberatamente finalizzati a diffondere una informazione "orientata" e destinata a sostenere gli interessi dei governi o delle organizzazioni che li creano e alimentano. Appartengono a questo tipo siti come il Russia Today e Sputnik.
Si potrebbero fare numerosissimi esempi di siti di questo genere, con riferimento a molti Paesi e organizzazioni, anche non governative.
In questi casi si tratta essenzialmente di siti di tendenza che però, per raggiungere le loro finalità, spesso diffondono in misura massiccia *fake news* funzionali alla strategia di chi li gestisce.
Un secondo tipo di *fake website*, assai più insidioso, riguarda quei siti che si presentano con home page e altre caratteristiche editoriali volutamente pressoché identiche a quelle di siti ben noti e molto autorevoli.
Si tratta di una tecnica particolarmente ingannevole, proprio perché questi siti sono costruiti in modo da ingannare l'utente e fargli credere che quanto su di essi pubblicato o diffuso faccia capo a strutture mediatiche di assoluta affidabilità, o comunque di larghissima e consolidata conoscenza e reputazione.

Sono siti particolarmente pericolosi proprio perché raddoppiano l'effetto ingannevole delle notizie diffuse.

9 Un ultimo fenomeno, infine, riguarda i motori di ricerca, e in particolare quello di Google che gode praticamente di una posizione di monopolio nel settore.
Come è facile capire, il fenomeno delle *fake news*, ma anche quello dell'*hate speech*, producono notizie che, diffuse sulla rete, possono entrare nella enorme banca dati del motore di ricerca, che le ridiffonde quando gli utenti svolgano determinati tipi di ricerca o pongano "*queries*" che conducono ai links connessi a tali notizie.
In questo modo il fenomeno delle *fake news* e delle manifestazioni del pensiero riconducibili al genere dei "discorsi di odio" è destinato a ripetersi e riprodursi illimitatamente, almeno finché il motore di ricerca non cancelli i *links* relativi.

10 In un quadro così complesso, sia per le molteplici e diverse finalità che le *fake news* possono perseguire, sia per i complicati sistemi attraverso i quali possono essere diffuse on line è evidente che la lotta di contrasto è particolarmente difficile.
Tuttavia il problema ha assunto ormai dimensioni tali da rendere centrale il tema di come combattere questo fenomeno che comporta la necessità di tutelare gli utenti della rete dall'inganno e tocca anche valori costituzionali e democratici fondamentali.
Nella fase attuale due sono soprattutto i settori sui quali è accentrata di più l'attenzione dei governi e in generale dei media.
Il primo riguarda le *fake news* che, operando nell'ambito dell'informazione politica, mettono a rischio un principio fondamentale della democrazia moderna: quello della libertà di informazione e di manifestazione del pensiero come base essenziale per il formarsi di una opinione pubblica in grado di esercitare consapevolmente i propri diritti politici e civili. Nell'ambito di questo settore una particolare dimensione assume la lotta all'*hate speech* che non solo presenta aspetti connessi alla tutela di diritti fondamentali e alla non discriminazione delle persone umane (riconosciuta da tutte le Carte dei diritti successive alla seconda guerra mondiale) ma comporta in molti Paesi, in particolare fra quelli aderenti alla CEDU, la violazione di norme giuridiche specifiche. Ancor più rilevante, poi, è il contrasto all'*hate speech* per l'Unione Europea, che dal 2009 ha adottato, come si è già ricordato, una apposita decisione quadro in materia.
Il secondo settore che ha suscitato particolare attenzione e ha avuto, specialmente con riguardo al dibattito sull'utilità o meno dei vaccini, una particolare attenzione in Italia, è quello della informazione scientifica e in particolare di quella relativa ai trattamenti sanitari e alla salute.
La lotta nell'ambito dei due settori avviene utilizzando metodi analoghi, rivolti soprattutto a chieder alle IT Companies, e specificamente a quelle che gestiscono *social* e motori di ricerca, di adottare misure atte a impedire la circolazione delle *fake news* o, almeno, di segnalarne la dubbia veridicità. In questo quadro, particolare attenzione è posta anche al sistema di media, invitati ad evitare di amplificare le *fake news* in rete attraverso l'ecosistema mediatico e, soprattutto per quanto riguarda l'*hate speech*, ai motori di ricerca, ai quali si chiede di garantire il delink di ogni notizia che faccia riferimento a discorsi che invitano all'odio raziale o religioso, con una particolare attenzione a ricostruzioni storiche negazioniste che possano concorrere a fomentarlo.
Merita sottolineare che le differenze tra *fake news* a fini di lotta politica o di condizionamento della conoscenza, anche storica, e le *fake news* nei settori scientifici.
La ragione sta nel fatto che la lotta alle *fake news* relative al dibattito politico o storico coinvolge delicati equilibri tra la protezione degli utenti dalla falsificazione degli eventi, attuali o passati, e la libertà di manifestazione di pensiero o di parola. La lotta alle informazioni scientifiche false, o ritenute tali in un determinato momento storico, comporta un ben più difficile equilibrio fra la libertà di ricerca, che implica sempre la rimessa in discussione e la possibilità di confutazione della scienza ufficiale, e la protezione dei cittadini nei confronti di una informazione ingannevole. Il motivo risiede nel fatto che tale informazione distorce, anche involontariamente, la corretta conoscenza scientifica, inducendo in tal modo in errore i lettori in settori delicatissimi per la vita di tutti. Cosa, questa, pericolosissima in un ambiente on line, caratterizzato dalla informazione "fai da te". In un contesto di questo genere, infatti, è facilissimo che una informazione inesatta o ingannevole data dalla stampa di divulgazione, anche senza finalità intenzionali, si traduca rapidamente in paure ingiustificate e nel rifiuto di trattamenti scientifici o terapeutici che invece la scienza ufficiale avvalora e difende.

11 Questi aspetti, particolarmente evidenti nel caso di informazioni false o inesatte relative a risultati scientifici, metodi terapeutici, conoscenze che riguardano la salute, sono stati messi di recente benissimo in rilievo da Dominique Brossard nel corso del *meeting* annuale dell'*American Association for Advancement of Science*, tenutosi a Boston il 18 febbraio 2017.
La Brossad, muovendo dalla definizione di *fake news* nel settore scientifico come «una notizia prodotta utilizzando false informazioni allo scopo di influenzare la gente«, ha precisato che «*the problem in the science realm is deciding where the line between bad science reporting and fake news*».
La studiosa ha infatti sottolineato che spesso è il modo col quale viene data l'informazione scientifica, specialmente se da parte di mezzi di informazione generalisti, ad essere inesatto e ingannevole.
Il problema è dunque quello di spingere gli scienziati a curare di più l'informazione sulle loro scoperte e a comunicare essi stessi i risultati dei loro lavori in modo intellegibile al pubblico, anche e soprattutto quello specializzato.
La Brossard giunge sino ad affermare che gli scienziati devono sentire il dovere, e rivendicare il diritto, alla buona comunicazione scientifica, impegnandosi essi stessi a tal fine.
Inoltre la studiosa americana afferma tre principi che, a suo parere, devono essere sempre rispettati nell'ambito dell'informazione scientifica, specialmente on line.
I tre principi sono i seguenti: 1) gli scienziati devono curare una comunicazione chiara, fornendo fatti e dimostrazioni che possano convincere la gente a non credere a *fake news* che confutano senza fondamento le loro scoperte; 2) le istituzioni e le agenzie devono fare di più per proteggere la qualità dell'informazione e il controllo delle fonti; 3) il motore di ricerca di Google deve rendere non più accessibili gli studi scientifici che si sono dimostrati successivamente infondati e che spesso gli stessi autori hanno ritrattato.
Il senso generale e il pregio maggiore, dell'intervento della Brossard è quello di invitare gli scienziati a responsabilizzarsi maggiormente per quanto riguarda la comunicazione dei loro risultati anche al di fuori della comunità scientifica, confutando anche direttamente le notizie che ritengono false e fornendo le prove di tali falsità. A questo si aggiunge l'invito alle istituzioni a vigilare e controllare la fonte delle notizie a carattere scientifico, al fine di dare alla popolazione informazioni corrette, basate sulle conoscenze ritenute valide dalla comunità scientifica.
E' esattamente quanto è avvenuto in Italia quando, dopo numerosi interventi a confutazione di *fake news* circolanti in rete in merito alla vaccinazione obbligatoria, il prof. Burioni è intervenuto in modo esplicito e pubblico contro la trasmissione Report dedicata al vaccino contro il Papilloma virus.
Si è trattato, in questo caso, di una reazione alle affermazioni contenute in un servizio su un media tradizionale, ma abbiamo già sottolineato come nella realtà attuale l'Ecosistema mediatico consente una circolazione costante tra media e notizie on line, e del resto già in altre occasioni proprio il Prof. Burioni, insieme ad altri scienziati, si era ribellato a notizie in rete che negano l'utilità di specifici trattamenti farmacologici, tra i quali i vaccini.
Analogamente anche il nostro Ministero della Salute si è mosso nel senso indicato dalla Brossard. La ministra Lorenzin, anche in risposta all'appello degli scienziati italiani, ha dichiarato la necessità di puntare attivamente sull'educazione scientifica della popolazione e, su sua indicazione, il sito del Ministero della salute è stato aggiornato in modo da essere in grado di accogliere e diffondere le notizie che la comunità scientifica intenda necessario confutare, ospitando anche le informazioni utili a far comprendere ai cittadini rischi e pericoli che esse presentano.
Insomma, pur essendo vero che anche rispetto alle *fake news* in materia scientifica è necessario chiedere e imporre alle IT Companies l'adozione di misure atte ad evitare la loro diffusione o ridiffusione, come nel caso del motore di ricerca che renda ancora accessibili lavori scientifici ritrattati dagli stessi autori, è anche vero che in questo settore si rivendica con forza tanto il diritto degli scienziati a confutare le notizie false, fornendo una adeguata informazione scientifica, quanto il dovere delle istituzioni a proteggere i cittadini dal pericolo di falsità che possano indurre a comportamenti dannosi o a speranze infondate.

12 Anche nell'ambito delle *fake news* che incidono sul dibattito politico la strada della confutazione e della formazione degli utenti a riconoscerle e rigettarle è ampiamente suggerita dagli studiosi.
Tuttavia in questo caso vi sono due difficoltà. La prima è che la distinzione tra *fake news* e propaganda politica non è sempre facilmente definibile. E' ben noto, infatti, che anche la propaganda politica tende a descrivere in modo diverso i medesimi fatti a seconda del sistema di valori o degli obiettivi di chi la promuove. La seconda è che l'intervento delle istituzioni pubbliche si configura quasi inevitabilmente come una forma di censura, che contrasta con i principi fondamentali che

reggono i nostri valori fondanti in materia di libertà di manifestazione e diffusione del pensiero e di libertà di parola.
In altri termini, mentre un intervento istituzionale a tutela della comunità scientifica, da un lato, della corretta informazione dei cittadini in materie vitali come la salute, dall'altro, è sentita quasi naturalmente come legata al dovere di tutelare il benessere dei cittadini e della comunità, nel campo politico un analogo intervento, a meno che si tratti di casi assolutamente clamorosi, è facilmente avvertito come indebita compressione della libertà e come una forma di censura propria degli Stati autoritari. Non è un caso, del resto che Cina, Russia e Turchia abbiano a più riprese vietato alcuni *social* all'interno delle loro frontiere, e che recentemente la Turchia abbia proibito la diffusione on line di Wikipedia sul suo territorio.
Non sono peraltro mancati tentativi di elaborare testi normativi finalizzati appunto a prevenire la manipolazione informatica on line. Tra questi merita un cenno il disegno di legge presentato in Senato il 7 febbraio 2017, prima firmataria la senatrice Gambaro (atti Senato n. 2688). Si tratta di un disegno di legge che, come dice la stessa relazione, intende dare attuazione alla raccomandazione espressa dall'Assemblea parlamentare del Consiglio d'Europa il 25 gennaio 2017, con l'approvazione della risoluzione 2143 dal titolo "I media *online* e il giornalismo: sfide e responsabilità".
Lo stesso ha fatto recentemente anche il governo tedesco il cui ministro della giustizia ha presentato uno specifico progetto di legge per regolare la diffusione di notizie false sui *social online*
Tuttavia il disegno di legge italiano ha subito suscitato reazioni molto negative, sia per il suo contenuto, anche tecnologicamente non adeguato ai problemi che intende affrontare, sia perché prevede nuove forme di reato che sono subito apparse alla generalità dei commentatori di carattere dichiaratamente limitativo della libertà di stampa e di opinione, tanto se espressa attraverso i media on line quanto se diffusa attraverso i *social*.
Più interessante è apparso invece agli studiosi europei il testo tedesco ma è presto per dire quale effetto potrà avere se approvato. Tuttavia l'aspetto più discutibile del progetto tedesco è quello di mirare a regolare l'attività delle piattaforme e dei motori di ricerca, anche tenendo conto che in linea generale il codice di condotta adottato per regolare e limitare lo *hate speech* on line non è stato, a detta del governo tedesco, adeguatamente rispettato. A questo fine il testo mira a dettare regole specifiche che definiscono gli obblighi dei *social*, fra i quali quello di garantire una risposta efficace di fronte alle segnalazioni di *fake news*, particolarmente se riferite a discorsi di odio; di tenere il registro delle segnalazioni ricevute; di avvalersi di personale qualificato e indipendente per valutare la fondatezza dei ricorsi. Si tratta, in un certo senso, di un progetto finalizzato a rendere normativamente prescritti gli impegni che le IT si erano già assunte con la Commissione Europea e che, come si dirà tra breve, hanno almeno finora ampiamente disatteso.
E' chiaro peraltro che, anche seguendo questa impostazione, è difficile escludere che l'effetto della regolazione sia quello di spingere a forme di censura, aggravate dal fatto che il compito di valutare la fondatezza dei reclami è rimesso in primo luogo ai *social* stessi. Tuttavia non vi è dubbio che il progetto di legge tedesco sia più in linea di quello italiano con la tendenza in atto circa i modi da seguire per affrontare questi problemi.

13 La difficoltà di trovare modalità giuridiche adeguate per regolare questi fenomeni spiega perché, soprattutto rispetto alle *fake news* che falsificano o modificano la realtà con finalità politiche o di inquinamento del dibattito pubblico, lo sforzo in atto da parte dei governi e degli studiosi sia rivolto essenzialmente a chiedere, o imporre, alle IT Companies misure di contrasto poste in essere dagli stessi *social* o dai motori di ricerca.
Da un lato questo è certamente più immediatamente produttivo di effetti, perché punta sul fatto che la stessa tecnologia utilizzata dalle IT impedisca il diffondersi di *fake news* che altrimenti essa stessa renderebbe possibile senza limiti. Dall'altro però rischia di affidare direttamente alle IT Companies funzioni e responsabilità censorie nei confronti della libertà di manifestazione del pensiero, di opinione e di parola.
Questo fa capire la complessità del dibattito pubblico in ordine a quali vincoli imporre alle IT, e a quali condizioni essi possano essere resi obbligatori.
Fermo restando che la principale responsabilità resta in capo alla società e ai mezzi di informazioni, che per primi devono essere direttamente capaci di fornire informazioni alternative corrette, la delicatezza del problema sta nel fatto che le istituzioni devono saper imporre alle IT vincoli che proteggano gli utenti dal rischio di essere ingannati, senza però affidare ad esse poteri dichiaratamente censori. Cosa estremamente complessa anche tenendo conto che le stesse Companies operanti nel settore sono in grande difficoltà a decidere le strategie, anche collaborative, più op-

portune. Da un lato, infatti, esse sanno bene che un sistema di comunicazione digitale e di informazione on line che non sappia proteggere gli utenti da falsi palesi e da vere e proprie menzogne, anche storiche, rischia di perdere la fiducia dei cittadini. E' questa del resto una delle ragioni del grido di allarme lanciato da Tim Berners-Lee nel già ricordato intervento. Dall'altro le Companies sanno che ogni intervento contrasta col loro interesse a rendere massima la circolazione delle notizie in rete, anche quando queste siano palesemente false. Abbiamo già ricordato, infatti, che ogni accesso a un *social* e a una notizia su di esso circolante, così come il "postare" una nuova informazione, si traduce per le Companies in un duplice profitto, in termini di clic che segnalano la frequenza al sito, e in termini di dati raccolti che costituiscono una enorme ricchezza informativa per ogni utilizzazione possibile.

14 E' giunto ora il momento di analizzare, sia pure sinteticamente, quali siano allo stato attuale delle cose le richieste che i governi hanno fatto alle IT Companies e quali le risposte date. A questo si deve aggiungere l'analisi dei provvedimenti che *social* e motori di ricerca stanno cercando di porre in essere autonomamente, sia per evitare imposizioni da parte di singoli governi (che sono estremamente onerose per *social* che operano a livello mondiale), sia per evitare che si diffonda nei loro confronti un sentimento popolare di sfiducia che potrebbe allontanare in misura massiccia gli utenti dall'uso dei *social*.

Per quanto riguarda il tema dell'*hate speech* merita ricordare che, come già si è detto, nel marzo 2016 la Commissione europea ha avanzato la formale richiesta che all'interno dell'Internet Forum, le IT Companies sottoscrivessero con la Commissione un codice di condotta contro le forme illegali di discorsi ispirati all'odio.

Il Codice, sottoscritto il 31 maggio 2016, impegna le IT sottoscrittrici (Facebook, Microsoft, Twitter e YouTube a una serie di comportamenti dettagliatamente elencati, il più importante dei quali consiste nell'impegno a rimuovere dalle proprie piattaforme entro meno di 24 ore i discorsi illegali ispiratori di odio, rimuovendo o disabilitando, se necessario, l'accesso al loro contenuto.

A questo si aggiungono poi altri impegni finalizzati a definire linee guida concordate con la Commissione che stabiliscano anche le modalità di notificazione e l'eventuale uso di flag relativi a contenuti illeciti. Di particolare interesse anche l'impegno assunto di consentire a esperti indipendenti, individuati dai singoli Stati, di notificare la richiesta di rimozione dai siti di quanto ritenuto in contrasto col Codice deontologico stesso.

Questo insieme di impegni e obblighi, definito formalmente con riguardo all'*hate speech*, ha un valore che va al di là di questo. Esso infatti individua un complesso di salvaguardie che potrebbe essere esteso agevolmente anche ad altri tipi di *fake news* e ad altre forme di illecito uso dei *social*, soprattutto se finalizzate a inquinare il contenuto delle notizie che circolano sulla rete.

Il problema però è che il primo rapporto elaborato allo scadere del primo semestre di sperimentazione e presentato dalla Commissione il 12 dicembre 2016 ha dimostrato che le IT stentano molto a mantenere gli impegni assunti.

In particolare si è registrato un generale grave ritardo nella rimozione dei contenuti illegalmente postati in rete nell'ambito del divieto di *hate speech*.

Utilizzando i dati relativi a 600 notificazioni fatte in un periodo di sei settimane da parte di 12 Organizzazioni non governative in 9 Stati membri, si registra che nelle 24 ore previste come termine massimo la rimozione dei contenuti illegali è stata del 39% dei casi da parte di Facebook, del 90% da parte di YouTube ma solo dell'1% da parte di Twitter, che si dimostra sotto questo aspetto una delle piattaforme *social* meno capace di contrastare le *fake news*.

Anche sulla scorta di questi risultati, particolarmente censurati dal governo tedesco che ne ha fatto anche la ragione prima della sua iniziativa legislativa, alcune piattaforme si sono impegnate autonomamente a individuare forme e modalità utili alla rimozione o alla segnalazione di *fake news* presenti in rete e la loro conseguente rimozione.

Tra queste merita segnalare l'iniziativa di Facebook che ha lanciato in Italia e in altri 14 Paesi una guida, articolata in dieci consigli, finalizzata ad aiutare gli utenti a non cadere nella trappola delle *fake news*. Sono consigli molto semplici, e persino banali, che però possono porre al riparo chi usa la piattaforma dai principali rischi che corre, offrendo anche alcuni orientamenti per evitarli.

Sempre Facebook ha anche avviato la lotta ai siti pornografici, utilizzando un apposito "Report Tool", incaricato di bloccare i siti che, in base all'algoritmo che lo guida, appaiono a contenuto vietato.

L'iniziativa è assai interessante, anche se ha già dato vita ad alcuni episodi umoristici che dimostrano come lo strumento debba ancora essere molto affinato. Vi sono stati casi, infatti, nei quali

il Tool di Facebook ha bloccato anche la riproduzione di quadri famosi considerati, in ragione del soggetto, a contenuto pornografico.
Altra recente iniziativa di Facebook, per ora ancora allo stato sperimentale, è quella di offrire la funzione "Related articles", nota in Italia come "Articoli Correlati". Lo scopo è di offrire, in connessione con una notizia che potrebbe essere falsa o falsamente presentata, l'indicazione di altri articoli, relativi agli stessi fatti o a episodi analoghi, che consentano all'utente di formarsi una opinione più completa.
L'iniziativa, ancora allo stato sperimentale, è molto interessante, anche se vi è già chi ha sottolineato che in tal modo, sia pure con le migliori intenzioni, Facebook orienta le opinioni e le letture degli utenti.
Ovviamente siamo solo ai primi passi, ancora molto inadeguati se solo si tiene conto che la piattaforma di Facebook, insieme a quella di Twitter, appare essere uno dei mezzi preferiti per far circolare in rete *fake news* prodotte ad arte, secondo istruzioni precise, allo scopo prevalente di inquinare il dibattito politico, specialmente in occasione delle elezioni politiche nei diversi Paesi.
Molto interessanti anche le iniziative che Google sta mettendo in campo.
La società di Mountain View ha annunciato che intende operare su due piani.
Da un lato sta modificando l'algoritmo che presiede al funzionamento del motore di ricerca per consentire, prima di mettere le notizie e le informazioni a disposizione degli utenti, anche la verifica dell'autorevolezza delle fonti. Dall'altro offre agli utenti la possibilità di segnalare i testi e gli "*snippet*" relativi a contenuti violenti, offensivi, sessualmente espliciti, inutili o falsi.
Il motore di ricerca terrà conto sia dell'autorevolezza delle fonti valutata dall'algoritmo sulla base delle istruzioni ricevute, sia delle segnalazioni "umane". La finalità è di far retrocedere le fonti più discusse o di scarsa qualità. Lo scopo è quello di evitare incidenti come quelli già verificatesi in tema di fonti negazioniste senza peraltro cancellare i link, operazione questa che Google ritiene di non poter fare data la logica e la funzione del motore di ricerca.
Fra le tante iniziative in atto, merita infine segnalare quella del fondatore di Wikipedia, Jimmy Wales. Egli intende dar vita a un nuovo sito chiamato Wikitribune. Lo scopo è di garantire un sito nel quale ogni notizia pubblicata sia stata verificata da giornalisti professionisti che ne garantiscono non solo la veridicità ma anche la verificabilità.
Al momento si tratta ancora soltanto di un progetto sul quale Jimmy Wales sta cercando le risorse sufficienti per avviare l'esperimento. Tuttavia si tratta di una iniziativa molto interessante perché sfida non tanto la rete e i *social* quanto i media e dunque tutto l'ecosistema informativo che lega strettamente media tradizionali, media on line e piattaforme *social*.

15

E' tempo di concludere queste riflessioni che, pur nella loro sinteticità e inevitabile frammentarietà, possono consentire, ci si augura, di gettare uno sguardo su un panorama, quello delle *fake news*, estremamente articolato e complesso.
Siamo ancora ben lontani dall'aver individuato misure adeguate a combattere il fenomeno, sia negli aspetti legati ai rischi dell'informazione "fai da te" che in quelli connessi a forme di inquinamento dell'informazione. Fenomeni, questi, che rischiano di mettere in discussione le radici della democrazia e la stessa affidabilità delle istituzioni.
Ciò che si può dire con assoluta certezza è che siamo di fronte a mutamenti profondissimi delle modalità di diffusione e di circolazione delle informazioni. Le nostre società devono interrogarsi a fondo su come e in che modo mettersi al riparo dall'uso perverso di un tecnologia che offre, allo stesso tempo, opportunità informative mai viste prima e rischi di inquinamento e distorcimento della realtà impensabili fino a un decennio fa.
Due ultime riflessioni.
La prima riguarda la tecnologia stessa e, in particolare, le piattaforme *social*. Uno dei rischi maggiori dell'inquinamento dell'informazione è dato dall'uso di robot che possono diffondere un numero elevatissimo di messaggi, utilizzando anche, grazie alle tecniche Big Data, gli argomenti e le modalità informative più adatte a influenzare gruppi, anche molto limitati, di cittadini.
Da questo punto di vista occorre chiedere con forza e senza alcun tentennamento che le piattaforme *social* blocchino l'accesso ai robot diffusori di falsi *account*, cosa che possono fare senza alcuna particolare difficoltà, salvo la rinuncia ai guadagni che una intensa attività sulle piattaforme può offrire, sia in termini di clic che di dati acquisiti.
La seconda riflessione riguarda gli utenti stessi e la società tutta, comprese le istituzioni politiche ed educative di ciascun Paese.
E' assolutamente urgente sviluppare una massiccia additività pedagogica e informativa, che con-

senta agli utenti della rete di autoproteggersi, e comunque di valutare autonomamente il valore delle informazioni che ricevono.
Da questo punto di vista la guida messa in campo da Facebook può costituire, pur nella sua semplicità ed essenzialità, un valido punto di orientamento.
Quello che serve, se vogliamo conservare all'umanità il libero arbitrio e la responsabilità delle proprie scelte e dei propri comportamenti, è non tanto impedire la circolazione delle *fake news* (cosa comunque necessaria in determinate situazioni, come quelle legate all'uso di robot o alla diffusione di notizie scientifiche false o non verificate che possono ingannare i cittadini), quanto consentire a tutti di poter operare scelte responsabili, avvalendosi di una conoscenza della rete che li metta in grado di decidere liberamente e consapevolmente i propri comportamenti.

Fake news e responsabilità: paradigmi classici e tendenze incriminatrici

Fake News and Liability: Old-Fashioned Paradigms and Trends of Criminalization

Carlo Melzi d'Eril
Avvocato in Milano

Abstract

L'articolo affronta la questione della responsabilità per la diffusione di *fake news* alla luce della recente proposta di punire il falso in quanto tale se pubblicato *online*. Premesso che il fenomeno delle *fake news* non è nuovo, né è limitato a *internet*, l'Autore indica che il falso diffuso *online* dovrebbe continuare a essere ritenuto punibile secondo i principi consolidati in materia, ovvero solo qualora danneggi un interesse costituzionalmente tutelato. Rispetto alle nuove proposte di incriminazione e ad alcune recenti tendenze della giurisprudenza, si suggeriscono alcune ipotesi alternative per assicurare la tutela degli interessi che possono essere lesi dalla diffusione su internet di notizie false, evitando di configurare responsabilità di tipo penale in capo a soggetti diversi dall'autore del falso.

The paper explores the problem of criminal responsibility for spreading fake news in the light of the recent legislative proposal to punish untrue statements published online. Given that fake news isn't just a new issue concerning the Internet, the Author suggests that the well-established general principles should be applied to untrue statements even if they are spread online, only punishing their authors when they harm an interest protected by the Constitution. Compared to the new legislative proposal of incrimination and to recent case law from the Italian Court of Cassation, the Author suggests different solutions aiming to protect interests that could be offended by fake news spreading online, excluding criminal sanctions for anyone other than the author of the untrue statement.

Sommario

fake news
Internet
diritto penale
responsabilità degli ISP
social network

1 Premessa.

All'improvviso, e non tra un esiguo numero di studiosi ma nell'intera opinione pubblica, le espressioni *fake news* e *post truth* hanno cominciato a farsi strada ingenerando preoccupazione e allarme. Probabilmente proprio perché il fenomeno ha contaminato il dibattito giornalistico a molti livelli[1] e quindi una larga parte di cittadini si sono interessati al tema, il mondo politico, e con esso il legislatore, ha rivolto il proprio, di solito pigro, sguardo in questa direzione. Precisiamo subito che la discussione, in generale, e non solo quella alimentata da sprovveduti alla ricerca del clamore, è stata caratterizzata da timori eccessivi.

In particolare, si perdoni l'inevitabile semplificazione, molti hanno sottolineato la novità e la gravità dei rischi: dati inattendibili, racconti inventati, episodi mai accaduti, "messi in rete", con la straordinaria capacità di diffusione tipica del mezzo, sarebbero in grado di causare danni enormi. Si sostiene che nell'era della partecipazione massiccia alla produzione dell'informazione tali falsi assumono un peso decisivo, per numero, velocità di diffusione e, inoltre, incapacità del pubblico di distinguere tra giornalismo professionale e informazione prodotta da un *quisque de populo*. Sicché questo inquinamento, generato dalla moltitudine dei diversi produttori di notizie, rischia di nuocere seriamente al dibattito pubblico, che si deve nutrire, viceversa, soltanto di dati trasparenti, e merita quindi una risposta sanzionatoria da parte dello Stato.

In altri termini, l'inquinamento del dibattito pubblico porrebbe nel nulla una delle ragioni che rendono la libertà di manifestazione del pensiero così connessa allo Stato democratico: si tratta del presupposto perché i cittadini possano *conoscere per deliberare*. Se conosci il falso, deliberi male. Da più parti, quindi, da tempo si invoca l'intervento del legislatore, pronto a rispondere alla chiamata come accade davanti a vere o presunte emergenze, questa volta con il disegno di legge "Gambaro"[2] nell'ambito del quale, come vedremo meglio tra un attimo, per la prima volta il falso di per sé diventa penalmente rilevante, evidentemente sull'assunto di una sua estraneità all'ambito di tutela garantito alla libertà di espressione.

Se questo è lo stato delle cose, prendiamo le mosse da una considerazione, forse banale, ma che aiuta a portare il discorso su quelli che paiono i binari corretti. *Fake news* sono, né più né meno, notizie false. Per restare in ambiente anglofono, si può citare la definizione che di «*fake*» dà l'Oxford dictionary, secondo cui, con la encomiabile stringatezza della lingua inglese, l'espressione designa ciò che «*appearing to be something it is not*».

Come accennato, la preoccupazione nei confronti di chi inventa, propone e pubblica notizie false è giunta fino a far invocare sanzioni per costoro, finanche di natura penale. Nella relazione al disegno di legge "Gambaro" il bilanciamento fra gli interessi in gioco sembra questo: «chiunque [...] può dire quello che vuole, per la più che legittima libertà di espressione, ma se il pubblico di Internet prende per buono e fondato qualsiasi cosa circoli *online*, senza più distinguere tra vero e falso il pericolo è enorme». Viene, quindi, tra l'altro, previsto il reato di cui all'art. 656-*bis*. ("Pubblicazione o diffusione di notizie false, esagerate o tendenziose, atte a turbare l'ordine pubblico, attraverso piattaforme informatiche"), in base al quale «chiunque pubblica o diffonde, attraverso piattaforme informatiche destinate alla pubblicazione o diffusione di informazione presso il pubblico, con mezzi prevalentemente elettronici o comunque telematici, notizie false, esagerate o tendenziose che riguardino dati o fatti manifestamente infondati o falsi, è punito, se il fatto non costituisce un più grave reato, con l'ammenda fino a euro 5.000». Con un atto di stima e di fiducia nei confronti del giornalismo professionale, la contravvenzione non si applica ai «soggetti e ai prodotti di cui alla legge 8 febbraio 1948, n. 47, e di cui all'articolo 1, comma 3-*bis*, della legge 7 marzo 2001, n. 62».

Su quest'ultimo punto non può sfuggire un paradosso. Se l'obiettivo è punire l'inquinamento dell'opinione pubblica, il fatto che la disposizione non si applichi nell'ambito del giornalismo professionale sembra incoerente con la premessa. Se infatti c'è una fonte rispetto alla quale il pubblico coltiva l'aspettativa di un'informazione di qualità, veritiera e puntuale, questa è proprio la cronaca giornalistica professionale. Muovendo da queste premesse, la diffusione di notizie tendenziose, esagerate o false avrebbe forse ragione di essere punita e di esserlo vieppiù severamente proprio quando promani dall'esercizio della professione giornalistica, perché qui si potrebbe assumere più forte il disvalore dell'inquinamento dell'opinione pubblica. Ma nei confronti della professione giornalistica, come accennato, il legislatore nutre una tale fiducia che lo spinge a escluderne gli appartenenti dai soggetti attivi del reato.

Diciamo subito che questa iniziativa, fortunatamente ancora allo stato di disegno di legge, non ci

[1] All'estero, di recente, v. T. Garton Ash, *Free Speech: Ten Principles for a Connected World*, New Haven, 2016 e M. Thompson, *Enough Said: What's Gone Wrong With the Language of Politics?*, New York, 2016.

[2] Disegno di legge n. 2688, presentato alla presidenza del Senato il 7 febbraio 2017.

pare convincente. Per spiegarne il motivo e fornire qualche indicazione su come affrontare quello che è comunque un fenomeno che merita attenzione, è anzitutto necessario puntualizzare che sotto l'ombrello di *fake news* abbiamo provato a ricondurre tre insiemi di fatti diversi[3], a cui è opportuno fornire risposte diverse e reagire con strumenti diversi, non tutti necessariamente per mano del legislatore e non tutti necessariamente dotati di una sanzione.

2 Tipi diversi di *fake news*.

Queste "categorie" sono state già approfondite in altro lavoro presente in questa stessa sezione della rivista[4] (e quindi non ci si dilungherà sull'argomento). La prima tipologia di notizie false ricondotta alla nozione in questione riguarda i tentativi, da parte di gruppi di potere, da singoli personaggi fino a Stati sovrani, di modellare la pubblica opinione a proprio piacimento (e vantaggio) manipolando l'informazione. Un buon esempio di questo caso è quanto si dice sia accaduto durante le elezioni americane, il cui esito – qualcuno sostiene – sarebbe stato influenzato pesantemente non tanto da contenuti veicolati in rete, quanto da soggetti molto influenti che, proprio grazie alla massiccia diffusione di notizie false, hanno modificato il voto di una parte consistente degli elettori. Insomma, uno tra i momenti cruciali di una delle democrazie più importanti del pianeta, le votazioni presidenziali statunitensi, avrebbe visto il proprio risultato condizionato da fatti falsi, sapientemente inoculati in rete[5].

Con questo tipo di distorsione si comincia a parlare insistentemente del fenomeno, trattandolo per quello che certo non è: una novità. È vero che il mezzo è relativamente nuovo, benché siano più di dieci anni che si parla di web 2.0, ovvero della rete come ambiente dove gli utenti non sono solo fruitori che raccolgono informazioni, ma le creano, contribuendo attivamente al flusso della comunicazione. È in ogni caso molto più antica (secondo alcuni endemica) la tendenza del potere – pubblico e privato; politico, economico, religioso – a creare masse plaudenti, anche attraverso una torsione della realtà, usando i media che il periodo storico mette a disposizione. Da quando esiste il potere esso cerca legittimazione non sempre usando una limpida comunicazione come regola di comportamento. Questa attività si chiama «propaganda» ed ha caratterizzato ogni regime, democratico e no.

Sanzioni penali, in casi del genere, non sembrano una buona idea. Al di là della aspirazione ad un ordinamento in cui esiste un diritto criminale minimo, davvero *extrema ratio* nei confronti di insulti a beni giuridici non altrimenti tutelabili, sono due i motivi che convincono in questo senso. Il primo: la ostilità ad affidare a un organo statale, dotato di poteri coercitivi, la possibilità di attribuire patenti di verità. Il secondo: la estrema difficoltà, a volte forse la impossibilità, di distinguere il grano del vero dal loglio del falso.

L'antidoto a questa particolare tipologia di *fake news*, dunque, pare un altro: un maggior pluralismo, che aiuti a smascherare le falsità, e una rigorosa disciplina sulla trasparenza della proprietà dei media che vieti le concentrazioni, indispensabile terreno di cultura per il pluralismo stesso. Insomma, è una specie di guerra batteriologica: il batterio della propaganda si combatte con iniezioni di maggiore libertà.

La nozione di *fake news*, poi, è stata usata per descrivere quella sterminata messe di dati, opinioni, racconti di scarsa autenticità di cui la rete letteralmente gronda. Soprattutto sui social media, infatti, ove ognuno può pubblicare ciò che vuole senza alcun controllo, è facile trovare episodi, commenti e affermazioni la cui affidabilità è pressoché nulla e che spesso si rivelano falsi. Sono informazioni circolanti in rete, che passano per lo più inosservate, ma che, per ragioni spesso casuali, a volte riescono ad avere una maggiore "audience", magari perché riprese da soggetti con un seguito consistente. È un chiacchiericcio originato dal continuo comunicare non coordinato di milioni di persone. E in questo profluvio di parole si trovano appunto anche affermazioni del tutto inventate, leggende metropolitane del tutto futili, ma talvolta anche suggestioni infondate su temi di grande rilievo quali la salute, che magari contrastano con le acquisizioni della scienza.

Anche in questo secondo ambito si sono levate voci che pretenderebbero di eliminare ogni contenuto falso dalla rete e, anzi, di "elevare" a reato la diffusione di messaggi non veri. Ma pure qui la soluzione non sembra né praticabile né opportuna. Oltre agli argomenti già spesi in precedenza, che convincerebbero a desistere dal proposito, ve n'è un altro non irrilevante.

[3] C. Melzi d'Eril – G.E. Vigevani, *Difesa giuridica dal social-chiacchiericcio*, in www.ilsole24ore.com, 2 aprile 2017.
[4] M. Bassini – G.E. Vigevani, *Primi appunti su* fake news *e dintorni*, in questa Rivista
[5] Per uno studio sul tema si veda H. Allcott - M. Gentzkow, *Social Media and Fake News in the 2016*, in *Journal of Economic Perspectives*, 2017, 211 ss.

Secondo alcuni la garanzia dell'art. 21 Cost. non si estenderebbe fino a tutelare affermazioni soggettivamente false[6]. Secondo altri, il "falso" non avrebbe in effetti ragioni di tutela in presenza di altri beni giuridici in conflitto, ma *di per sé* non potrebbe essere punito[7]. Questa seconda posizione pare quella più convincente. Può essere condivisibile che l'ordinamento non difenda chi diffonde affermazioni false, poiché in effetti non sembra esistere un interesse meritevole di tutela da salvaguardare in questo caso. Tuttavia, ciò non significa che il "falso" debba essere, lo si ripete, *di per sé* bandito, con tanto di sanzione, dall'orizzonte della comunicazione pubblica.
In altri termini: la asserzione di un dato falso potrebbe essere espressamente vietata, e chi l'ha diffusa dovrebbe andare incontro a una pena, solo se ciò danneggia o mette in pericolo un altro interesse, individuale o collettivo, di valore costituzionale (si tratta di un approccio in cui risuonano orientamenti della giurisprudenza della Corte suprema statunitense, che ha sempre ritenuto incostituzionali per contrasto con il Primo Emendamento le incriminazioni del falso *tout court* che non colpissero un interesse costituzionalmente rilevante, indirizzo confermato di recente dalla sentenza *United States v. Alvarez* del 2012[8] che fa un riepilogo della casistica affrontata). In questo caso, infatti, la bilancia tra il bene giuridico "in contrasto" e la libertà di manifestazione del pensiero difficilmente pende a favore della seconda. Ciò perché di solito non vi sono ragioni perché l'ordinamento privilegi la libertà di espressione quando veicola un fatto non vero.
Perché l'ordinamento compia un bilanciamento tra interessi meritevoli di tutela a livello costituzionale, dunque, è necessario che ve ne siano almeno due in contrasto. E mentre certamente la libertà di espressione lo è, la verità – qualunque cosa sia; da Pilato a Tarski se lo sono chiesti in molti – dei dati veicolati in pubblico, salvo casi eccezionali, non sembra esserlo altrettanto.
Veniamo, infine, a una terza accezione di *fake news*: affermazioni non vere che ledono o mettono in pericolo interessi individuali o collettivi riconosciuti in Costituzione. Una dichiarazione offensiva e falsa; la diffusione di dati personali scorretti o di notizie fuorvianti in grado di condizionare l'andamento dei mercati.
Questo è il solo terreno in cui si possono utilizzare le categorie di *legale* e di *illegale*. E siccome quel che è illegale off line è illegale on line, sembra anche l'unico campo in cui il legislatore sembra poter legittimamente e fruttuosamente fare applicazione di divieti e sanzioni penali.

3 Diversi paradigmi di attribuzione della responsabilità.

Si è visto qual è l'unica tipologia, se così si può chiamare, di *fake news* a cui pare ipotizzabile applicare una pena. Ora cerchiamo di precisare chi può essere punito.
Il meccanismo per così dire "classico" di attribuzione della responsabilità passa attraverso il principio personalistico, per cui risponde chi fa le cose, o meglio, in base ai principi sul concorso di persone nel reato tutti coloro che hanno contribuito causalmente alla realizzazione del fatto. Certo, esiste anche la possibilità di ascrivere la responsabilità penale a titolo omissivo, tuttavia è necessario che il "reo" avesse l'obbligo giuridico di impedire il fatto illecito verificatosi. È cioè necessaria una posizione di garanzia, che può derivare dalla legge, da un contratto o dall'esercizio di una precedente attività.
Nell'ambito del diritto dell'informazione l'art. 57 c.p. – che stabilisce una posizione di garanzia per il direttore responsabile di una testata per i fatti illeciti commessi mediante la testata stessa – è certamente la disposizione più applicata. Essa, fino a qualche tempo fa con certezza, era applicabile soltanto alla carta stampata. Prima del 2015, infatti, una giurisprudenza solida, partendo dal presupposto per cui Internet non è riconducibile alla nozione di stampa prevista dall'art. 1 della legge n. 47 del 1948, escludeva l'applicabilità alla rete di disposizioni incriminatrici, come quella menzionata, o di aggravanti, in base al noto divieto di analogia *in malam partem* in materia penale[9].
La ricerca di un meccanismo di attribuzione di responsabilità per i fatti illeciti in rete è probabilmente uno dei problemi di maggior rilievo degli ultimi anni nella materia del diritto dei media. E ciò non soltanto per ragioni di ordine sistematico, bensì per esigenze molto concrete, in primo luogo la frequenza con cui si presentano casi di illeciti commessi in rete, in seguito ai quali si vaga alla ricerca della disposizione adatta.

---

[6] C. Esposito, *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Milano, 1958, 36-37; A. Pace, M. Manetti, *Commentario della Costituzione. Art. 21*, Bologna, 2006, 89-90.
[7] P. Barile, *Diritti dell'uomo e libertà fondamentali*, Bologna, Il Mulino, 229; G.E. Vigevani, *Radici della Costituzione e repressione della negazione della Shoah*, in *Rivista AIC*, 2014, n. 4; A. Pugiotto, *Le parole sono pietre? I discorsi di odio e la libertà di espressione nel diritto costituzionale*, in *Diritto Penale Contemporaneo. Rivista trimestrale*, 2013, 77.
[8] *United States v. Alvarez*, 567 U.S. 709 (2012).
[9] Si pensi alle sentenze della V sezione penale della Cassazione n. 35511/2010, n. 44126/2011 e n. 23230/2012.

Le ragioni di tale imponente casistica sono molteplici, eccone alcune: rispetto al passato, sono numerosissime le persone che si sono trovate a diffondere il proprio pensiero, magari la maggior parte di esse senza un grande pubblico, ma soltanto alle decine o centinaia di "amici" su Facebook, così come, specularmente, sono numerosissime quelle che si sono trovate protagoniste di un episodio narrato o di un giudizio espresso da altri. Accade inoltre che l'assenza di contatto fisico tra chi scrive e chi legge diminuisca i freni inibitori. Il messaggio, poi, una volta diffuso in rete, rimane ed è reperibile con facilità, se si trova la parola chiave che lo rintracci. Ma uno dei problemi che rende insidiosa la rete e complesso ipotizzare soluzioni per gli illeciti ivi commessi, è la facilità con cui l'autore del messaggio può celarsi dietro l'anonimato, magari in astratto non impenetrabile, ma che diventa tale in concreto perché la maggioranza dei privati non ha mezzi per superarlo e l'autorità giudiziaria ha risorse scarse rispetto all'imponenza della casistica.
Di fronte a questa situazione, una soluzione che non frustri la legittima domanda di giustizia delle persone offese implica un'alternativa. O si vieta (al più si sfavorisce) la possibilità di usufruire dell'anonimato, o si individua un terzo soggetto noto, o che ha l'obbligo di mostrarsi, a cui porre in capo la responsabilità del messaggio (dall'ISP al gestore del sito).
Forse la scarsa simpatia per le ortodossie in genere fa sì che né l'una né l'altra paiano del tutto convincenti. Cerco di spiegarne le ragioni assumendo per entrambe due punti di vista: uno *de iure condito* e l'altro *de iure condendo*.

3.1 (segue) Il divieto di anonimato.

Oggi un divieto di anonimato può essere applicato ai contenuti diffusi in rete applicando, in modo evolutivo va da sé, le disposizioni previste per la stampa. Più precisamente, bisognerebbe riferire ai siti Internet le disposizioni della legge stampa sulla individuazione dei responsabili e sulla registrazione. Col risultato di imporre ad ogni sito, come per gli stampati, l'obbligo di indicare almeno il nome di un responsabile e la data di immissione in rete e per i periodici la registrazione presso la cancelleria del tribunale.
Seguendo questa impostazione, però, per le sanzioni previste per la stampa clandestina si porrebbe un serio problema di analogia *in malam partem*, costituzionalmente vietata in materia penale. La questione potrebbe, in teoria, essere risolta attribuendo al termine «stampa» il significato «figurato» che di recente, in materia di sequestro, la Cassazione ha ritenuto di assegnarle. Più precisamente, la Suprema Corte a Sezioni Unite, sia in sede penale[10], sia poco dopo in sede civile[11], ha stabilito che le disposizioni di cui all'art. 21 Cost. a tutela del sequestro di stampati siano applicabili anche ad alcuni contenuti diffusi in rete. E ciò in quanto, secondo la Corte, almeno in materia di sequestri, la nozione di stampa o stampati non deve essere tratta dall'art. 1 della legge n. 47 del 1948, che ne fornisce appunto la definizione. Sarebbe viceversa necessario interpretare tale termine in modo, appunto, "figurato": la stampa equivarrebbe ai giornali, che diffondono informazione in modo professionale.
Le difficoltà di applicare una simile regola, tuttavia, sono molte. A cominciare da quella di stabilire, in un mondo liquido come la rete, quale sia l'informazione professionale e quella non professionale, per continuare con gli interrogativi sulla ragionevolezza di un obbligo di identificazione soltanto per i giornali *online* e non per tutti gli altri siti e blog, laddove evidentemente i primi sono più controllati dei secondi. Inoltre, sarebbe quasi paradossale che l'ordinamento pretendesse una maggior trasparenza sugli autori di stampati cartacei anche non periodici, che su chi diffonde messaggi in rete.
Ma nemmeno *de iure condendo* la soluzione di introdurre un divieto di anonimato in rete, assistito da una sanzione penale, sembra quella corretta. Anzitutto, in generale, poiché essendo la libertà di manifestazione del pensiero, almeno tradizionalmente, una libertà "negativa", meno è circondata da divieti e più si estendono i suoi benefici. In secondo luogo, non pare che la diffusione in forma anonima di un pensiero di per sé offenda a tal punto un bene giuridico costituzionalmente tutelato da consentire di introdurre una punizione per tale comportamento.
Infine, una considerazione di ordine pratico: risulta assai complicato imporre in modo rigoroso il divieto di anonimato. E anche se ciò fosse possibile, lo sarebbe a scapito di una notevole burocratizzazione della comunicazione *online*, circostanza che se non altro ingesserebbe il fenomeno, tanto da snaturarlo. Questo punto non è di poco rilievo poiché, in presenza di un fatto di per sé non

[10] Cass. pen., sez. un., sent. 31022/2015.
[11] Cass. civ., sez. un., sent. 23469/2016.

illecito, anzi che costituisce la manifestazione di una libertà costituzionale, il legislatore dovrebbe soltanto prendere atto di quel che accade e intervenire per regolarlo ove strettamente necessario. Non dovrebbe, invece, con la propria azione, determinare modificazioni e cambiamenti radicali nel fenomeno stesso.

3.1 (segue) La responsabilizzazione di chi gestisce il sito o la piattaforma.

Anche in questo caso proviamo ad analizzare se una responsabilizzazione di terzi sia possibile con le regole oggi in vigore o se sia auspicabile con un intervento del Parlamento.
Le ragioni della spinta ad attribuire una responsabilità al gestore del sito o della piattaforma sono almeno due: anzitutto si tratta di un soggetto identificato o identificabile facilmente e poi si tratta anche di chi, da un lato, ha la signoria sui contenuti e dunque può porre barriere all'ingresso di contenuti illeciti, dall'altro, guadagna – in termini economici o di notorietà – dal mantenimento in rete dei contenuti in questione.
Va detto, però, che quella "per pubblicazione" sembra una classica responsabilità commissiva; per renderla punibile anche a titolo omissivo è necessaria una posizione di garanzia che non può certo essere individuata dalla giurisprudenza.
E se il legislatore, con il proverbiale tratto di penna, aggiungesse una simile posizione di garanzia? A mio avviso otterrebbe un doppio risultato negativo. In primo luogo aumenterebbero i soggetti penalmente responsabili con la difficoltà però di rinvenire una concreta rimproverabilità in capo ad essi, circostanza che creerebbe non poca tensione con l'elemento soggettivo del reato. In secondo luogo, l'attribuzione di responsabilità porta con sé anche un'inevitabile concessione di signoria sui contenuti, che verrebbero perciò sottoposti a rigorosa censura. È prevedibile che i gestori, anche solo per evitare di incorrere in "guai" giudiziari, eliminerebbero ogni contenuto sensibile, col risultato di creare un appiattimento generale della comunicazione. L'osservazione è talmente nota e condivisa che qui è impossibile fornire una bibliografia, anche solo essenziale. Piace, però citare almeno Balkin[12], che parla di «*collateral censorship*», se non altro perché l'argomento è stato ripreso anche da una *dissenting opinion* (Sajo-Tsotsoria) nella sentenza della Grande Camera nel caso *Delfi*, di cui tra un attimo.

4 Una soluzione alternativa.

Un possibile compromesso rispetto alle due strade sopra descritte potrebbe essere quello di porre una responsabilità, solo di tipo risarcitorio, quindi non penale, in capo a terzi, esclusivamente a determinate condizioni, nel caso in cui, ad esempio, costoro non contrastino l'anonimo autore di contenuti illeciti e non collaborino con le persone offese.
In materia di "rimproverabilità" ai gestori di siti o piattaforme per i contenuti prodotti da terzi, la disposizione oggi di riferimento è l'art. 16, d.lgs. 70/2003 che, appunto, la esclude a meno che il titolare non sia a conoscenza di un contenuto chiaramente illecito e non lo rimuova nonostante una esplicita richiesta dell'autorità. Al legislatore si potrebbe chiedere un intervento, prendendo spunto dai suggerimenti della Corte Europea (stiamo parlando in particolare della sentenza CEDU *Delfi c. Estonia*[13]). Più precisamente, si potrebbe prevedere una responsabilità civile per danni in capo al gestore del sito o della piattaforma qualora: non tenti l'identificazione dei soggetti che pubblicano; non registri e non conservi i file di log almeno per un certo periodo; non comunichi tali dati, anche a richiesta del privato, al fine di far valere un diritto in giudizio; non imponga filtri automatici per evitare gli insulti più comuni; non elimini i contenuti palesemente illeciti anche a richiesta del privato. Ferme restando responsabilità civile e penale dell'autore del messaggio, quindi, il gestore del sito o della piattaforma potrebbe essere chiamato a rispondere dei danni derivanti dalla pubblicazione, a condizione che con la propria inattività abbia favorito la realizzazione del fatto, ne abbia aggravato le conseguenze o non abbia collaborato affinché l'autorità, chiamata ad occuparsene, possa giudicarne la liceità. Una responsabilità limitata alla sede civile, poiché analoga previsione in sede penale pare assai più difficilmente armonizzabile con i principi generali del sistema.
Si tratta comunque di una disposizione non semplice da scrivere. Il tema è delicato perché, solo

[12] J.M. Balkin, *Free Speech and Hostile Environments*, in *Columbia Law Review*, 1999, ora consultabile in jackbalkin.yale.edu.
[13] CEDU, *Delfi c. Estonia*, ric. 64669/09 (2015).

per fare un esempio, si rischia da una parte di prevedere obblighi inesigibili, qualora si imponga una vera e propria identificazione, dall'altro se ci si limiti a chiedere un tentativo in tal senso non è improbabile che la norma resti "lettera morta".

Una seconda soluzione che, insieme alla prima, potrebbe migliorare l'attuale stato di profonda anarchia che regna nella materia è l'introduzione di una disciplina che estenda il diritto di replica e rettifica dalla stampa al web. Sul modello di quanto previsto dall'art. 8 della legge stampa, si potrebbe prevedere il diritto per il soggetto interessato a rispondere o rettificare fatti che lo riguardano, purché falsi e lesivi di diritti, a patto che il testo sia di dimensione contenuta e non penalmente rilevante. Dovrebbe essere introdotta anche la possibilità per l'interessato di rivolgersi velocemente al giudice per ottenere la pubblicazione qualora questa, pur in presenza dei requisiti di legge, non fosse stata effettuata.

Insomma, pare equilibrato un ordinamento in cui, di fronte a una diffamazione *online* commessa divulgando un fatto consapevolmente falso, l'autore dell'affermazione ne risponda in sede penale e civile, mentre il titolare del sito ne risponda, sia pure solo in sede civile, e qualora non collabori (anche con l'interessato e non solo con l'autorità giudiziaria) per rinvenire il responsabile e minimizzare gli effetti della sua condotta, non tenti in generale di contenere l'anonimato e non consenta risposte e rettifiche.

C'è la consapevolezza che l'ordinamento, in verità, sembra andare nella direzione opposta. Basti pensare, per quanto riguarda l'azione del legislatore, al ddl "Gambaro" citato all'inizio, ma anche alla legislazione tedesca di recente approvata che attribuisce ai gestori delle piattaforme un ruolo paragiurisdizionale, nonché li rende destinatari di sanzioni non irrilevanti. Per quanto riguarda invece la giurisprudenza, si pensi alla recente sentenza in cui sembra che la V sezione penale della Cassazione abbia ritenuto responsabile il gestore di un blog per contenuti prodotti da terzi, solo perché sarebbe stato a conoscenza degli stessi[14], o alle menzionate pronunce delle Sezioni Unite civili e penali in materia di sequestro in cui si delinea una nozione di "stampa" che, se sarà generalmente utilizzata, consentirà di estendere la responsabilità per omesso controllo anche al direttore di una testata telematica[15].

Ma, si sa, come affermava quel filosofo di Charles M. Schulz, per bocca di Snoopy, «un'intera montagna di consapevolezze non uguaglierà mai una piccola speranza».

[14] Cass. pen., sez. V, sent. 54946/2016; per un commento si veda R. Carbone, *Responsabilità del blogger: parziale revirement della Cassazione?*, in *Cassazione penale*, 2017, 2782 ss., nonché, volendo C. Melzi d'Eril, *Una pronuncia problematica in materia di responsabilità del gestore del sito web per i commenti diffamatori pubblicati dai lettori*, in *questa Rivista.*

[15] Per qualche primo spunto si veda C. Melzi d'Eril – G.E. Vigevani, *Diffamazione, il gestore del sito non risponde se elimina i commenti*, in www.ilsole24ore.com, 10 marzo 2017.

Alcune riflessioni preliminari (e provvisorie) sui rapporti tra i motori di ricerca ed il pluralismo informativo

Some Preliminary Thoughts on the Relationship Between Search Engine Service Providers and Media Pluralism

Roberto Borrello
Professore ordinario di Diritto costituzionale presso l'Università degli Studi di Siena

Abstract

Il contributo affronta la delicata ed ancora poco esplorata problematica della qualificazione della posizione giuridica dei c.d. motori di ricerca, rispetto alla tutela del pluralismo informativo quale valore fondante della forma di stato democratico di derivazione liberale. Partendo dalla ricostruzione della varietà e peculiarità dei diversi attori che animano il mondo di Internet, viene criticata la visione che tende ad attribuire un ruolo di meccanici ed acritici "trasportatori" di contenuti informativi, ai motori di ricerca, come tali non sottoponibili alla varia tipologia di strumenti elaborati nei vari ordinamenti a tutela del pluralismo. Si evidenziano a tale riguardo i profili, connessi anche all'attuale evoluzione qualitativa dei *search engines*, che renderebbero invece necessari interventi intesi a garantire il pluralismo, con particolare riguardo all'ambito dell'ordinamento italiano, anche se in forme e con qualificazioni che, allo stato dell'arte, appaiono realizzabili più *de iure condendo* che *de iure condito*.

The article aims at tackling the controversial legal qualification of search engine service providers, with particular regard to their impact on media pluralism, meant as founding value of liberal democracy. Moving from an overview of the different actors operating on the Internet, the understanding of search engines as purely passive conveyors of third parties information, resulting in the exclusion of the same from the scope of the legislation protecting media pluralism, is subject to criticism. The paper explores some distinguishing features of the evolving nature and role of search engines, in light of which some interventions are claimed to be necessary with a view to ensuring media pluralism.

Sommario

Internet
libertà di espressione
motori di ricerca
pluralismo informativo
media

1 La problematica dei rapporti tra principio del pluralismo informativo e rete Internet, sul piano del ruolo dei motori di ricerca. Profili introduttivi generali.

Ricordava Paolo Caretti, in un convegno su Internet ed il pluralismo[1], le parole di Carl Schmitt: «la terra è il luogo del diritto, il mare il luogo della libertà». Adattando questa affermazione al contesto contemporaneo, secondo Caretti, Internet dovrebbe essere il mare (virtuale) degli internauti, ma tale mito va a suo avviso sfatato, in quanto l'esperienza degli ultimi anni ha dimostrato a chiare lettere che Internet è spesso luogo di scontro di interessi diversi e richiede anche regolazione.
Appare interessante, in tale quadro, la possibile rilevanza di una categoria degli operatori del web, i motori di ricerca, nel contesto della tutela del pluralismo informativo, alla luce di un recente conflitto tra Agcom e Google, in ordine all'obbligo da parte di consociate di tale gruppo di fornire dati sulla situazione economica mediante la c.d Informativa Economica di Sistema-IES.
La centralità del principio del pluralismo nell'ambito degli ordinamenti nazionali, sovranazionali ed internazionali, regionali e non[2], quale strumento di tutela della libertà di pensiero, intesa nella dimensione della libertà di informazione (che comprende, a sua volta il diritto ad informare ed ad essere informati), è un dato ormai consolidato.
L'essenza del pluralismo informativo consiste nella efficace circolazione delle diverse idee ed opinioni, che è, strategicamente, una delle condizioni essenziali per il funzionamento dello stato democratico nella sua attuale evoluzione, in quanto consente ai cittadini di esercitare la sovranità in modo informato e consapevole, rendendo effettiva l'eguaglianza nell'esercizio del voto.
L' efficace attuazione di tale fondamentale principio richiede che vi sia il più ampio numero possibile di voci presenti nell'area pubblica di discussione e dibattito (pluralismo esterno) e che vi sia il rispetto da parte di tutte tali voci, pubbliche o private, sia pure con diversa intensità, di regole di indipendenza, obiettività e completezza nell'attività comunicativa, al fine di garantire il diritto ad essere informati dei cittadini (pluralismo interno o dei contenuti).
In Italia, come in tutti i paesi di quelle che, una volta, si chiamavano, *lato sensu*, le democrazie occidentali, l'attenzione è stata rivolta, in origine, soprattutto nei confronti di mezzi di comunicazione ad alta valenza suggestiva, quali la televisione, nel momento in cui è stato superato il modello del monopolio pubblico ed è stata ammessa l'iniziativa privata in un contesto "misto".
In particolare, dopo che la sentenza n. 148 del 1981 della Corte aveva già condizionato l'apertura ai privati nel settore televisivo a livello nazionale all'adozione di norme antitrust (evidenziando il lato del pluralismo esterno), si è accentrata l'attenzione anche sui profili di pluralismo interno, non limitati alla presenza necessaria del servizio pubblico, ma anche da riferire ai soggetti privati, specie, come si ricordava più sopra, nel settore della comunicazione politica. Al di là del dibattito sollevato sulla compatibilità del modello di pluralismo interno così configurantesi con la caratterizzazione in senso liberale e non funzionale della libertà di manifestazione del pensiero con ogni mezzo di diffusione *ex* art 21 cost. (v. in tal senso la sent. n. 155 del 2002 della Corte e la giurisprudenza del giudice amministrativo favorevole verso alcune regolazioni dell'Agcom attuate dal 2006 in poi[3]), ciò che in questa sede ci interessa evidenziare è il modello di garanzia del pluralismo esterno attuato nel nostro ordinamento a partire dal 2004, mediante la legge n. 112 (c.d Gasparri)[4] e con la creazione del c.d. Sistema Integrato delle Comunicazioni – SIC.
Vi sono vari modi di attuare il pluralismo esterno. Una tendenza tipica della disciplina dell'informazione, al fine della tutela del pluralismo è stata, nel passato, quella di attuare gli interventi secondo una logica di differenziazione basata sulle caratteristiche dei mezzi di comunicazione usati (la grande dicotomia originaria è stata, notoriamente, quella tra stampa e televisione e quindi con norme anticoncentrazione nel primo settore e limiti tecnici concernenti il mezzo nel secondo).
La successiva convergenza e digitalizzazione hanno determinato approcci regolativi basati invece su una considerazione complessiva o quantomeno aggregata per talune tipologie di mezzi, con l'applicazione dell'approccio di tipo antitrust, ma adattato alla logica del pluralismo delle voci, inteso a vietare posizioni dominanti consistenti nel superamento di un certo livello della titolarità dei

[1] Convegno svoltosi alla Università Bocconi il 5 giugno 2013: v. il resoconto in http://www.millecanali.it/Internet-e-il-pluralismo/ .
[2] Per una ricostruzione ampia del tema, con indicazioni dottrinarie e giurisprudenziali, appare utile l'allegato A alla delibera 28 ottobre 2010, n. 555/2010/CONS ("Procedimento per l'individuazione dei mercati rilevanti nell'ambito del sistema integrato delle comunicazioni"), 37 ss.
[3] Su cui v. A. Pace, *Libertà di informare e diritto ad essere informati:due prospettive a confronto nell'interpretazione e nelle prime applicazioni dell'art. 7, primo comma del T.U. della Radiotelevisione*; in V. Cuffaro - G. Di Rosa (a cura di), *Studi in onore di Nicolò Lipari*, Milano 2008, t. 2, 1995 ss.
[4] L. 3 maggio 2004, n. 112, poi trasfusa ed integrata nell'ambito del d.lgs. 31 luglio 2005, n.177 (Testo Unico della Radiotelevisione), a sua volta, successivamente, modificato ed integrato con il d.lgs. 15 marzo 2010, n. 44, con l'assunzione dell'attuale denominazione di Testo Unico dei Servizi di Media Audiovisivi e Radiofonici (d'ora in poi TUSMAR).

ricavi nell'ambito aggregato di riferimento.
Tra le varie soluzioni si può ricordare ad esempio il modello statunitense, elaborato dalla *Federal Communications Commission* (FCC) nel 2003, del *Diversity Index* (DI), basato sull'assunto che alcuni media (quotidiani, settimanali, TV via etere, radio e Internet, ma non altra stampa periodica, come i mensili, la TV satellitare e via cavo) debbano essere considerati come tutti afferenti a un unico mercato ma che l'impatto di ciascuno (cioè la "presa" sull'opinione pubblica e la capacità di influenzare quest'ultima) cambi da caso a caso e quindi sia necessario ponderare il peso specifico di ciascun medium. In altri ordinamenti si è tentato poi di introdurre metodi basati non su fattori economici ma sulla qualità dell'informazione: in Germania, sin dal 1997, la Commissione sulla concentrazione nei media (*Kommission zur Ermittlung der Konzentration im Medienbereich*, KEK) è andata sviluppando un meccanismo di tutela del pluralismo, applicato al mercato televisivo, basato sul criterio del potere predominante nella formazione dell'opinione pubblica, che a nessun soggetto deve essere consentito detenere, avendo riguardo al potere suggestivo del messaggio diffuso, così come nel Regno Unito grazie alla riforma varata con il *Communications Act 2003* l'*Ofcom* utilizza un controllo battezzato *public interest o plurality test* che utilizza un mix di criteri di pluralismo esterno ed interno[5].
In questa prospettiva, il modello del SIC italiano[6] vorrebbe attuare l'approccio integrato sopra indicato attraverso la creazione di un coacervo comprendente le attività inerenti alla stampa quotidiana e periodica, all'editoria annuaristica ed elettronica, alla radio e ai servizi di media audiovisivi, al cinema, alla pubblicità esterna, alle iniziative di comunicazione di prodotti e servizi, nonché alle sponsorizzazioni. E' a tale "calderone" che si commisura la posizione dominante di un soggetto (20%). In ogni caso, la legge demanda all'Agcom, la vigilanza sulle concentrazioni monosettoriali, autorizzandola a porre in essere misure che vanno dal mero richiamo a l'imposizione di dismissione di aziende o di rami d'aziende (T.U. radiotelevisione, art. 43 cc. 1-5).

2 La rete Internet ed il Sistema Integrato della Comunicazione – SIC nell'ordinamento italiano.

Rispetto al SIC, la rete Internet non è stata presa in origine in considerazione, se non, appunto, in ordine all'editoria elettronica "anche via Internet".
La limitatezza di tale visione è stata ben presto evidenziata dall'Agcom.
In particolare, con la delibera di indizione di una consultazione pubblica[7], l'Agcom osservava che «nell'attuale formulazione del TU rientra la mera editoria elettronica (anche attraverso tale mezzo) che rappresenta, come ampiamente dimostrato da questa istruttoria, un segmento di un più ampio mercato, al momento riconducibile ad Internet, nella sua parte finale di fruizione di contenuti e servizi (ma non di accesso). Internet rappresenta non solo un ambito economico al momento unitario, ma anche il terzo mezzo di informazione per i cittadini italiani, con un'assoluta valenza ai fini del pluralismo, sia attuale che, ancor più, prospettica. In questo senso, si suggerisce un intervento del Legislatore volto a ridefinire le aree economiche rilevanti ai fini di un'analisi a tutela del pluralismo in senso più conforme a quanto appena illustrato. Più in generale, appare auspicabile un approccio più flessibile di quello attuale che preveda la possibilità per l'Autorità di considerare anche nuovi ambiti di attività che dovessero emergere in conseguenza dell'evoluzione tecnologica e di mercato».
Tali considerazioni erano ribadite nell'allegato A alla delibera 555/10/CONS[8], resa in esito alla sopra menzionata indagine ed intesa alla «individuazione dei mercati rilevanti nell'ambito del sistema integrato delle comunicazioni», nella quale si rilevava che «includendo nel Sistema Integrato delle

[5] V. ampie indicazioni sulle forme della tutela del pluralismo in prospettiva comparata nell'allegato A alla delibera Agcom n. 555/2010/CONS., cit., 47 ss. V. per il *diversity index* negli USA, A. Marcus, *Media Diversity And Substitutability: Problems with the FCC's Diversity Index*, in *A journal of law and policy for the information society*, 2007.
[6] Su cui v. A. Valastro - R. Zaccaria - E. Albanesi, *Diritto dell'informazione e della comunicazione,* Padova, 2014, 515 ss.
[7] Delibera 367/10/CONS, allegato B, 230 – 231. In tal senso anche la più recente delibera 41/17/CONS, riferita alla individuazione dei mercati riferibili ai servizi di media audiovisivi - SMA, allegato A, 8, n. 37.
[8] V. *supra*, nota 2.

Comunicazioni soltanto l'attività di editoria elettronica, come sopra definita[9] e chiaramente rilevante ai fini della tutela del pluralismo, rimangono escluse tutte le altre forme di comunicazione on line, non qualificabili come prodotti o servizi di editoria elettronica, ma ugualmente rilevanti. Infatti, l'attività di diffusione di informazioni al pubblico tramite il web è svolta tanto da soggetti già operanti nel settore delle comunicazioni di massa - in comparti anche diversi da quello editoriale - quanto da aggregatori di notizie, gestori di portali, *social network,* blogger»[10]. Tuttavia la stessa Autorità evidenziava che «in tale contesto, una corretta interpretazione del dato normativo non consente di estendere il concetto di editoria elettronica oltre a quello descritto nel procedimento…» e veniva riaffermata la necessità di «una modifica normativa» per attuare tale necessaria estensione.
A tale riguardo, nello stesso Allegato, l'Autorità aveva premesso, su un piano generale, che la finalizzazione del processo di definizione dei mercati del SIC alla tutela del pluralismo presuppone uno scrutinio circa la rilevanza di tali ambiti merceologici e geografici rispetto agli obiettivi individuati dal legislatore[11]. A tal fine l'Agcom effettuava una fondamentale distinzione tra i mercati potenzialmente rilevanti ai fini della garanzia de pluralismo (quelli connessi all'attività radiotelevisiva e all'editoria quotidiana e periodica) e le altre aree economiche elencate nel Testo Unico (annuaristica, cinema, pubblicità esterna, iniziative di comunicazione, sponsorizzazioni) che «seppur rientranti nel comparto della comunicazione, rilevano rispetto ad altri profili del pluralismo (culturale per il cinema, politico per la pubblicità esterna) e non appaiono, già prima facie, avere una specifica valenza per le garanzie del pluralismo»[12]. Veniva ribadito, tuttavia, che «[n]on vi è dubbio alcuno poi che, nonostante il legislatore non lo abbia esplicitamente considerato, Internet si pone oggi, e ancora di più in prospettiva, come un mezzo di pregnante rilevanza ai fini della tutela del pluralismo.»
In quel momento, quindi, *de iure condito*, l'offerta di informazione on line, secondo modalità distinte dalla tradizionale nozione di editoria elettronica (intesa come offerta periodica di prodotti editoriali su supporto digitale), non poteva essere presa in considerazione sotto nessun punto di vista ai fini della tutela del pluralismo, secondo il modello del SIC[13].
L'invito delle autorità di regolazione a valutare i profili qui sopra messi in luce, non è stato recepito dal legislatore attraverso una proposta di origine governativa, ma attraverso un emendamento politicamente trasversale (PDL-PD) introdotto nei confronti del d.l. 18 maggio 2012, n. 63, conv. con l. 16 luglio 2012, n. 103 (Disposizioni urgenti in materia di riordino dei contributi alle imprese editrici, nonchè di vendita della stampa quotidiana e periodica e di pubblicità istituzionale»), all'art. 3, comma 5-*bis*. Tale emendamento ha inserito nel comma 10 dell'art. 43 del TUSMAR un inciso che ha aggiunto, tra i ricavi rilevanti al fine del calcolo dell'ammontare del SIC a cui commisurare il tetto del 20%, quelli derivanti «da pubblicità on line e sulle diverse piattaforme anche in forma diretta, incluse le risorse raccolte da motori di ricerca, da piattaforme sociali e di condivisione». Nel contempo ha introdotto l'obbligo di iscrizione nel registro degli operatori della comunicazione (ROC: art. 1, comma 6, lett. a), numero 5), della l. 31 luglio 1997, n. 249) per le imprese concessionarie di pubblicità da trasmettere «sul web e altre piattaforme digitali fisse o mobili».
Sotto tale punto di vista va ricordato che, come più volte evidenziato dall'AGcom, il settore dei mezzi di comunicazione si compone di una serie di mercati, distinti ma collegati fra di loro, che presentano una struttura a due versanti[14]. Nel primo versante, i consumatori o utenti soddisfano attraverso il mezzo le proprie esigenze di informazione, comunicazione e intrattenimento. Nel secondo versante, gli inserzionisti di pubblicità domandano spazi pubblicitari all'editore del mezzo di comunicazione per promuovere i propri prodotti ai consumatori finali in cambio di un numero di contatti pubblicitari realizzati dal mezzo. Il mezzo di comunicazione gestito da un editore (di quotidiani, periodici), da un'emittente radiotelevisiva e/o da un sito Internet rappresenta pertanto l'elemento di congiunzione che consente di soddisfare la domanda dei due gruppi di consumatori: i fruitori del mezzo, da un lato, gli inserzionisti di pubblicità, dall'altro.

[9] La nozione "ristretta" di editoria elettronica ai sensi del SIC, è stata ricostruita dall'Agcom (vedi sempre Allegato A alla delibera 555/10/CONS, 188) mediante il riferimento al Regolamento per l'organizzazione e la tenuta del Registro degli operatori di comunicazione ("ROC"), approvato con delibera 666/08/CONS. In particolare, l'art. 2, comma 1, lett. *i)*, includendo tra i soggetti obbligati ad inscriversi al ROC quelli che esercitano un'attività di editoria elettronica, li definisce come quei soggetti che pubblicano in modalità elettronica testate diffuse al pubblico con carattere di periodicità, quotidiana o non quotidiana. Secondo l'Autorità, quindi, la norma, avrebbe introdotto il carattere della regolare periodicità della testata come requisito per poter essere qualificati soggetti esercenti l'editoria elettronica o digitale. In tal senso, notava sempre, l'Agcom, l'impostazione adottata dalla delibera di escludere l'editoria non periodica appare coerente con la scelta adottata dal legislatore di non considerare, tra le attività rilevanti ai fini del SIC, la stampa cartacea non periodica, quale l'editoria libraria.
[10] Allegato A, 199.
[11] *Ibidem*, 78.
[12] *Ibidem*
[13] Su tale base l'Agcom non riteneva sussistere un mercato rilevante autonomo, nell'ambito del SIC per l'editoria elettronica intesa nel senso ristretto sopra ricordato ed individuava i seguenti mercati: Mercato della televisione in chiaro; Mercato della televisione a pagamento; Mercato radiofonico; Mercato dell'editoria quotidiana; Mercato dell'editoria periodica (nell'ambito del quale veniva inserito quello dell'editoria elettronica).
[14] http://www.agcom.it/mercati-media

Ritenendo di dovere monitorare il mercato di Internet su entrambi i versanti ora descritti, l'Agcom ha richiesto l'invio dell'Informativa Economica di Sistema (IES) a tutti i soggetti che effettuano l'attività di raccolta pubblicitaria *online* in Italia, compresi quelli che realizzano ricavi sul territorio nazionale ma li fatturano all'estero[15].

Tale decisione ha provocato la reazione di Google contro il coinvolgimento di due sue consociate, aventi sede, una in Irlanda e l'altra in Italia, che hanno impugnato la delibera del 2013 dinanzi al TAR Lazio, sostenendo che l'impugnata delibera avrebbe illegittimamente esteso l'obbligo di comunicare all'Autorità, con scadenza annuale, i dati d'impresa contenuti nella c.d. "informativa economica di sistema" anche a società, come le ricorrenti medesime, che non presterebbero, in Italia, servizi di media audiovisivi, né sarebbero, comunque, attive nell'ambito dei settori economici che costituiscono il sistema integrato delle comunicazioni.

Il TAR del Lazio chiamato a decidere in tempi rapidi nel merito, ha sollevato una questione pregiudiziale *ex* art. 267 TFUE con ordinanza n. 8405/2015. Tale questione è così formulata: «se l'art. 56 del Trattato sul Funzionamento dell'Unione Europea (TFUE) osti all'applicazione dell'impugnata delibera dell'Autorità di garanzia delle Telecomunicazioni n. 397/13/CONS, e delle relative disposizioni di legge nazionale di riferimento ove interpretate nel senso indicato dalla medesima Autorità, che richiedono una complessa "informativa economica di sistema" (necessariamente redatta secondo le norme di contabilità italiane) sulle attività economiche svolte nei confronti dei consumatori italiani, motivata da finalità di tutela della concorrenza ma necessariamente connesse alle diverse e più limitate funzioni istituzionali della medesima Autorità di tutela del pluralismo nel settore considerato, ad operatori pur non ricompresi nell'ambito di applicazione della legislazione nazionale di disciplina del medesimo settore (Testo Unico dei Servizi di Media Audiovisivi e Radiofonici) ed in particolare, nella fattispecie in esame, ad un operatore nazionale svolgente solo servizi per la sua consociata di diritto irlandese nonché, con riferimento a quest'ultima, ad un operatore non avente sede e non svolgente attività con impiego di dipendenti sul territorio nazionale, ovvero se ciò costituisca una misura restrittiva della libera prestazione dei servizi all'interno dell'Unione Europea in violazione dell'art. 56 del Trattato» [16].

La causa C-322/15 è stata decisa dalla Corte con una ordinanza, ai sensi dell'art. 53, par. 2 e 94 del Regolamento di Procedura, con la quale è stata pronunciata la "irricevibilità manifesta" per mancanza di sufficienti precisazioni concernenti il contesto di fatto e di diritto della controversia nel giudizio principale nonché le ragioni che giustificano la necessità di una risposta alla questione pregiudiziale.

La Corte non è, quindi, entrata nel merito della questione, ma ha rilevato, pregiudizialmente, la mancata cooperazione da parte del giudice remittente nella ricostruzione del contesto nazionale e nella adeguata motivazione della effettiva pregiudizialità della questione[17].

La problematica è, comunque, di estrema complessità[18], in quanto involge diversi profili, tra cui anche quello della aterritorialità dello svolgimento di attività sul web e sulle società con sede legale estera ma sostanzialmente operanti in un certo ambito spaziale sul piano degli effetti economici. Ai nostri fini, tuttavia, l'aspetto che interessa è quello della possibile rilevanza del tipo di attività dei motori di ricerca ai fini della tutela del pluralismo.

---

[15] Vedi l'art. 2, comma 1, lett. e) della delibera 397/13/CONS: «Le imprese concessionarie di pubblicità: i soggetti che esercitano, direttamente o per conto di terzi, attività di negoziazione e conclusione di contratti di vendita di spazi pubblicitari da trasmettere mediante impianti radiofonici o televisivi o da diffondere su giornali quotidiani, periodici, sul web e altre piattaforme digitali fisse o mobili, sugli annuari, al cinema e attraverso agenzie di stampa». L'art. 3 comma 5, ult. periodo stabilisce che «Ai fini della dichiarazione, devono essere altresì considerati i ricavi realizzati sul territorio nazionale, anche se contabilizzati nei bilanci di società aventi sede all'estero». La lett. f) dello stesso art. 2 ribadisce, per altro, la nozione tradizionale di editoria elettronica, obligando alla IES «Gli editori, anche in formato elettronico, di giornali quotidiani, periodici oriviste, altre pubblicazioni periodiche ed annuaristiche e altri prodotti editoriali: 1) i soggetti editori di cui all'articolo 1, comma 1, e quelli equiparati di cui all'articolo 18, comma 1, della legge n. 416 del 1981, che pubblicano, anche in formato elettronico, testate diffuse al pubblico con periodicità quotidiana, o altri prodotti editoriali in misura superiore a dodici numeri l'anno; 2) gli altri soggetti editori, anche ad azionariato diffuso, che pubblicano, anche in formato elettronico, una o più testate giornalistiche diffuse al pubblico con regolare periodicità, ovvero prodotti realizzati su supporto informatico, destinati alla diffusione di informazioni presso il pubblico (con esclusione dei prodotti discografici o cinematografici), purché sotto la direzione di un giornalista o di un pubblicista (art. 46, legge n. 69 del 1963; C. cost., sent. n. 98 del 1968)».

[16] V. per una ricostruzione della vicenda D. Mula, *L'informativa economica di sistema alla luce della più recente giurisprudenza*, in *federalismi.it, - Focus TMT* - 28 settembre 2015.

[17] Ordinanza dell'8 settembre 2016, causa C-322/15. La Corte ha al riguardo rilevato che, sebbene la domanda di pronuncia pregiudiziale menzionasse nel complesso il quadro normativo che veniva in questione nel giudizio principale, essa però non indicava le disposizioni concretamente applicabili alla lite costituente l'oggetto di quest'ultimo. Non venivano esplicitati, in particolare, né la portata né il contenuto dell'obbligo di cui è stato esteso l'ambito di applicazione, ossia le informazioni che tali operatori economici sono tenuti, in virtù della IES, a fornire all' Agcom, nonché le implicazioni risultanti dal formulario predisposto dall' Agcom per gli operatori economici in questione. Al riguardo la Corte ha ricordato che la domanda di pronuncia pregiudiziale deve fornire tali fondamentali indicazioni «al fine di permettere ai soggetti interessati contemplati dall'articolo 23 dello Statuto della Corte di giustizia dell'Unione europea nonché alla Corte di valutare la conformità dell'obbligo suddetto al diritto dell'Unione, alla luce segnatamente della sua natura, del suo contenuto e della sua portata», nonché «di verificare se e in quale misura tale provvedimento sia idoneo e necessario per conseguire l'obiettivo di interesse generale che esso persegue».

[18] A questo punto si attende la pronuncia di merito da parte del TAR del Lazio, per la quale è stata fissata l'udienza pubblica del 31 gennaio 2018.

3 Pluralismo informativo e motori di ricerca: i nodi della problematica.

Su di un piano generale, occorre considerare, anche alla stregua della ricostruzione più sopra delineata, che i soggetti che operano nel web sono di diversa natura: a) soggetti operanti in altri settori tradizionali dei media, con offerta *online* (quotidiani e periodici); b) gli editori nativi digitali c) gli aggregatori (motori di ricerca, portali e altri siti) e i *social media* (*social network* e blog).
Ciò che vene contestato in sede giudiziale da Google è, tra l'altro, il carattere non editoriale della propria attività, nel senso della non idoneità a produrre e controllare contenuti informativi che sarebbe proprio del motore di ricerca.
Tale profilo è stato messo in luce in sede dottrinaria in sede di commento della modifica legislativa avvenuta nel 2012[19], sulla base di una equazione tra attività di predisposizione di contenuti informativi (nozione di editore) e legittimazione passiva alla tutela, a qualsiasi titolo, del pluralismo informativo.
Viene fatto anche riferimento al d. lgs. n. 70 del 2003, che classifica gli aggregatori tra i prestatori di servizi nella società dell'informazione, esimendoli da una serie di responsabilità, proprio in virtù della presunta assenza di controllo sui contenuti da essi trasportati (articoli da 14 a 17)[20]. Viene infine richiamata una certa giurisprudenza che ha escluso la responsabilità dei motori di ricerca in alcune fattispecie, proprio in ordine alla mancanza di controllo dei contenuti diffusi[21].
La peculiarità dell'attività svolta dai motori di ricerca nel Sistema Integrato delle Comunicazioni-SIC (Google è quello che detiene una posizione ampiamente dominante sul mercato della raccolta pubblicitaria), non determinerebbe, quindi, in tale prospettiva, un impatto sul pluralismo dell'informazione, così come invece avviene nel caso di monopolio in mercati quali quelli tipici dell'audiovisivo, da parte dei soggetti che creano il prodotto audiovisivo stesso e quindi fanno informazione (mentre i motori di ricerca aggregherebbero e diffonderebbero informazione fatta da altri).
Tuttavia, la posizione dottrinaria in esame pone in evidenza anche un profilo attinente alla natura degli stessi *search engines*, in ordine alla loro forte incidenza sulla mediazione tra interessi diversi, in quanto "intermediari digitali" che forniscono l'accesso all'informazione. In tal senso, viene evidenziato come i motori di ricerca siano di ausilio al pluralismo, inteso tanto come accesso quanto come scelta delle informazioni da parte degli utenti, aumentando le fonti da cui attingere e garantendo la totale personalizzazione dell'esperienza di ricerca[22].
Sembrerebbe, allora, emergere una ricostruzione in base alla quale i motori di ricerca, da un lato, favoriscono il pluralismo (e quindi sono rilevanti per il pluralismo), ma, dall'altro, non dovrebbero essere assoggettati ad alcuna forma di controllo connessa alla garanzia del mantenimento del pluralismo stesso (anche semplicemente attraverso l'obbligo imposto alle loro concessionarie di pubblicità, di fornire dati sull'ammontare dei loro ricavi ai fini del SIC), in quanto non influirebbero sui contenuti del pluralismo stesso.
La posizione ora ricostruita, se la si è ben compresa, non appare condivisibile, in quanto la sussistenza, comunque, di un impatto da parte dei motori di ricerca sulle dinamiche del pluralismo, determina una rilevanza che non può essere priva di conseguenze, secondo il ben noto principio della correlazione tendenziale tra potere (lato sensu) e responsabilità, da intendere anche, ai fini della latitudine della sua valenza giuridica, nelle sue alte implicazioni valoriali-etiche, secondo la nota lezione di Jonas[23].
In realtà, tale impatto, per i *search engines*, sembra sussistere sotto due punti di vista: a) in ordine al loro diretto (e rilevato dalla stessa posizione dottrinaria in esame) apporto al processo informativo, sia come diffusori di prodotti del pensiero (anche se non direttamente creati), sia in ordine alla determinazione delle condizioni per l'effettività del diritto ad essere informati dei cittadini; b) in ordine, comunque, anche alle forme di condizionamento che essi sono in grado di generare sui soggetti che realizzano in forma originaria i contenuti informativi).
Su tali aspetti, appare opportuno svolgere qualche ulteriore riflessione, da considerare *in progress*, vista anche la brevità del presente contributo.

---

[19] O. Pollicino, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider,* in ConsultaOnline, 2014.

[20] Per altro va fatto presente (ma v. anche *infra* nel testo) che all'art. 1, comma 6 della direttiva 2000/31 di cui il d.lgs. costituisce attuazione, si stabilisce che: «La presente direttiva lascia impregiudicate le misure adottate a livello comunitario, o nazionale nel rispetto del diritto comunitario, per promuovere la diversità linguistica e culturale e garantire la salvaguardia del pluralismo».

[21] O. Pollicino, *op. cit.*, 13 ss.

[22] Su tali profili v. lo studio a cura di L. Bolognini e G. Ragusa (Istituto Nazionale per la Privacy e la valorizzazione dei dati) del 2015 dal titolo Effetti dei motori di ricerca sul pluralismo dell'informazione - Aspetti giuridici e di analisi econometrica.

[23] H. Jonas, *Il principio responsabilità. Un'etica per la civiltà tecnologica* (trad.it. a cura di P. P. Portinaro), Milano 2009.

3.1 Sulla presunta ininfluenza dei motori di ricerca sul contenuto delle informazioni veicolate. La connessione tra l'attività dei motori di ricerca ed il diritto ad essere informati come diritto ad accedere a tutti i prodotti del pensiero a diffusione generalizzata presenti nello spazio pubblico di discussione.

Quanto al primo aspetto, sembra debba essere oggetto di più attenta riflessione il sopra segnalato profilo della presunta assenza di una capacità di influire sui contenuti dei prodotti del pensiero (informazioni raccolte sul web) che da essi vengono trasmessi verso gli utenti.
Si può partire al riguardo, dall'insegnamento della nostra Corte costituzionale che ha evidenziato come la libertà di manifestazione del pensiero comprenda anche la diffusione di pensiero "altrui" (sent. n. 94 del 1977[24]), che, nel contesto della rete digitale, potrebbe portare a considerare come processi comunicativi *ex* art. 21 Cost., la veicolazione di pensiero altrui, selezionato dai motori di ricerca, che ne farebbero *content provider*, piuttosto che *service provider*.
Su di un piano generale, in un' ottica di superamento di una visione tradizionale della individuazione di un ruolo attivo nei processi di circolazione dell'informazione, va segnalato quel relativamente recente orientamento giurisprudenziale che, attento alla necessità di non sottrarre nessun processo rilevante nel contesto del sistema delle comunicazioni, ha incluso i pacchetti di abbonamento a pagamento diffusi dalla piattaforma satellitare Sky tra i SMA (servizi di media audiovisivi), rilevanti, sul piano dei ricavi, al fine della loro inclusione nella IES, ancorchè essi non siano riconducibili ad una diretta responsabilità editoriale da parte dell'operatore satellitare[25].
I motori di ricerca sono certamente esclusi dall'area dei SMA, ai sensi dell'art. 1, comma 1, lett. a, n.1, lett. (c) del TUSMAR, ma l'orientamento segnalato appare importante, per come detto, nell'ottica della conferma della considerazione dell'influenza sui processi comunicativi di attività comunque idonee alla diffusione di prodotti del pensiero, anche se non intesi direttamente ad esprimere un pensiero proprio del "diffusore".
In ogni caso, al di là della loro neutralità o meno rispetto ai contenuti diffusi, i motori di ricerca non possono considerarsi irrilevanti per il pluralismo informativo a causa della loro oggettiva incidenza sull'esercizio di diritti fondamentali.
Tale incidenza non è stata evidenziata soltanto a livello nazionale, ma anche nell'ambito dell'Unione europea. Va ricordata, in primo luogo, la fondamentale decisione della Corte di Giustizia UE del 13 maggio 2014 (*Google Spain*, C-131/12) nella quale, si è sottolineato il ruolo importante che svolgono Internet e i motori di ricerca nella società moderna, i quali conferiscono alle informazioni contenute in un siffatto elenco di risultati carattere ubiquitario", richiamandosi l'altra fondamentale sentenza *eDate Advertising e a.* (C-509/09 e C-161/10, punto 45).
Di conseguenza, anche attribuendo a Google un mero ruolo di "intermediario" nell'informazione, tale ruolo appare estremamente importante e cruciale nell'ambito dei complessi processi che caratterizzano la circolazione delle idee e delle opinioni nello spazio pubblico.
In particolar modo acquista rilievo il profilo della tutela del segmento più importante del processo dell'informazione pubblica e cioè quello della ricezione dell'informazione da parte dei cittadini, nella specie come utenti del web.
Della libertà fondamentale di ricevere informazioni, quale aspetto della libertà di informazione garantito dall'art. 11, paragrafo 1, della Carta ha parlato la Corte di Giustizia UE nella decisione del 2013 (*Sky Österreich,* C-283/11), ritenendo legittime misure, a livello dell'Unione, che comportano limitazioni della libertà d'impresa privilegiando, con riguardo alla necessaria ponderazione dei diritti e degli interessi in gioco, l'accesso del pubblico all'informazione rispetto alla libertà contrattuale.
Il pluralismo nel contesto europeo tende a garantire che gli Stati adottino politiche funzionali a promuovere la libertà di informazione sia dal punto di vista degli operatori, ma sia anche da quello degli utenti. Infatti, i governi hanno un ruolo attivo nel garantire la circolazione e il reperimento di diversi punti di vista funzionali alla formazione dell'opinione pubblica.
Sotto tale punto di vista i motori di ricerca sono gli attori, sul web, della effettività del diritto ad es-

[24] Ci sia consentito il riferimento anche a R. Borrello, *Pay tv e circolazione di prodotti del pensiero a vocazione comunicativa*, in P. Barile - R. Zaccaria (a cura di), *Rapporto '93 sui problemi giuridici della radiotelevisione in Italia*, Torino, 1994 e Id., *Il prodotto radiotelevisivo*, cap. X, parte I del *Trattato di diritto amministrativo* (a cura di santaniello), vol. XV, t. 2, Padova, 1996, 499.
[25] Trattandosi di programmi creati da altri soggetti: si tratta di Cons. St., sez. III, sent. 5 febbraio 2015, n. 582, sulla quale v. R.Petti, *L'informativa economica di sistema: quale perimetro? L'assenza di responsabilità editoriale, non esime dalla comunicazione all'Agcom*, in *Quaderni di Diritto Mercato Tecnologia*, n. 2, 2015-Rivista On line.

sere informati, consentendo agli utenti di raggiungere in modo sistematico e rapido informazioni disperse in uno spazio virtuale tendenzialmente infinito ed inesplorabile con le capacità del singolo. di una serie di accertamenti empirici eseguiti dall'Agcom sui temi in esame, che rivelano profili di estremo interesse nell'ottica qui considerata.

Nel 2010, ricorda l'Agcom nell'indagine conoscitiva sopra menzionata, risultava da una ricerca realizzata da Gfk Eurisko, che il 20,6% di coloro che dichiarano di interessarsi alle tematiche di attualità (economia, politica internazionale, nazionale o locale) si informa *online*. Tale dato evidenzia che, nonostante l'*audience* del mezzo sia ancora inferiore rispetto a quella dei media tradizionali, il numero di individui che fruisce di Internet allo scopo di reperire notizie è più elevato del numero di persone che utilizzano la *pay tv*, la radio o le testate periodiche per la medesima finalità. Negli Stati Uniti, la quota di coloro che si informano attraverso il web sugli argomenti di carattere nazionale e internazionale raggiunge il 42%, un valore addirittura superiore a quello che si registra per i quotidiani e la radio[26].

Rispetto a tale quadro generale, emergono poi ulteriori elementi. Uno dei primi servizi ad affermarsi quando Internet è diventata una rete aperta ai servizi web di produttori privati è stato senz'altro il *search*. Il *search* nasce, infatti, dall'esigenza degli utenti di trovare pagine e servizi desiderati, in un contesto in cui la mera elencazione di alcuni siti raggruppati per categorie non era più sufficiente, considerata la crescente mole di informazioni presenti sulla rete. L'intento dell'utente nell'uso del servizio può essere molteplice: informativo (ricerca di informazioni), di navigazione (ricerca dell'url di una pagina), transazionale (ricerca di un servizio per effettuare una determinata transazione).

I *search* risultano, quindi, fondamentali per i cittadini, sia per acquisire informazioni e formarsi opinioni, sia per orientare le proprie scelte, da quelle di consumo fino a quelle di voto. In tale funzione (condivisa con gli altri c.d servizi orizzontali quali i social e gli aggregatori) si realizza un rapporto virtuoso con i creatori originari dei contenuti informativi (editori *online* nativi o derivati) rispetto ai quali essi fanno da veicoli di diffusione.

Più in generale, quindi, i motori di ricerca e gli *store*, nel caso di navigazione da *device* mobile, si configurano come piattaforme di aggregazione e di accesso ai contenuti informativi. Il dato importante è che gli utenti tendono spesso a percepire questi ultimi e non le piattaforme informative originarie come i fornitori di *news online*, anche perché la ri-aggregazione dei singoli contenuti e la personalizzazione dell'offerta al pubblico avviene spesso proprio a livello di porta di ingresso alla rete (e, quindi, di motori di ricerca, portali e *social network*). Il dato è poi confermato dall'analisi dei singoli siti ritenuti più rilevanti per informarsi *online* sull'attualità (nazionale e/o locale). Google è di gran lunga il sito più utilizzato dagli utenti a questi fini (21,5%). Nella indagine conoscitiva "TV 2.0", la stessa Agcom[27] ha sottolineato, sulla base di evidenze empiriche, la rilevanza del ruolo di Google nel settore dei nuovi media, ponendo in evidenza come «la presente analisi ha inequivocabilmente dimostrato come, a prescindere dalla responsabilità editoriale, le nuove forme di comunicazione su Internet, pur eventualmente non rientrando nel tradizionale concetto di editore, presentino significativi effetti sul pluralismo dell'informazione tanto che tali voci rappresentano già ora fonti di informazioni più seguite di quelle classiche» [28].

In tal senso, quindi, come si osservava più sopra, i *search engines*, aumentano le fonti da cui attingere e garantiscono la totale personalizzazione dell'esperienza informativa, amplificando il surplus informativo tipico dell'*information society*[29]. Questa capacità di raccogliere dati è rilevante nell'ottica di una verifica della effettività del pluralismo nel contesto nazionale alla stregua dei parametri costituzionali rilevanti (per altro ripresi in sede sovranazionale e internazionale), in presenza di posizioni dominanti nell'effettuazione di tali attività e anche (ma il profilo appare più problematico, sul piano delle sue implicazioni) in quanto distorsioni o alterazioni delle modalità di raccolta e fornitura dei dati potrebbero incidere sulla qualità del pluralismo stesso.

---

[26] All. A delibera 355/2010/CONS., cit., 196.

[27] All. A delibera 19/15/CONS del 5 febbraio 2015. V. anche, della stessa Agcom, sul ruolo sempre più rilevante dell'informazione on line nel settore della comunicazione politica, il documento del 23 febbraio 2016 Il consumo di informazione e la comunicazione politica in campagna elettorale, disponibile alla pagina web

[28] In tale prospettiva si colloca l'evoluzione dell'attività dei motori di ricerca, da semplici intermediari per la fornitura dei classici *ten blue links*, da cui attingere le informazioni a diretti fornitori delle informazioni stesse. Il tema è studiato sul piano del principio della c.d. *search neutrality* e del diritto antitrust, in ordine alla possibilità per il motore di ricerca di privilegiare fonti informative a sé riconducibili nella indicizzazione o nella costruzione del diretto processo informativo (secondo l'evoluzione segnalata), ma ha anche riflessi, come si è evidenziato nel testo, sul piano della tematica del pluralismo informativo. Si v. al riguardo D. A. Crane, *Search Neutrality as an Antitrust Principle*, George Mason Law Review, n 5. 2012, 1199 ss., nonché, sulla riconducibilità dell'attività di indicizzazione da parte di Google al Primo Emendamento, la decisione della *Superior Court of the State of California, County of San Francisco* del 13 novembre 2014 nel caso St. Louis Martin vs. Google Inc., che si rifà (sia pure in modo implicito, visto che il riferimento a tale decisione era l'argomentazione principale della difesa di Google) alla fondamentale decisione della Corte Suprema della California *Blatty vs. New York Times Co.* ((1986) 42 Cal.3d 1033, 232 Cal.Rptr. 542; 728 P.2d 1177), che ha ricondotto la più tradizionale redazione di una lista di best sellers da parte di un giornale cartaceo al Primo Emendamento.

[29] V. ancora il contributo citato alla nota 19 di L. Bolognini - G. Ragusa.

3.2 La rilevanza dei motori di ricerca sulla distribuzione delle risorse del mercato dei media e le conseguenze sul pluralismo informativo

In ordine al secondo profilo occorre tenere conto che, se l'affermazione dell'informazione *online* sta determinando ricadute positive sul benessere sociale, in quanto genera un surplus informativo spesso a costo quasi nullo per i cittadini; dall'altro lato, non possono non trascurarsi le ricadute che tale situazione determina sulla distribuzione delle risorse del mercato di Internet sugli operatori, con conseguenze rilevanti sul profilo del pluralismo dell'informazione.
La raccolta pubblicitaria *online*, costituisce la principale fonte di finanziamento delle attività informative svolte sul web, che sono generalmente offerte agli utenti in forma gratuita.
In particolare ciò accade «per gli editori di siti web, i cui contenuti sono oggetto di riaggregazione dai motori di ricerca e gli altri veicolatori di informazione (portali e social). Sono gli editori in senso proprio quelli dai quali dipende la qualità dei contenuti veicolati *online*. La pubblicità che essi diffondono è atta ad influire sul design della piattaforma (ossia, su come il contenuto viene presentato agli utenti e restrizioni concorrenziali dal lato pubblicitario possono avere conseguenze negative appunto in una prospettiva di tutela del pluralismo informativo»[30]. In questo senso, il mercato della pubblicità *online* assume una rilevanza strategica non solo per gli assetti concorrenziali del web, ma anche per la tutela del pluralismo.
Eventuali strozzature concorrenziali nella raccolta pubblicitaria *online* determinerebbero effetti negativi sia sulla natura stessa, aperta e competitiva, di Internet sia sulle informazioni e notizie a disposizione di cittadini e utenti.
In particolar modo, l'incremento dei ricavi pubblicitari da parte dei motori di ricerca per le inserzioni che vengono fatte direttamente su di essi (distinguendosi da quelle che vengono effettuate sui siti degli editori in senso originario), che, come si rilevava più sopra, si presentano agli occhi degli utenti, come una diretta fonte di informazione, determinerebbe effetti negativi sulle piattaforme tradizionali a cui è imputabile l'informazione per così dire "nativa". Tali piattaforme sono costrette, a causa della drastica riduzione dei propri ricavi, a tagliare i costi di parte della propria attività giornalistica. L'effetto di questo processo potrebbe essere un incremento della diffusione delle notizie ma a spese di un depauperamento della fase di generazione della notizia stessa. È per questo che a livello internazionale (sia comunitario che statunitense) sono state avviate una serie di iniziative (pubbliche e private) volte a finanziare l'attività giornalistica *online*, ed in particolare quella d'inchiesta.

4 Considerazioni finali

In conclusione, pur non potendosi negare che quanto esaminato sopra e nel paragrafo precedente abbia carattere controverso, il dato che emerge è che non appare priva di fondamento la necessità di una particolare attenzione su taluni degli operatori del web che, al di là del loro oggettivo peso economico (e delle collegate problematiche in termini anche tributari, ben noti) svolgono attività aventi riflessi importanti sulle dinamiche essenziali del funzionamento del circuito democratico.
La risposta fornita dall'ordinamento italiano è stata quella, come si è visto, dell'inserimento dei ricavi delle concessionarie di pubblicità *online*, nel calcolo del "calderone" del monte ricavi del SIC e della previsione dell'obbligo per tali soggetti di iscriversi nel registro degli operatori della comunicazione- ROC. Il comma 9 dell'art. 43 del TUSMAR stabilisce che «[f]ermo restando il divieto di costituzione di posizioni dominanti nei singoli mercati che compongono il sistema integrato delle comunicazioni, i soggetti tenuti all'iscrizione nel registro degli operatori di comunicazione (...) non possono ne' direttamente, ne' attraverso soggetti controllati o collegati ai sensi dei commi 14 e 15, conseguire ricavi superiori al 20 per cento dei ricavi complessivi del sistema integrato delle comunicazioni.»
Si può rilevare, al riguardo, che, allo stato, non esiste un mercato rilevante a cui possa commisurarsi una posizione dominante delle concessionarie ed inoltre sono quest'ultime e non i motori di ricerca a doversi iscrivere al ROC, in ordine alla operatività del limite generale del 20% rispetto al SIC
Se tale assetto appaia sufficiente nell'ottica della tutela del pluralismo, non è chiaro, anche alla stregua del quadro sopra ricostruito, che evidenzia come il fenomeno appaia ancora più comples-

[30] V. Allegato A alla Delibera Agcom n. 19/14/CONS (Indagine conoscitiva sul settore dei servizi Internet e sulla pubblicità *online)*, cap. 4 n. 586.

so ed articolato rispetto non solo alla percezione comune, ma anche a quella istituzionale.
Oltre a quanto si rilevava più sopra[31], appare interessante segnalare quanto è emerso nelle valutazioni dell'Agcom nell'ambito dell'adozione della più sopra citata delibera 41/17/CONS, nella quale si afferma che se è pur vero che «alla luce del quadro normativo vigente» i servizi operanti *online*, indicati nel citato art. 2 del TUSMAR, non possono venire in rilievo «ai fini delle valutazioni sulla perimetrazione dei mercati nell'ambito del settore dei servizi di media audiovisivi», è altrettanto vero che «l'emersione del modello di business dei c.d. OTT (*Over the Top*: ad es. portali di *e-commerce*, motori di ricerca, *social network*), che attraverso Internet operano su scala globale e che sono sempre più attivi nell'aggregazione e nella distribuzione di vari contenuti, anche audiovisivi, apre possibili nuovi scenari». Secondo l'Agcom, in particolare, le «dinamiche generate dai nuovi servizi audiovisivi diffusi *online* (afferenti ad un ambito di mercato distinto), in particolare offerti dagli operatori OTT, e i relativi impatti sul livello di concorrenza all'interno del sistema integrato delle comunicazioni, saranno oggetto di valutazione nell'ambito della Fase 2 della presente istruttoria, alla luce dei criteri indicati dallo stesso articolo 43, comma 2 del Testo Unico»[32].
Ecco che, quindi, l'attività dei motori di ricerca potrebbe acquistare rilievo direttamente (in forme e modi ancora da definire) quale ulteriore ed autonoma "voce" stessa del pluralismo, da prendere in considerazione più che altro nella declinazione "esterna" di quest'ultimo, nell'ottica della posizione dominante, apparendo molto più problematica (ed il punto merita una autonoma riflessione) una valutazione in termini di pluralismo "interno". Tale diretta considerazione potrebbe avvenire, con l'inserzione in un mercato rilevante preesistente o in uno nuovo, nel settore dei servizi di media audiovisivi (sulla base degli spunti, sopra indicati, elaborati dall'Agcom), o attraverso l'inquadramento in una accezione più ampia di editoria elettronica o, meglio ancora, potrebbe ipotizzarsi, *de iure condendo*, la costruzione di una nozione *ad hoc*, commisurata al rilevato, atipico ma influente, concorso al processo informativo (da considerare, ovviamente, in relazione a tutti i parametri costituzionali ed eurounitari rilevanti).

[31] *Supra*, par. 3.1.
[32] V. p. 9 e 10 della cit. delibera.

Fake news e *social network*: la verità ai tempi di Facebook

Fake news and social networks: truth in the time of Facebook

Matteo Monti
Dottorando di ricerca in Persona e tutele giuridiche, Scuola Superiore Sant'Anna

Abstract

L'articolo intende studiare la problematica della diffusione delle *fake news* sui *social networks* e le soluzioni di contrasto sviluppate sia dal legislatore nazionale e da quello sovranazionale (UE) sia dalle stesse compagnie proprietarie dei social. Lo studio non potrà che risolversi in una lettura problematizzante della situazione attuale, provando però a suggerire alcune possibili soluzioni tecnico-giuridiche al problema. Nel secondo paragrafo sarà necessario in via preliminare accennare brevemente alla relazione fra libertà di informazione e verità/veridicità delle notizie trasmesse. Si affronterà dunque la tematica del rapporto fra libertà di informazione e il «subiettivamente falso», per usare le parole di Alessandro Pace, rilevando come nel nostro sistema costituzionale la diffusione dolosa di false notizie non trovi protezione. Nel terzo paragrafo si evidenzieranno le particolari problematiche del fenomeno della diffusione delle *fake news* sui *social networks*. Si analizzerà quindi l'importanza assunta dai *social networks* come strumento di divulgazione d'informazioni, il problema della diffusione virale dei contenuti falsi e la debolezza del fenomeno sociale del *debunking*. Nel paragrafo quarto si rileverà il problema dell'inefficacia degli strumenti extra-penali attualmente presenti in Italia, in particolare dell'istituto della rettifica, e si affronterà la questione dell'assenza di una disciplina di regolamentazione dei *social networks*. Nel sotto paragrafo 4.2 si darà conto delle tecniche di "censura privata" che Facebook sta applicando e dei loro possibili problemi. Nelle conclusioni si tenterà di arrivare a una sintesi delle questioni analizzate, cercando di prospettare possibili soluzioni alla diffusione di *fake news* sui *social networks*.

The paper explores the problem of the spread of fake news on the social networks and the forms of censorship developed by the national government, the EU system and Facebook. In a very complex matter, such as the diffusion of fake news on the Internet, the Article will propose some solutions designed for the Italian legal system. In Part II, the paper briefly explores the concept of freedom of information in Italy. I claim that the Italian paradigm of freedom of information, as it derives from the Constitution and the decisions of Italian Constitutional Court, does not protect the diffusion of fake news in bad faith. In the Part III, the paper shall highlight the radical changes in the media landscape and how Facebook is getting far more prominence in the diffusion of news. I shall argue that the marketplace of ideas alone is not able to win the battle against fake news. Finally in Part IV, the Article analyzes the fail of current regulations rectifying fake news and the new solutions proposed by the Italian Parliament. In addition I shall argue also that the "Facebook's Fact-Checking Partnership" is a tool with some huge problems, concerning both effectiveness and legality. In the final section, I shall suggest some possible solutions in order to contrast fake news on social networks without risks of chilling effect on freedom of information.

Sommario

fake news
libertà di informazione
social networks
Facebook
rettifica

1 Introduzione

Il mondo dei *social networks* ha radicalmente cambiato il paradigma del discorso pubblico nelle democrazie occidentali da un duplice punto di vista. Da un lato ha favorito la diffusione del pensiero alternativo e della c.d. controinformazione, permettendo anche lo sviluppo di innovative e dinamiche forme di democrazia "partecipativa"[1], dall'altro ha incrementato la diffusione di false informazioni con grave nocumento per l'economia e la democrazia[2]. La rete è nel bene e nel male «una società c.d. a "potere diffuso" [..] nella gestione della divulgazione di contenuti *online*»[3] e questo comporta il rischio che – più che ogni altro mezzo di comunicazione causa l'assenza dei controlli tipici dei media tradizionali – la stessa rete sia in grado di inquinare il *public discourse* veicolando informazioni false, le c.d. *fake news* o bufale.

Questo risvolto negativo della rete e in particolare dei *social networks* ha contribuito ad un inquinamento del *public discourse,* talvolta sfociato persino in una distorsione dei meccanismi di partecipazione democratica[4]. Il fenomeno delle false notizie non è un fenomeno nuovo[5], ma oggi assume una rilevanza notevole a causa dello sviluppo dei *social networks*, uno strumento che permette una maggior diffusione delle stesse.

In questa sede s'intende studiare la problematica della diffusione delle *fake news* sui *social networks* (concentrandosi su quello più diffuso: Facebook) e le soluzioni di contrasto formulate sia dal legislatore nazionale e sovranazionale (UE) sia dalle stesse compagnie proprietarie dei social. Lo studio non potrà che risolversi in una lettura problematica della situazione attuale, provando però a suggerire alcune possibili soluzioni tecnico-giuridiche al problema.

Sarà necessario in via preliminare accennare brevemente alla relazione fra libertà di informazione e verità/veridicità delle notizie trasmesse. Nel secondo paragrafo si affronterà dunque la tematica del rapporto fra libertà di informazione, come *species* del più ampio *genus* della libertà di espressione, e il «subiettivamente falso»[6] (la creazione di notizie false) nell'ordinamento italiano. Si constaterà che la libertà di informazione non garantisce protezione al subiettivamente falso nell'ambito specifico del diritto di cronaca. Successivamente sarà necessario evidenziare le particolari problematiche del fenomeno della diffusione delle *fake news* sui *social networks*: il perno del problema della diffusione delle bufale è infatti legato alla capacità dei *social networks* di farsi "cassa di risonanza" di qualsiasi notizia (anche falsa). Nel paragrafo terzo si analizzerà quindi l'importanza assunta dai *social networks* come strumento di divulgazione di informazioni, il problema della diffusione virale dei contenuti falsi e la debolezza del fenomeno sociale del *debunking* (la decostruzione della notizia falsa in una sorta di rettifica "privata" della verità da parte di soggetti terzi). Poste queste premesse si studieranno infine gli attuali strumenti giuridici ed extra-giuridici a tutela della verità/veridicità delle notizie. Nel paragrafo quarto si rileverà il problema dell'inefficacia degli strumenti extra-penali attualmente presenti in Italia, in particolare dell'istituto della rettifica, e si affronterà la questione dell'assenza di una disciplina di regolamentazione dei *social networks* in relazione anche al c.d. ddl anti-bufale in discussione in Parlamento. In seguito si darà conto delle tecniche di "censura privata" che Facebook sta applicando e delle loro possibili problematiche.

Nelle conclusioni si tenterà di arrivare ad una sintesi delle questioni analizzate, cercando di prospettare possibili soluzioni alla diffusione di *fake news* sui *social networks*. Si suggerirà la necessità dell'*extrema ratio* del diritto penale solo in casi determinati, preferendo ad esso in generale soluzioni di *debunking*. Tali soluzioni necessitano tuttavia di forme di collaborazione fra *social networks* e stato (o UE) affinché quest'ultimo non abdichi alla tutela/controllo della libertà d'informazione delegandolo di fatto completamente a società private.

---

1 F. Colombo, *Web 2.0 e democrazia: un rapporto problematico*, in P. Aroldi (a cura di), *La piazza, la rete e il voto*, Roma, 2014, 32 ss.

2 W. Lee Howell, *Digital wildfires in a hyperconnected world*, in *Report Global Risks*, 2013, 23.

3 E. Faletti, *Internet la diffusione della cultura non accademica e la formazione dell'opinione pubblica*, in *Ciberspazio e diritto*, 10/2009, 325 ss.

4 Si pensi all'influenza giocata dalle *fake news* nella campagna elettorale americana, ma anche per quanto concerne la recente campagna referendaria italiana il dato è inquietante: la notizia più diffusa sui *social networks* è stata la bufala relativa alla presenza di 500.000 schede già contrassegnate con il "Sì". Cfr. M. Rovelli, *Referendum, la notizia più condivisa sui social è una bufala*, in www.corriere.it, 2 dicembre 2016.

5 Non che questo fosse estraneo al mondo del passato, segnatamente connotato da un "mal costume giornalistico" di drogare l'opinione pubblica con notizie false. Cfr. G. Verrina, *L'art. 656 c.p. e la libertà di pensiero*, in *Giurisprudenza di merito*, 1977, 340 ss. Nella sentenza commentata dall'Autrice, per esempio, si parlava della diffusione di notizie false relative ad un nuovo "piano Solo" di golpe militare in Italia. Come riportato quello della diffusione di false notizie era problema già discusso dalle associazioni di giornalisti negli anni '30. Come si vedrà il fenomeno è stato affrontato anche nei lavori della Costituente. Anche nella prospettiva giornalistica questa problematica è ben presente: Cfr. F. Colombo, *Oscurando la verità*, in *Problemi dell'informazione*, 2001, 181 ss.

6 A. Pace - M. Manetti *Art. 21. La libertà di manifestazione del pensiero*, in G. Branca - A. Pizzorusso (a cura di), *Commentario alla Costituzione. Rapporti civili*, Bologna-Roma, 2006, 89.

2 La libertà di informazione nella Costituzione Italiana e la (non) protezione del falso

La Costituzione Italiana non prevede espressamente la sussistenza di una specifica libertà di informazione, ma la stessa è ricavabile dalle decisioni della Corte costituzionale che la riconducono al parametro generale dell'art. 21 Cost[7]. La diffusione di *fake news* comporta la necessità di confrontarsi con il tema della verità/veridicità dei fatti nell'ambito del diritto all'informazione. Più nello specifico la prospettiva va traslata dalla necessità di tutelare il vero/verosimile a quella di tutelare il «subiettivamente falso», per usare le parole di Alessandro Pace. La questione è se la creazione e diffusione del falso nell'ambito dell'informazione possa essere inquadrata come libertà d'informazione e quindi da ultimo come libertà di espressione.

Per quanto riguarda lo specifico tema della veridicità delle notizie, esso aveva avuto un peso notevole all'interno dei dibattiti dell'Assemblea costituente. L'art. 16 (attuale art. 21 Cost.) comma 5 prevedeva, come uscito dalla Prima Sottocommissione, che «Per le funzioni speciali della stampa periodica la legge dispone controlli sulle fonti di notizie e sui mezzi di finanziamento idonei a garantire la fede pubblica»[8]. Le esigenze del comma riportato erano, per l'appunto, quelle della tutela contro le *fake news*: «Queste norme, (..) che debbono servire come un invito e come una traccia per il legislatore, sono di grande importanza, perché si riferiscono principalmente all'obbligo dell'indicazione dei bilanci e delle fonti delle notizie. Si sa quali sconvolgimenti possano produrre le notizie false od inventate»[9]. Successivamente il testo dell'art. 16 co. 5 del primo dicembre, come approvato dalla Commissione, mantiene il riferimento al controllo delle fonti («La legge può stabilire controlli per l'accertamento delle fonti di notizie e dei mezzi di finanziamento della stampa periodica»), ma perde tuttavia il riferimento alla "fede pubblica", anche in ragione di una generale semplificazione e riduzione dell'articolo.

La paura della (ri)costituzione di un "ministero della verità" orwelliano aveva da ultimo portato i costituenti, nei lavori dell'Assemblea del 14 aprile 1947, alla cancellazione del comma 5 dell'art. 16 nella parte relativa al "controllo delle fonti"[10]. Serve tuttavia rilevare che la soppressione del "controllo delle fonti" fu dettata dal timore di svolte autoritarie e non da considerazioni tese a inquadrare anche le notizie dolosamente inventate come protette dall'art. 21. Il timore espresso dall'On. Celotto e da altri, distanziandosi dalle considerazioni originarie per il quale era stato pensato il comma (la censura del falso), sposta l'ambito della questione dalla censura del falso alla necessità di non fornire ai futuri governi strumenti costituzionali per la limitazione della libertà di stampa. Sembra dunque doversi continuare a considerare principio orientativo e parametro interpretativo generale in materia di falso nell'ambito del diritto all'informazione quanto ritenuto in sede di Sottocommissione, non essendo alcun intervento successivo postosi a difesa della libertà giornalistica a diffondere notizie false, anzi essendosi espressi alcuni interventi in maniera molto dura, come quello dell'On. Cavallari[11].

La dottrina costituzionalistica italiana, a prescindere dalla sua volontà di abbracciare una tesi funzionale della libertà di espressione o una individualistica, sembra unanime nel ritenere il subiettivamente falso non protetto dall'art. 21 Cost.[12]. Il dilemma sarebbe dunque solo quello dell'opportunità della repressione, secondo la teoria individualistica, o della necessità della repressione, secondo quella funzionalista[13].

Per quanto riguarda la giurisprudenza costituzionale, la Corte sembra in un *obiter dictum* sancire

---

[7] *Ex pluribus* C. Cost., sent. 112/93. La tematica non fu comunque estranea al dibattitto in Assemblea Costituente in particolare in riferimento all' «interesse dei destinatari a ricevere le notizie, specie quando tale interesse venne bilanciato con l'interesse di chi quelle notizie avrebbe inteso diffondere». P. Costanzo, *Informazione nel diritto Costituzionale*, in *Digesto delle discipline pubblicistiche*. VIII, Torino, 1993, 319 ss.

[8] Seduta della Prima Sottocommissione del 27 settembre 1946, in *La Costituzione della Repubblica nei lavori preparatori della Assemblea Costituente*, Edizione a cura della Camera dei Deputati, Roma, 1976, 158.

[9] Così il Relatore On. Basso, *ibidem*, 151.

[10] Guida la carica "paranoica" l'On. Cevelotto, seguito dall'On. Badini Confalonieri e dall'On. Giannini. Lavori in Assemblea, seduta pomeridiana del 14 aprile 1947, in *La Costituzione della Repubblica nei lavori preparatori della Assemblea Costituente*, edizione a cura della Camera dei Deputati, Roma, 1976, 2855 ss.

[11] "Ma noi domandiamo ai colleghi democristiani se non ritengano che anche la propalazione di certe notizie non pornografiche non rappresenti un pericolo altrettanto grave. Mi riferisco alle notizie che appaiono in alcuni giornali a cui ho accennato poco fa, le quali vorrebbero far credere al Paese che, per esempio, il Governo sta per cadere da un momento all'altro, che la moneta italiana è svalutata al massimo grado, o che il maresciallo Tito sta marciando verso Trieste da più di un anno e mezzo con un ritmo tale per cui a quest'ora sarebbe giunto già in America. Se tutte queste notizie fossero prese sul serio, esse creerebbero un tale stato di disorientamento dell'opinione pubblica da far correre al nostro Paese dei gravi pericoli». *Ivi*, 2808.

[12] Cfr. P. Barile, *Il soggetto privato nella Costituzione Italiana*, Padova, 1953, 121; C. Esposito, *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Milano, 1958, 37; A. Pace, *op. cit.,* 89; S. Fois, *Principi costituzionali e libera manifestazione del pensiero*, Milano, 1957, 210-211.

[13] Cfr. A. Pace, *op. cit.*, 89.

la necessità di veridicità delle notizie nell'ambito della stampa[14] e sicuramente ritiene legittima la sanzione (penale) della diffusione di false notizie, anche se solo nel caso di turbamento dell'ordine pubblico[15].
Appare dunque doversi affermare una "non protezione" della creazione di notizie false. Ove con notizie si intendano esclusivamente divulgazione di fatti di cronaca. In altri ambiti il falso, anche subiettivo, potrebbe trovare protezione[16]: si pensi al falso nell'ambito del diritto di satira (del quale spesso è presupposto), nell'ambito del diritto di critica e nell'ambito dell'espressione politica (nei quali può essere usato come espediente dialettico), nell'ambito della libertà religiosa (soprattutto in relazione alle nuove religioni come ad esempio quella raeliana) e infine nell'ambito delle teorie politiche "complottiste", ossia quelle complesse costruzioni ideologiche che imputano "politicamente" determinati avvenimenti a determinate categorie o gruppi (da quelle sul Gruppo Bilderberg a quelle sulle lobby dei vaccini).
Tale protezione non è prevista nell'ambito dell'informazione. È, dunque, costituzionalmente legittimo addivenire a forme di repressione delle false notizie diffuse con dolo.

3 L'importanza dei *social networks* nel mondo dell'informazione e il problema delle bufale

La rete internet ha radicalmente cambiato il mondo della comunicazione ed è uno strumento ormai diffuso, come rilevato dal XII° Rapporto Censis-Ucsi[17]: il 70,9% della popolazione italiana utilizza la rete, la percentuale di internauti cresce fino al 91,9%, fra i giovani (mentre si ferma al 27,8% tra gli anziani). Per quanto riguarda i *social networks* il 50,3% dell'intera popolazione e il 77,4% dei giovani *under* 30 sono iscritti al più famoso e diffuso *social network*: Facebook. Nell'ambito dell'informazione, stante ancora il primato dei mezzi d'informazione tradizionali (il 76,5% utilizza i telegiornali; il 52% i radio-giornali), il 51,4% degli italiani utilizza anche motori di ricerca per informarsi e il 43,7% si affida anche a Facebook. La percentuale s'inverte in relazione ai giovani fra cui Facebook è il principale strumento per informarsi (71,1%), seguito dai motori di ricerca (68,7%) e dai telegiornali (68,5%). Il ruolo dei *social networks* nel mondo dell'informazione è quindi destinato a crescere con il ricambio generazionale. Stiamo assistendo alla costruzione di una «*nuova gerarchia delle fonti di informazione*», secondo le parole del XII° Rapporto Censis-Ucsi.
Inoltre come è evidenziato dal Rapporto Eurobarometro 82.3[18], che analizza l'andamento dell'opinione pubblica di 34 paesi, il 58,2% degli italiani considera il web una fonte credibile di informazione contro una media europea pari al 49,1%. Il dato è ancora più impressionante se si considera che solo il 53,5% degli italiani ritiene la carta stampata un mezzo d'informazione affidabile e che un 17,6% si fida della rete e non della stampa periodica.
Questi dati evidenziano la vastità problematica della circolazione delle *fake news* sui *social networks*, aggravata dalla mancanza di una regolamentazione di quella particolare "cassa di risonanza" per le notizie che è Facebook. Infatti, se è vero che Facebook non produce direttamente notizie e informazione, esso è ormai uno dei principali strumenti di diffusione di notizie.
Il problema principale delle *fake news* è legato poi proprio a questo fenomeno di cassa di risonanza dei *social networks*: i siti di bufale non avrebbero probabilmente una così grande portata senza la diffusione sui *social networks*. Inoltre la problematica della diffusione di notizie false sui motori di ricerca è, in teoria, più controllabile rispetto a quella sui *social networks*, essendo legata maggiormente al controllo degli algoritmi da parte dei motori di ricerca stessi[19].
La diffusione di *fake news* sui *social networks* è correlata ad una serie di fenomeni "tecnici" e cognitivi/sociologici. I primi sono legati da una parte alla capacità dei *social networks* di raggiungere in maniera unilaterale determinati utenti (si tratta del fenomeno della capillarizzazione dell'informazione[20]) e dall'altra al problema della c.d. viralità. In particolare la capacità di un contenuto di

[14] Dopo aver ripreso le dichiarazioni del Congresso internazionale dei giornalisti di Bordeaux (maggio 1954), la Corte evidenzia che «il diritto di attingere notizie, pubblicarle e sottoporle al vaglio della critica deve essere conforme alla verità sostanziale dei fatti». C. Cost., sent. 16/1981.
[15] C. Cost. sent. 19/1962, sent. 199/1972 e sent. 210/1976.
[16] Si permetta un rimando per ulteriori specificazioni relative alla necessità di distinguere il falso nell'ambito del diritto all'informazione da altre tipologie di espressioni a: M. Monti, *Le "bufale" online e l'inquinamento del public discourse*, in P. Passaglia - D. Poletti (a cura di), *Nodi virtuali, legami informali: Internet alla ricerca di regole*, Pisa, 2017, 182 ss.
[17] XII° Rapporto Censis-Ucsi, 2015.
[18] SI342 - Eurobarometer 82.3: condizioni di vita e fiducia nelle istituzioni, impatto della crisi economica, cittadinanza europea, Europa 2020 (2014).
[19] Cfr. Redazione, *Google, nuovo algoritmo contro le fake news*, in www.ansa.it, 26 aprile 2017.
[20] «I media tradizionali […] possono certo ancora filtrare le notizie per il grande pubblico, ma la circolazione alternativa dei *social network* li minaccia perché raggiunge in modo selettivo esattamente quei cittadini che sfuggono all'informazione mainstream per curiosità intellettuale o sospetto programmatico». F. Colombo, *op. cit.*, p. 33.

diventare virale[21] attraverso condivisioni che si incrementano in modo esponenziale, a causa degli innumerevoli utenti che ogni singola condivisione raggiunge, è in grado di rendere un contenuto di conoscenza globale in poche ore. Le problematiche sociologico-cognitive corrispondono invece ad alcuni fenomeni quali la c.d. *social cascade* (la diffusione a cascata delle informazioni, che ne incrementa la diffusione senza appurarne la veridicità)[22], la c.d. *group polarization* (la polarizzazione dei gruppi, che tende a favorire la diffusione e il rafforzamento di convinzioni all'interno di gruppi omogenei)[23] e l'influenza delle *prior convictions* (le convinzioni personali) sulla lettura della notizia[24]. A questi caratteri sembra doversi aggiungere una generale *collective credulity*[25] in relazione ai contenuti on-line.

La diffusione delle *fake news* non ha trovato una risposta efficace da parte del *marketplace of ideas*. I tentativi di *debunking* sembrano destinati a scontrarsi con una produzione numericamente insostenibile di bufale, complice anche sicuramente la sopra citata *collective credulity* che contribuisce alla diffusione anche delle più inverosimili "panzane", smentibili da semplici ricerche sulla rete. In attesa della formazione di una "coscienza critica" sociale rispetto ai contenuti diffusi *online* sembrerebbe indispensabile lo sviluppo di forme di regolamentazione dei *social networks* che siano in grado di prevenire i gravi rischi di inquinamento del *public discourse* legati alla diffusione di *fake news* sugli stessi.

4 Soluzioni giuridiche ed extra-giuridiche alla diffusione delle bufale sui *social networks*

4.1 Inefficacia delle soluzioni giuridiche ed embrioni di regolamentazione

Il problema della diffusione delle false notizie sui *social networks* è principalmente dovuto alla mancata regolamentazione di questo particolare *new media*. Se è vero che Facebook non può essere considerato un vero e proprio mezzo d'informazione, alla stregua dei giornali e delle televisioni, è anche vero che esso è il principale strumento di un nuovo attivismo giornalistico individuale. La condivisione della cronaca è difatti sempre meno materia esclusiva dei media tradizionali, essendo ormai a disposizione del *quivis de populo* e dei media non convenzionali[26]. La controinformazione – fenomeno indubbiamente positivo – circola principalmente sui *social networks*, attraverso condivisioni di notizie da siti web da parte dei singoli utenti. Da tutto ciò sembrerebbe auspicabile una regolamentazione pubblica di quello che a tutti gli effetti è la cassa di risonanza dei mass media della rete. Infatti Facebook, in particolare, non produce direttamente notizie, ma contribuisce alla loro divulgazione e in quanto tale dovrebbe rispondere a qualche forma di regolamentazione pubblica e responsabilizzazione in relazione soprattutto alla diffusione di *fake news*. L'unica istituzione che sembra preoccuparsi specificatamente di questo tipo di problematica è, ad oggi, l'Unione europea che ha invitato i *social networks* ad intraprendere uno sforzo di contrasto alle *fake news*[27], sotto la minaccia di avviare un'opera di regolamentazione (probabilmente sul modello del *Code of Conduct on countering illegal hate speech online*[28] del 31 maggio 2016). La necessità di regolamentare i *social networks* è stata riaffermata anche a livello di Consiglio d'Europa il 25 gennaio 2017 con la risoluzione n. 2143 dell'Assemblea "*Online media and journalism: challenges and*

[21] Cfr. W. Lee Howell, *op. cit.* e F. Vis, *The rapid spread of misinformation online*, in *Outlook on the Global Agenda 2014*, 2014, 28a. Cfr. sulla diffusione a "senso unico" dei *false rumors* su Facebook: Aa.Vv., *Viral Misinformation: The Role of Homophily and Polarization*, in *Proceedings of the 24th International Conference on World Wide Web*, New York, 2015, 335. Cfr. C. Sunstein, *On Rumors: How Falsehoods Spread, Why We Believe Them and What can be Done*, Princeton, 2014, spec. 97-102.

[22] Si rimanda a C.Sunstein, *op. cit.*, 36-45. In particolare sul fenomeno come correlato ai *social networks, ibidem*, spec. 40 e 48.

[23] *Ivi*, 50 ss.

[24] *Ivi*, 75 ss.

[25] Cfr. D. Mocanu – L. Rossi – Q. Zhang – M. Karsai – W. Quattrociocchi, *Collective attention in the age of (mis)information*, in Av.Vv., *Computers in Human Behavior*, 2015, 1198 ss.

[26] Per alcuni l'impatto della rete è stato così epocale da comportare una trasformazione dello stesso concetto di giornalismo, riportando indietro le lancette dell'orologio a quando il giornalismo e l'informazione non erano altro che una branca dell'attivismo politico. M.C. Dorf - S. Tarrow, *Stings and Scams: fake news, the First Amendment, and the New Activist Journalism*, in *Cornell Legal Studies Research Paper*, 17/2017.

[27] D. Bond - D. Robinson, *European Commission fires warning at Facebook over fake news*, in www.financialtimes.com, 30 gennaio 2017. Serve anche dar conto della Risoluzione del Parlamento Europeo del 23 novembre 2016 sulla comunicazione strategica dell'UE per contrastare la propaganda nei suoi confronti da parte di terzi (2016/2030(INI)) con la quale il PE aveva già espresso preoccupazioni per la diffusione di *fake news* sui social media della rete.

[28] Si tratta di un codice di condotta pensato per gli *hate speech* razzisti e terroristici che impegna i *social networks* a rimuovere con tempi rapidi i contenuti odiosi in rete. Il codice nelle prime sperimentazioni è sembrato funzionare in parte: V. Jourová, *Code of Conduct on countering illegal hate speech online: First results on implementation*, dicembre 2016.

accountability"[29] , con la quale si auspica che i 47 stati membri si impegnino alla regolamentazione della rete e dei *social networks*[30], implementando soluzioni simili al codice di condotta dell'UE[31].
Il problema dell'assenza di un'attenzione specifica ai *social networks* porta ad una scarsa efficacia degli strumenti penali attualmente vigenti per la repressione del falso[32], ma anche (e soprattutto) a un totale fallimento degli strumenti di rettifica.
In generale si ritiene, per quanto riguarda la condivisione in buona fede di *fake news* sui *social networks* da parte del *quivis de populo*, che la correzione del falso dovrebbe essere svolta con strumenti estranei all'*extrema ratio* del diritto penale (salvo la nascita di nuovi fenomeni, come pagine Facebook che diffondano in prima persona notizie false) per evitare eccessive opere di *silencing*.
Quante persone nel dubbio di essere soggette anche solo a una sanzione pecuniaria si arrischierebbero a condividere una notizia non proveniente dai mass media tradizionali? La soluzione migliore per "correggere" la diffusione mediante condivisione sui *social networks* delle false notizie sembra dunque essere quello della rettifica.
Gli strumenti della rettifica della verità (il plurale è d'obbligo) hanno sia un carattere di attivazione privato-personale (diritto alla rettifica) che uno pubblico (obbligo deontologico di correggere il falso per i giornalisti oppure pubblicazione della rettifica a seguito di sentenza).
L'istituto del diritto alla rettifica, ossia la rettifica di carattere privato-personale, previsto nel nostro ordinamento in materia di stampa dall'art. 8 della l. 47/1948 e in materia radiotelevisiva dall'art. 32-*quinquies* del d.lgs. 277/2005, si pone infatti come autonomo diritto della personalità[33], correlato tuttavia anche alla necessità di pluralismo informativo[34] e all'«interesse pubblico all'obiettività dell'informazione» (C. Cost. sent. 133/1974). Nell'ambito della stampa essa si pone a tutela della verità soggettiva (c.d. rettifica soggettiva), ossia senza necessario accertamento della verità oggettiva, mentre nella disciplina originaria della radio-televisione essa aveva come presupposto la verità oggettiva (art. 10, l. 223/1993) e quindi un carattere marcatamente più funzionale all'interesse pubblico ad un'informazione veritiera[35]. Nessuno di questi istituti è specificatamente applicabile alla rete internet, o meglio ai mass media della rete, mancando una legge in materia o un'interpretazione estensiva da parte della giurisprudenza. Il ddl 1119-B in studio al Parlamento[36] in tema di "Modifiche alla legge 8 febbraio 1948, n. 47" estendendo la necessità di rettifica soggettiva anche alla stampa *online* cerca di supplire a questa lacuna, ma non contempla i *social networks*.
In relazione alla rettifica attivata da organi pubblici vi sono invece due tipi di strumenti: la rettifica come dovere deontologico del giornalista e la rettifica come pena accessoria giudiziale. Entrambe hanno come fine principale quello dell'interesse pubblico all'informazione.
L'istituto della rettifica in capo ai giornalisti è previsto dall'art. 2 della l. 69/1963 secondo cui «Devono essere rettificate le notizie che risultino inesatte, e riparati gli eventuali errori»: insomma «la

[29] Risoluzione n. 2143, 25 gennaio 2017. Cfr. Committee on Culture, Science, Education and Media, Report doc. 14228, 9 gennaio 2017. Il report in particolare avvertiva come: «*Social media such as Facebook and online platforms for user-generated content such as Twitter and YouTube have emerged with market prominence as new online media […] become the primary contact point for users seeking news*».

[30] Riconoscendo comunque i tentativi dei social: «*The Assembly welcomes the fact that large online media have established a policy whereby users can identify factual errors or factually false posts by third parties on their websites, such as on Facebook News Feed or through Google's "webpage removal request tool". Credibility and reliability of online media require that they remove or correct false information*». Risoluzione n. 2143.

[31] Gli stati infatti «*should co-operate with online media and internet service providers in order to set up codes of conduct which are inspired by the code of conduct countering illegal hate speech online agreed upon by the European Commission and major internet companies on 31 May 2016*». Risoluzione n. 2143. Si riporta anche nella stessa risoluzione che la European Internet Services Providers Association invita: «*to voluntarily correct false content or publish a reply in accordance with the right of reply or remove such false content; they are legally obliged to co-operate in combating illegal content*».

[32] Si consenta un rimando in relazione alla non applicazione degli strumenti penali della diffamazione (art. 595 c.p.), della diffusione di false notizie (art. 656 c.p.) e di altri reati connessi alla diffusione di false notizie (segnatamente: il reato di truffa *ex* art. 640 c.p., il reato di abuso della credulità popolare *ex* art. 661 c.p., il reato di procurato pericolo ex art. 658 c.p.) a M. Monti, *op. cit*. Tutti questi reati tesi in vario modo alla repressione della diffusione di notizie false non risultano applicabili o applicati alla fattispecie delle *fake news* sui *social networks* a causa della loro formulazione correlata al mondo pre-digitale. Se certamente alcuni di essi, come la diffamazione, trovano applicazioni anche in relazione al mondo della rete, nessuno riesce a essere efficace nel contrasto alla diffusione di *fake news* online e, soprattutto, sui *social networks*. Qualche reato pensato e riformulato recentemente potrebbe forse essere applicato ai c.d. siti fabbrica di bufale qualora diffondano una particolare *species* di false notizie, ma non sicuramente ai *social networks*: il riferimento è alle fattispecie sanzionatore del Tuif, art. 185 e 187-ter, relative alla diffusione di false notizie che possano alterare il mercato. In particolare l'art. 187-ter prevede specificatamente anche la sanzione di condotte poste in essere attraverso la rete Internet. Cfr. C. Melzi d'Eril, *Diffusione di notizie false tramite Internet e manipolazione del mercato*, in *Il diritto dell'informazione e dell'informatica*, 2/2012, 224 ss. Sulla differenza fra 185 e 187-*ter*, il secondo configurato come reato di pericolo astratto, si veda: Cass. pen., sez. V, sent. 40393/2012. Cfr. V. Notargiacomo, *Osservazioni a Cass. pen., sez. V, n. 40393, 20 giugno 2012*, in *Cassazione penale*, 2013, 4627 ss. La fattispecie è limitata nell'oggetto (la repressione di determinate *fake news*) e nell'applicazione concreta (non risulta essere mai stata applicata ai siti di bufale) e sicuramente difficilmente potrebbe trovare applicazione in relazione ai *social networks*.

[33] G. Corasaniti, *Rettifica (diritto alla*), in *Enciclopedia giuridica Treccani,* XXVII, Roma, 1991, 1 ss.; V. Zeno Zencovich, *La disciplina del diritto di rettifica nella nuova legge radiotelevisiva,* in *Diritto dell'informazione e informatica,* 1990, 836-837. Anche la Corte Costituzionale in un *obiter* enuncia «che venga riconosciuto e garantito - come imposto dal rispetto dei fondamentali diritti dell'uomo - il diritto anche del singolo alla rettifica». C. Cost. sent.. 225/1974.

[34] In dottrina, V. Roppo, *Il diritto di rettifica nella disciplina dei mezzi di comunicazione di massa*, in *Foro italiano*, 1983, I, 463 ss. *Contra* F. Macioce, *La rettifica delle notizie lesive della personalità: disciplina attuale e prospettive future*, in *Riv. trim. dir. e proc. civ.*, 1996, 654 ss. L'Autore rinviene solo la necessità di accertamento della verità.

[35] Cfr. A. Pace - M. Manetti *Art. 21. La libertà di manifestazione del pensiero*, in G. Branca - A. Pizzorusso (a cura di), *Commentario alla Costituzione. Rapporti civili*, Bologna-Roma, 2006, 75.

[36] Ddl 1119-B, Senato della Repubblica, XVII Legislatura.

rettifica della falsa notizia è, per il giornalista, obbligatoria»[37].
La rettifica come correzione della falsa notizia può essere poi imposta a livello giudiziale – come pena accessoria – mediante pubblicazione della sentenza *ex* art. 9 l. 47/1948.
La disciplina della rettifica per i giornalisti è sicuramente obbligatoria anche su Internet (e i *social networks*), in quanto essa è legata al carattere personale del giornalista, indipendentemente dal fatto che esso scriva su una testata *online* o su una pagina di un *social networks*, mentre la rettifica giudiziale potrebbe forse trovare una sua applicazione, teoricamente, anche alla rete perlomeno in relazione ai periodici *online*, che parte della giurisprudenza inizia a considerare come assimilabili a quelli cartacei[38].
In generale il problema della rettifica è che la notizia falsa avrebbe una "portata limitata" «se non ci fosse Internet, pronta a risputare ad ogni *search* il quadro preciso di quel momento di clamore mediatico, a far rimbalzare per l'eternità»[39] la notizia falsa. Alcuni innovativi orientamenti giurisprudenziali della Cassazione[40] hanno cercato di rispondere a queste problematiche imponendo forme di rettifica ai quotidiani *online*, ma il fenomeno non riguarda ancora i *social networks*.
Le soluzioni di rettifica risultano invero, come oggi formulate, del tutto inapplicabili rispetto ai *social networks*: è ormai non rimandabile una regolamentazione che permetta di applicare questi istituti anche a Facebook. La rettifica, come oggi intesa, andrebbe infatti richiesta contro il sito Internet diffusore delle false notizie; ma anche qualora quest'ultimo ottemperasse alla richiesta individuale o all'obbligo giudiziale la rettifica difficilmente raggiungerebbe gli utenti di Facebook che abbiano letto la bufala condivisa sul social. La correzione della *fake news* sul sito non garantirebbe la circolazione della rettifica sui *social networks* a causa della diffusione della stessa da parte dei singoli utenti e non dello stesso sito di bufale (che tendenzialmente non agisce direttamente sui *social networks*)[41]. Se è vero che il *locus* nel quale riproporre la rettifica sarebbe per l'appunto il sito produttore di *fake news*, un'applicazione di tal fatta disattenderebbe completamente la *ratio* della rettifica, in quanto il vero *locus* di diffusione sono i *social networks*. Nella più rosea delle previsioni difatti la rettifica riuscirebbe a raggiungere i nuovi fruitori della notizia, mediante modifica/cancellazione dell'articolo originale, ma non tutti quelli che ne hanno visionato il contenuto sui social. Raramente infatti gli internauti visionano contenuti direttamente sui siti fuori da Facebook (soprattutto per quanto riguarda le bufale), non tornando quindi sui siti da cui provengono determinate notizie (come avviene invece con un giornale o un programma televisivo/radiofonico). Da tutto ciò deriva che la rettifica dovrebbe dunque oggi, per avere efficacia, essere diretta ai *social networks* stessi. Una soluzione praticabile potrebbe dunque essere quella di delegare in parte la rettifica ai *social networks*: ossia mantenendo la rettifica sul sito originale, ma affiancandovi anche una rettifica sui *social networks* stessi. Se un *social networks* come Facebook riproponesse la rettifica della notizia falsa direttamente sulla *News Feed* (la sezione notizie) o sulla bacheca (ossia l'interfaccia principale del *social networks* dei singoli utenti) degli internauti che abbiano interagito con la bufala condivisa sul *social networks* (condividendola, mettendovi "mi piace" o commentandola) si avrebbe una rettifica realmente efficace.
Niente di tutto ciò oggi avviene. A seguito della risoluzione n. 2143 dell'Assemblea del Consiglio d'Europa, il legislatore italiano sta avviando un tentativo di regolamentazione della diffusione delle false notizie *online*: è in discussione al Senato il ddl 2688 "Disposizioni per prevenire la manipolazione dell'informazione *online*, garantire la trasparenza sul web e incentivare l'alfabetizzazione mediatica". Il ddl ha il merito di rilevare che «Le notizie false, o fake news o bufale, ci sono sempre state, ma non sono mai circolate alla velocità di oggi. Per questo non è più rinviabile un dibattito serio in questo senso»[42], ma non riesce a rilevare con altrettanta lucidità l'importanza giocata dai *social networks* nella divulgazione di *fake news*. Al contrario della risoluzione n. 2143, il ddl 2688 e

[37] Cass. pen., sez. II, sent. 16323/2006.
[38] Si veda in materia di sequestro preventivo delle testate *online* Cass. pen., sez. V, sent. 31022/2015. Cfr. C. Melzi d'Eril, *Contrordine compagni: le sezioni unite estendono le garanzie costituzionali previste per il sequestro degli stampati alle testate on-line registrate*, in www.penalecontemporaneo.it, 9 marzo 2016. Cfr. in relazione a Facebook ma anche a determinate implicazioni dell'orientamento estensivo della Cassazione del 2015: Cass. pen., sez. V, sent. 4873/2016; E. Birritteri, *Diffamazione e Facebook: la Cassazione conferma il suo indirizzo ma apre a un'estensione analogica in malam partem delle norme sulla stampa*, in www. penalecontemporaneo.it, 20 aprile 2017 e C. Melzi d'Eril - S. Vimercati, *Diffamazione, Facebook non è stampa*, in www.ilsole24ore.com, 8 febbraio 2017.
[39] E. Ciccarelli, *Le rettifiche al tempo di Internet*, in *New Media e Culture Digitali*, 2, 2011.
[40] «… non potendo (..) considerarsi in proposito sufficiente la mera generica possibilità di rinvenire all'interno del "mare di internet" ulteriori notizie concernenti il caso di specie, ma richiedendosi la predisposizione di sistema idoneo a segnalare (nel corpo o a margine) la sussistenza nel caso di un seguito e di uno sviluppo della notizia, e quale esso sia, consentendone il rapido ed agevole accesso ai fini del relativo adeguato approfondimento …». Cass. civ., sez. III, sent. 5525/2012. Cfr. G. Citarella, *Aggiornamento degli archivi online: tra diritto all'oblio e rettifica atipica*, in *Responsabilità civile e previdenza*, 3/2012, 1155 ss. Non si discutono le interessanti implicazioni fra verità storica e assoluta, ma si utilizza il caso come esplicativo delle esigenze di risposta all'eternità di Internet che è in grado di vanificare il diritto alla rettifica e alla verità dei fatti.
[41] Altro discorso potrebbe in teoria valere per le pagine Facebook dei giornali, per le quali la rettifica potrebbe effettivamente avere l'effetto di raggiungere gli stessi utenti, se non vi fosse il fenomeno della viralità. La rettifica ha molte poche probabilità di divenire virale come la bufala che vorrebbe smentire. Da cui la necessità di applicare la soluzione per i social che si proporrà anche in questo caso.
[42] Ddl S. 2688 - Senato della Repubblica, XVII Legislatura, 6.

la sua relazione di accompagnamento non fanno esplicito riferimento ai *social networks*.
Il ddl 2688 prevede per i soggetti gestori di «piattaforma informatica destinata alla pubblicazione o diffusione di informazione presso il pubblico», ai sensi dell'art. 3, l'applicazione della c.d. rettifica soggettiva (all'art. 4) e l'obbligo di rimozione di contenuti non ritenuti attendibili su segnalazione degli utenti o di propria iniziativa (all'art. 7).
Non è dato sapere dalla relazione[43] che accompagna il ddl se anche i *social networks* siano da inquadrare come «piattaforme informatiche». Supponendo che tale disciplina si applichi ai *social networks* essa risulterebbe molto problematica. In primo luogo la misura della rettifica "soggettiva" risulta spinosa perché dissociata da qualsiasi forma di controllo sulla verità oggettiva (mentre più efficace e sicura sarebbe stata la rettifica oggettiva). In secondo luogo l'intento – sicuramente lodevole – dell'obbligo di rimozione dei contenuti non attendibili, in una sorta di obbligo deontologico di rispetto della verità della cronaca, da un lato è collegato direttamente a una sanzione pecuniaria[44] di difficile applicazione e dall'altro delega questo controllo a soggetti di natura privata. Tutto ciò contribuisce ad un'ulteriore privatizzazione della censura: chi controlla che i gestori delle piattaforme (i *social networks*) non compromettano in maniera arbitraria l'informazione?
Questo discorso ovviamente vale qualora si dovesse ritenere l'art. 3 del ddl 2688 come comprendente anche i *social networks*; nel caso in cui la disciplina dovesse riguardare solo il c.d. giornalismo individuale (blog, forum, etc.) potrebbe probabilmente essere in qualche modo adeguata[45]. In quest'ultimo caso si tratterebbe della costituzione di un obbligo deontologico occulto, che in qualche modo equipara un gestore di un blog ad un giornalista.
Come invece si diceva prima, i *social networks* non sono strumenti di produzione di informazione in prima persona (come i blog, i forum etc.) ma casse di risonanza, che gestiscono contenuti di terzi. Un conto difatti sarebbe affidare il controllo di un blog al suo "proprietario", più rischioso sarebbe invece affidare il controllo della veridicità dei fatti ai gestori dei *social networks*: sarebbe come affidar loro le chiavi del sistema "new media – *social networks*", ricreando un "ministero della verità" privato, senza garanzie di imparzialità e neutralità. Non si può considerare infatti Facebook come una testata giornalistica, ma andrebbe oggi considerato come l'infrastruttura su cui circola l'informazione e come tale richiederebbe forme di tutela del pluralismo informativo.

4.2 I tentativi di contrasto alle *fake news* dei *social networks*: Facebook censore del vero e del male.

Nell'assordante silenzio dei legislatori sono stati gli stessi *social networks* a scendere in campo contro le *fake news*. Dal discorso del 16 febbraio 2017 di Mark Zuckerberg [46] sembra che i *social networks* siano molto più consapevoli della loro importanza per il mondo dell'informazione di quanto non lo siano i poteri pubblici. Peraltro già in passato il *CEO* di Facebook era stato costretto ad ammettere la natura di *media company* del *social network*[47]. Facebook ha deciso in questi mesi, dopo innumerevoli tentativi fallimentari di lotta alla diffusione di *fake news*[48], di intraprendere una nuova strategia di contrasto alle bufale (per ora solo negli USA)[49]. Dopo la segnalazione – attuabile da qualsiasi utente – dei contenuti ritenuti falsi, segue il controllo della veridicità della notizia da parte di una squadra di professionisti dell'informazione. Questo "controllo" è articolato su un

[43] «L'articolo 3, al comma 1, prevede che quando si apre un sito web privato, un blog, un forum o comunque una qualsiasi piattaforma elettronica destinata alla pubblicazione o diffusione online di informazione presso il pubblico» (Ddl S. 2688 Senato della Repubblica, XVII Legislatura, 8). Non si esplicita quindi se i *social networks* siano considerabili piattaforme informatiche ai sensi del ddl.

[44] La legge ha pensato alla sanzione dell'art. 656-*bis* (diffusione di false notizie on-line) in caso di non ottemperanza del "dovere deontologico occulto", sostituendo alla sanzione disciplinare direttamente il diritto penale.

[45] In ogni caso la rimozione del contenuto su un blog o un forum non garantisce la ricostruzione della verità dei fatti per gli utenti che abbiano già visionato la *fake news*, come circolata sui *social networks*.

[46] "*The two most discussed concerns this past year were about diversity of viewpoints we see (filter bubbles) and accuracy of information (fake news). I worry about these and we have studied them extensively, but I also worry there are even more powerful effects we must mitigate around sensationalism and polarization leading to a loss of common understanding. Social media already provides more diverse viewpoints than traditional media ever has. (..) Compared with getting our news from the same two or three TV networks or reading the same newspapers with their consistent editorial views, our networks on Facebook show us more diverse content*». M. Zuckerberg, *Building Global Community*, Facebook note, giovedì 16 febbraio 2017.

[47] *Clamorosa ammissione di Zuckerberg*, in www.ilfoglio.it, 22 dicembre 2016.

[48] Si pensi a strumenti quali la modifica degli algoritmi o a *Facebook Newswire* (P.L. Pisa, *Addio bufale, nasce Facebook Newswire*, in www.repubblica.it, 24 aprile 2014) che non erano efficaci e non erano in grado di disincentivare la condivisione, né evitare la viralità né di fornire rettifica, dove addirittura non finivano per promuovere le bufale nella sezione *Trending*, come avvenuto in Inghilterra (*Facebook ha altri problemi con i Trending Topics*, in www.ilpost.it, 31 agosto 2016. In generale per i problemi di Facebook con le bufale: Cfr. C. Dewey, *Il problema di Facebook con le notizie false,* in www.ilpost.it, 15 ottobre 2016).

[49] Ovviamente si tratta di un tipo di controllo coerente con il paradigma della libertà di espressione come tutelata dal Primo Emendamento, che non è equivalente a quella italiana/europea in termini di repressione delle notizie false. Per alcune prime analisi circa la sua efficacia cfr. G. Pennycook - T. Cannon - D.G. Rand, *Prior Exposure Increases Perceived Accuracy of Fake News*, in SSRN: https://ssrn.com, 30 aprile 2017.

double check di agenzie di *fact-checking* (in America si alternano: *Abc News*, *The Associated Press*, *PolitiFact* e *Snopes*[50]) il cui parere negativo sulla veridicità della notizia comporta la segnalazione della stessa come notizia "non attendibile". Questo tipo di controllo non è ancora approdato in Italia, ma mostra già alcune problematiche: in particolare questo strumento è lento ed efficace solo *pro futuro*, non fornendo alcun tipo di rettifica. È lento, perlomeno in queste sue applicazioni iniziali, poiché, come riportato dalla Stampa.it[51], la prima bufala sottoposta al regime *de quo* nella pendenza del processo di *fact-checking* aveva già raggiunto le 81mila condivisioni. Il secondo problema è per l'appunto correlato alla rilevanza solo *pro futuro* della segnalazione, mentre una corretta rettifica dovrebbe riuscire a raggiungere gli internauti che abbiano ricevuto false notizie al fine di ricostruire la verità, o meglio segnalare la completa falsità dei fatti descritti.
Il principale problema di questa disciplina è poi quello dei soggetti controllori. In Italia il mondo del giornalismo[52] ha sollevato alcuni dubbi sulla possibilità di scelte "politicamente orientate" dei *fact-checkers* da parte di Facebook. Il problema è serio ed è di nuovo dovuto alla latitanza dei legislatori che dovrebbero imporre quantomeno una selezione di *fact-checkers* che possa garantire il pluralismo informativo e la neutralità del controllo[53]. I *fact-checkers* infatti non sono angeli politicamente asessuati, ma soggetti che possono avere determinate idee politiche e decidere di "correggere" determinate notizie rispetto ad altre. Indubbiamente, dovendosi la tecnica applicare soprattutto a notizie di cronaca palesemente inventate (fatti di cronaca nera inventati con protagonisti stranieri, istituzione di vitalizi o tasse mai esistiti, denunce di brogli mai avvenuti), la parzialità politica viene ridotta, ma certamente in assenza di rigide procedure di azione potrebbe incidere, ad esempio, nei tempi di controllo delle bufale, che come si è visto sono vitali. Qualora questo sistema dovesse approdare anche in Italia, affidare la selezione o la stessa gestione del *fact checking* al tanto vituperato ordine dei giornalisti, salvato invece dalla Corte costituzionale[54], o a qualche autorità indipendente farebbe superare molte delle obiezioni inerenti a pluralismo e neutralità nel controllo. Non da ultimo non va dimenticato che ad oggi queste agenzie di *fact-checking* negli Stati Uniti agiscono a titolo gratuito, ma sono legate a determinati ambienti giornalistici e finanziari, che ne minano i presupposti di imparzialità. Da tutto ciò è necessario che un eventuale controllo non sia affidato esclusivamente a strutture di natura privata: lo stato dovrebbe infatti garantire la pluralità e la neutralità di questo particolare mezzo di controllo[55].

5 Conclusioni

L'avvento dell'epoca digitale e dei *social networks* ha cambiato definitivamente il modello dell'informazione e non si può tornare indietro a vecchi paradigmi e logiche pensate per un diverso mondo: «Come una forza della natura l'era digitale non può essere rifiutata o fermata»[56]. Per quanto riguarda il problema dei siti Internet che diffondono *fake news*, esso appare di minor rilevanza per diffusione e importanza e di più facile soluzione. Probabilmente un'adeguata sanzione penale per i siti sarebbe bastevole[57], ma il problema, come già detto, rimarrebbe in relazione ai *social networks* e alla diffusione delle notizie avvenuta nelle more dei procedimenti di sanzione. Un'eventuale repressione, benché efficace *pro futuro*, non garantirebbe la rettifica per gli utenti ormai (dis)informati a seguito della circolazione virale della notizia sui social. Inoltre, per i fenomeni cognitivi e sociologici già esplicitati, difficilmente la rettifica, anche pubblicata da altre parti, potrebbe raggiungere lo stesso grado di diffusione *virale* delle *fake news* sui *social networks*. Da tutto ciò dovrebbe derivare la necessità di attuazione di una regolamentazione dei *social networks* che potrebbe funzionare sul modello di verifica già sviluppato da Facebook per gli Stati Uniti con l'aggiunta di un meccanismo di visibilità della rettifica (la semplice riproposizione in bacheca o nella *News Feed* ad esempio) per gli utenti che abbiano in passato interagito con una notizia falsa (mettendovi *like*, condividendola

[50] M. Isaac, *How Facebook's Fact-Checking Partnership Will Work*, in www.nytimes.com, 15 dicembre 2016.
[51] B. Ruffilli, *Il sistema di verifica delle notizie false di Facebook arriverà presto anche in Italia*, in www.lastampa.it, 6 marzo 2017.
[52] D. Scalea, *Perché il fact-checking di Facebook resterà politicamente orientato*, in www.ilfoglio.it, 18 dicembre 2016.
[53] È vero che i *fact-checkers* devono avere sottoscritto il "Poynter's non-partisan code of principles", ma la sua attuale portata non è ancora certa.
[54] C. Cost. sentt. 11/1968 e 98/1968.
[55] Questa soluzione deriva da una precisa posizione teorica-dottrinale che è quella della fiducia nello stato democratico e che certamente si differenzia da quella di chi, in un'ottica di libertà di pensiero esclusivamente come libertà negativa dallo stato, sia portato a ritenere auspicabile il minore intervento possibile dello stato nel c.d. *marketplace of ideas*.
[56] Cfr. N. Negroponte, *Essere digitali*, Milano, 1995, 237-239.
[57] Ci si è occupati in altra sede degli strumenti penali per sanzionare i siti-fabbrica di bufale. Cfr. M. Monti, *op. cit.*. Ad oggi gli strumenti vigenti paiono inefficaci e neanche l'art. 656-bis del ddl 2688 sembra idoneo ad una repressione efficace dei siti-fabbrica, in quanto una sanzione pecuniaria non commisurata agli introiti dei siti potrebbe risultare inefficace rispetto agli enormi guadagni derivati dal *click-baiting*.

o commentandola[58]). Gli utenti che abbiano interagito con una bufala potrebbero così essere informati del carattere inventato della notizia letta con avviso mediante "notifica" (il meccanismo di segnalazione di interesse di Facebook) o con indicazione al posto del c.d. *Buongiorno* (la sorta di icona *pop-up* o di *alert* che appare in cima al *News Feed* degli utenti).
Ovviamente il procedimento di "rettifica" dovrebbe essere comunque attivato a seguito di una verifica, la quale non può però essere delegata a soggetti privati: i rischi della privatizzazione della censura sono enormi[59]. Per questo il procedimento di rettifica della falsità delle notizie dovrebbe connotarsi come un procedimento pubblico-privato dove solo l'esecuzione sarebbe delegata ai *social networks*, mentre la verifica sarebbe principalmente delegata ad organi pubblici, come l'ordine dei giornalisti o qualche autorità indipendente (o a seguito di verifica giudiziale). Si tratterebbe quindi di individuare i *social networks* come *social media* e imporre loro quest'obbligo di rettifica: una volta accertata la falsità di un contenuto da parte di un soggetto pubblico, connotato dai caratteri di imparzialità e neutralità, Facebook dovrebbe riproporre sulla *News Feed* o sulla bacheca degli utenti che abbiano interagito con una *fake news* la rettifica della stessa mediante anche un meccanismo di visibilità come la notifica o il c.d. *Buongiorno*. In questo modo si rispetterebbe il principio che vuole la rettifica pubblicata nello stesso *locus* ove veniva a trovarsi la notizia falsa, si garantirebbe un'opportunità di *debunking* e non si arriverebbe ad alcuna forma di *silencing*.
Il controllo sulla verità "oggettiva" delle notizie, sul modello di quello svolto in materia di radiotelevisione, certamente non lederebbe il pluralismo informativo, anzi: l'importanza di Facebook nella diffusione di notizie *online* impone qualche forma di regolamentazione, esattamente come avvenne in passato per le notizie diffuse dal sistema radio-televisivo[60]. Il controllo sulla verità oggettiva e la riproposizione della rettifica nel sistema radio-televisivo è infatti uno degli strumenti a tutela (anche) dell'interesse pubblico alla corretta informazione che non si pone in contrasto con il pluralismo informativo, ma anzi ne è a fondamento.
Nella soluzione testé proposta il controllo, preliminare alla attivazione di questa forma di rettifica su Facebook, sarebbe tuttavia attivabile da qualsiasi utente: prevalente sarebbe dunque l'interesse generale ad una corretta informazione più che quello del diritto soggettivo alla rettifica.
Ovviamente questa soluzione, affidando questa forma di controllo a soggetti terzi, neutri e indipendenti (autorità indipendenti od ordine dei giornalisti), non contrasterebbe con la tutela garantita dall'art. 21 Cost. alla libertà di informazione (essendo, come visto, il subiettivamente falso categoria non protetta) e anzi garantirebbe mediante questa rettifica (come già avviene per la radiotelevisione e la carta stampata[61]) forme di tutela del *public discourse* contro l'inquinamento dovuto alle false notizie. Inoltre la soluzione, rimanendo estranea al diritto penale e prospettandosi solo come forma di rettifica, non impatterebbe sulla libertà personale e nemmeno si configurerebbe come forma di censura, in quanto si limiterebbe a "proporre" la verità oggettiva al lettore.
La maggior problematica di questo sistema riguarda ovviamente la fattibilità e sostenibilità di una tale soluzione: il costo dell'allestimento di un ufficio che si occupi a tempo pieno dell'attività di *fact-checking* non appare tuttavia proibitivo per uno stato e i costi sarebbero giustificati dai benefici per il sistema democratico e il dibattitto pubblico; inoltre la maggior parte delle bufale essendo fatti palesemente inventati è di facilissima smentibilità. Il lavoro di controllo – dotando il soggetto controllore delle risorse necessarie – sarebbe dunque di facile esplicazione. Facebook dovrebbe dunque inviare all'ufficio le notizie segnalate dagli utenti – come fa negli Usa con le agenzie esterne di *fact-checking* – e una volta attuato il controllo dovrebbe rettificare nella modalità sopra vista la notizia falsa: questa rettifica raggiungerebbe tutti gli utenti che abbiano interagito con la *fake news*. Rispetto al sistema di controllo/avviso privato sperimentato da Facebook negli Usa, di cui si è dato conto nel paragrafo precedente, il sistema *de quo* garantirebbe da una parte l'imparzialità dei controllori e dall'altra parte un risultato efficace della rettifica delle *fake news* con il raggiungimento di tutti gli utenti che abbiano *interagito* con le stesse. A tal proposito giova evidenziare che anche qualora il sistema si rilevasse lento come quello Usa – eventualità peraltro non scontata, vista la possibilità di approntare un apparato pubblico efficiente e non organismi privati operanti a titolo gratuito come in America – questo non graverebbe eccessivamente sull'efficienza dello stesso. La tempistica è infatti fondamentale per il sistema sviluppato da Facebook negli Stati Uniti in grado di agire solo *pro futuro* (avvertendo della possibilità della falsità della notizia

[58] La soluzione non garantirebbe comunque il raggiungimento di quegli utenti che abbiano letto la notizia senza "interagirvi", ma sarebbe senz'altro un buon primo passo.
[59] Cfr. M. Bettoni, *Profili giuridici della privatizzazione della censura*, in *Ciberspazio e Diritto*, 12/2011, 363 ss., spec. 375. In particolare si veda in relazione ai problemi di censura legati ai *social networks* la bibliografia in nota 27. Si veda anche per qualche spunto dal diritto straniero la bozza del ddl tedesco in materia di *fake news* sui *social networks* ("Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken")
[60] Cfr. per qualche considerazione in relazione alla necessità di regolamentare mass media dal notevole impatto "pervasivo": C. Cost., sent. 155/2002.
[61] Su questi mass media tradizionali, giova ricordarlo, agiscono altri strumenti di tutela della verità come il codice deontologico dei giornalisti che impone, *ex* art. 2 l. 69/1963, «il rispetto della verità sostanziale dei fatti».

solo i nuovi internauti-lettori), ma non sarebbe altrettanto fondamentale per quanto prospettato in questa sede: anche se nella pendenza del procedimento di controllo della falsità della notizia la bufala dovesse diffondersi, la rettifica su Facebook raggiungerebbe tutti gli utenti che vi abbiano interagito in passato e che vi potrebbero interagire in futuro. Certo, il problema continuerebbe a rilevare per gli utenti che non abbiano interagito con la *fake news* (leggendo la notizia e basta, non condividendola, non mettendovi *like* o non commentandola), ma senz'altro tale procedimento risulterebbe fortemente di impatto e riduzione del fenomeno delle bufale sul *social networks* Facebook[62]. Questo tipo di soluzione garantirebbe infatti un più corretto funzionamento del *marketplace of ideas* per gli utenti dei social: la smentita/rettifica da parte di organi autorevoli è forse in grado di garantire un'adeguata credibilità alla ricostruzione della falsità/verità di un fatto anche dal punto di vista sociologico/cognitivo[63].

Peraltro proprio questa forma di rettifica se da un lato potrebbe essere coerente anche con l'idea americana del *marketplace of ideas* – non addivenendosi a forme di censura o repressione, ma solo all'inserimento nel mercato della verità – da un altro potrebbe contribuire anche allo sviluppo di una coscienza critica degli internauti. Invero, questo strumento di rettifica potrebbe divenire negli anni obsoleto qualora dovesse svilupparsi il giusto senso critico negli utenti dei social rispetto alle *fake news*. Nell'attesa della nascita di questo "scetticismo programmatico", tuttavia, sembra necessario lo sviluppo di tale forma di rettifica a causa dei rischi per il *public discourse* derivanti dalla diffusione delle *fake news* sul *social network* Facebook.

[62] Questa considerazione va svolta nella consapevolezza che Facebook sarebbe comunque in grado di sapere quali utenti abbiano anche solo aperto un link postato sulla piattaforma del *social network* e quindi potrebbe probabilmente e potenzialmente essere in grado di raggiungere tutti gli internauti che abbiano anche solo cliccato sul link di una *fake news*.

[63] È infatti importantissima da questo punto di vista la «*credibility of the source of the correction*» (C. Sunstein, *op. cit.*, 75-80).

The market place of ideas nell'era della post-verità: quali responsabilità per gli attori pubblici e privati *online*?

The Market Place of Ideas in the Post-Truth Age: which Liability for Public and Private Actors on the Internet?

Giovanni De Gregorio
Dottorando di ricerca in Diritto costituzionale, Università degli Studi di Milano "Bicocca"

Abstract

Nella società dell'informazione il web è diventato fonte di notizie e di conoscenza. Una sempre maggiore fetta della popolazione tende a soddisfare il proprio bisogno informativo attraverso la consultazione di svariate piattaforme *online* sebbene i tradizionali canali di comunicazione quali TV e radio conservino tutt'ora un ruolo rilevante. L'aumento delle fonti di informazioni ha condotto ad un incremento del pluralismo informativo rendendo spesso difficile per il cittadino medio discernere tra le numerose informazioni offerte sulla rete. Grazie alla possibilità di accedere a tali contenuti direttamente dal proprio *device* in ogni momento della giornata, le notizie *online* hanno assunto una forte influenza sulla formazione dell'opinione pubblica e, di conseguenza, sulla società nel suo insieme. Negli ultimi mesi la sempre maggiore diffusione di notizie false sul web, conosciute come *fake news*, ha acceso il dibattito sulla libertà di espressione e sui diritti degli utenti nel *free market place of ideas*. In tale contesto, nonostante il concetto di *free market place of ideas* possa affascinare i difensori della libertà di espressione, tuttavia nell'attuale sistema europeo dei diritti non è possibile far prevalere incondizionatamente la libertà di espressione sugli altri diritti fondamentali che, in quanto tali, meritano di essere tutelati attraverso un'attività di bilanciamento che avviene *ex-ante* da parte del legislatore in sede di emanazione delle leggi o *ex-post* da parte delle Corti. A tal punto, risulta necessario un ripensamento del concetto di *free market place of ideas*, e, pertanto, sarà opportuno esaminare il ruolo degli attori pubblici e degli attori privati nella società dell'informazione – o meglio nel nuovo *digital market place of ideas*.

In the information society, the Internet has become one of the main source of information and knowledge. People increasingly rely on different online platforms in order to satisfy their information needs although the traditional channels of communications, such as TV and radio, still play a relevant role. However, the development of new sources of information has led to the increase of media pluralism, making particularly difficult for citizens to understand the level of truth of the online information. Moreover, thanks to the possibility to access online contents directly by using personal devices in any situation, the online information has strongly impacted on the formation of the public opinion and, consequently, on the overall society. In the last months, the diffusion of fake news on the Internet has led to the development of a debate about the freedom of expression online and the rights of users in the free market place of ideas. Although the free market place of ideas doctrine could fascinate the supporters of freedom of expression, however, in the current European framework of protection of fundamental rights, freedom of expression cannot always prevail over the other fundamental rights which deserve protection through the balancing activity performed by public actors. Hence, it is necessary to contextualize the free market place of ideas doctrine in the information society in order to understand the role of public and private actors in the new digital market place of ideas.

Sommario

libertà di espressione
responsabilità degli ISP
social network
fake news
Internet

1 *Fake news* e post-verità.

Negli ultimi mesi la sempre maggiore diffusione di notizie false sul web, le cosiddette *fake news,* ha acceso il dibattito sulla libertà di espressione, in particolare sul concetto di post-verità. Il termine post-verità, ormai diffusosi a seguito degli avvenimenti riguardanti le elezioni presidenziali negli Stati Uniti e il referendum sulla Brexit, non è tuttavia di facile definizione. L'Oxford Dictionary, scegliendo il termine *post-truth* come parola dell'anno 2016, ha fornito la seguente definizione: «*relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief*». In altre parole, con la suddetta espressione ci si riferisce alla sfera delle argomentazioni, caratterizzate da un forte appello all'emotività, spesso radicate su credenze diffuse e su fatti non verificati, che tendono ad essere accettate come realtà, influenzando l'opinione pubblica convinta del senso logico-emozionale delle affermazioni presentate.
Seppur il suddetto termine risulta essere stata coniato in tempi piuttosto recenti[1], il fenomeno non è sconosciuto nella storia: da tempo immemore l'emotività e i pregiudizi hanno influenzato la verità connotandola di elementi tutt'altro che oggettivi. In particolare, da sempre nello scontro politico o nella concorrenza commerciale lo screditamento dell'avversario o del concorrente attraverso notizie false o non del tutto vere ha costituito uno strumento forte di influenza dell'opinione pubblica[2].
Tuttavia, comprendere quali notizie possano essere definite *fake* e quali invece debbano essere tollerate ricadendo all'interno dell'ambito di protezione della libertà di manifestazione del pensiero può non risultare sempre immediato. Nei sistemi costituzionali occidentali la libera manifestazione del pensiero costituisce uno dei capisaldi dei sistemi democratici e, come tale, gode di un riconoscimento di matrice costituzionale tutelando anche espressioni del pensiero diverse anche se opposte alla propria posizione o particolarmente critiche. La portata della libertà di espressione è inoltre alla base di ulteriori valori costituzionali come la libertà di ricerca scientifica e artistica o la libertà di professare liberamente il proprio culto.
Secondo la definizione fornita Allcott e Gentzkow, le *fake news* comprenderebbero quegli articoli le cui notizie o informazioni sono intenzionalmente false nonché possibili da verificare tali da trarre in inganno i lettori[3]. Sulla base di tale definizione, soltanto le notizie false e capaci di ingannare i lettori rientrerebbero nel campo delle *fake news*. Al contrario, molte altre informazioni che sembrerebbero ricadere nell'ambito delle notizie false, potrebbero invece essere ritenute espressioni libere del pensiero di ciascuno[4]. In particolare, è necessario sottolineare la differenza che sussiste tra i fatti e le opinioni espresse in merito, essendo i primi connotati di un livello di veridicità spesso accertabile diversamente dalle opinioni che consistono in giudizi critici o ipotetici sui medesimi fatti. Il rischio di concentrarsi sul censurare le opinioni piuttosto che condannare quei dati fattuali che risultano falsi condurrebbe a rendere impossibile in astratto mettere in dubbio lo *status quo* dal momento che ogni opinione riconducibile ad un messaggio ostile o divergente rispetto allo stato dei fatti verrebbe probabilmente etichettata come falsa.
Il breve inquadramento proposto non sembra chiarire però il motivo per cui il dibattito sul tema si sia (ri)acceso. Infatti, ciò che ha spinto l'opinione pubblica ad interessarsi alle notizie false attiene al mezzo con cui vengono diffuse ossia la rete, o più in generale il mondo dei bit. Nella società dell'informazione il web sta diventando fonte – spesso primaria – di notizie e di conoscenza. Una sempre maggiore fetta della popolazione tende a soddisfare il proprio bisogno informativo attraverso la consultazione di svariate piattaforme *online*, nonostante occorra sottolineare che in molti paesi tra cui l'Italia la fruizione delle informazioni sia legata in gran parte ai canali tradizionali, in

[1] Secondo la breve ricostruzione fornita dall'Oxford Dictionary, il termine *post-truth* fu usato per la prima volta nel 1992, in un articolo scritto dal drammaturgo Steve Tesich, apparso sulla rivista statunitense The Nation. In merito al caso Iran-Contra e sulla prima guerra del Golfo, Tesich scriveva: «noi, come popolo libero, abbiamo liberamente scelto di voler vivere in una specie di mondo di post-verità».

[2] Le *fake news*, infatti, non costituiscono una novità o una rivoluzione nel mondo dell'informazione. Un esempio non troppo recente risale al 1835 quando il New York Times ha pubblicato una serie di articoli che parlavano della scoperta della vita sulla Luna ("Great Moon Hoax"). Un esempio meno risalente riguarda una stazione televisiva pubblica belga che, nel 2006, riportava che il Parlamento fiammingo avrebbe dichiarato la secessione dal Belgio, notizia che fu ritenuta vera da molti telespettatori ("Flemish Secession Hoax"). Spunti interessanti di riflessione sulla società moderna si ricavano da Z. Baumann, *Modernità liquida,* Bari-Roma, 2011. Si veda anche J. Baldwin-Philippi, *Using Technology, Building Democracy. Digital Campaign and the Construction of Citizenship*, New York, 2015.

[3] H. Allcott - M. Gentzkow, *Social Media and Fake News in the 2016 Election*, in 31(2) *Journal of Economic Perspectives*, 2017, 211 ss.

[4] Si pensi in particolare gli errori colposi derivanti dalla diffusa credenza riguardo uno specifico fatto, spesso stimolati da notizie frammentate del web che non originano da una particolare fonte che essendo comunicati tra gli internauti acquistano credibilità non attraverso la verifica dei relativi fatti, ma tramite l'accettazione sociale della loro veridicità. Un altro esempio è la satira che è formata interamente da opinioni su fatti presentate in modo critico oppure i risultati del giornalismo investigativo che spesso non sono del tutto veritieri a causa di ricostruzioni dei fatti basate su ipotesi.

particolare la televisione[5]. Tra le diverse piattaforme *online* è possibile distinguere tra quelle che forniscono servizi tradizionali di informazione, come i giornali e le radio, che hanno esteso la loro attività anche sul web e dall'altra i *social network* dove le informazioni non derivano da un preciso progetto editoriale dalla piattaforma, ma sono il frutto degli *upload* degli utenti. L'aumento delle fonti di informazioni ha condotto ad un incremento del pluralismo informativo rendendo spesso difficile per il cittadino medio discernere tra le numerose informazioni offerte sulla rete[6]. Grazie alla possibilità di accedere a tali contenuti direttamente dal proprio *device* in ogni momento della giornata senza sostenere alcun costo se non quello legato al traffico dati, le notizie *online* hanno assunto una forte influenza sulla formazione dell'opinione pubblica e, di conseguenza, sulla società nel suo insieme. Nonostante l'ascesa del pluralismo informativo sia da considerarsi generalmente un fenomeno particolarmente positivo per lo sviluppo e il mantenimento di società democratiche dal momento che contribuisce a promuovere diverse manifestazioni del pensiero in un confronto sempre più eterogeno, tuttavia occorre sottolineare come il "sovraccarico informativo" della rete ha condotto gli internauti a ridurre sempre più il tempo speso per i singoli contenuti divenendo sempre meno attenti[7].

In un tale contesto, lo sviluppo delle nuove tecnologie, in particolare quelle legate agli algoritmi, ha reso ancor più complesso il quadro d'insieme dal momento che, oltre alla difficoltà di orientarsi nell'infinito numero di informazioni a disposizione, i cittadini non sono consapevoli delle implicazioni derivanti dall'implementazione di tecnologie di profilazione che, utilizzando meccanismi di decisione automatizzata, stabiliscono la presentazione e l'organizzazione dei contenuti ossia l'*an*, il *quantum* e il *modus* con cui le informazioni vengono presentate sulla base di interessi e logiche scarsamente trasparenti[8]. Nel libro "The Filter Bubble: What the Internet Is Hiding from You"[9], Pariser ritiene che il fenomeno della "personalizzazione" dei contenuti *online* comporta la creazione di bolle di filtraggio all'interno delle quali ciascun internauta rimane isolato da ciò che differisce dai propri interessi sulla base di un mero calcolo algoritmico. In altre parole, durante la navigazione sul web, gli algoritmi delle più note piattaforme *online* quali ad esempio Google e Facebook selezionano le informazioni da mostrare agli utenti sulla base di criteri, quali ad esempio le precedenti ricerche o il tempo di visualizzazione di un singolo contenuto. Tali criteri sono di volta in volta aggiornati ai fini di ottenere una profilazione sempre più precisa degli utenti che sono spinti a fruire maggiormente di quelle informazioni che appartengono maggiormente alle proprie categorie d'interessi con un conseguente svilimento del pluralismo informativo esistente.

La mancanza di consapevolezza di tale quadro d'insieme da parte della maggior parte dei fruitori delle informazioni *online* comporta che gli internauti non siano particolarmente attenti nel verificare il grado di veridicità delle notizie *online* considerata inoltre la mole di informazioni da fronteggiare.

Attraverso uno sforzo di semplificazione è possibile individuare i due opposti schieramenti del dibattito relativo alla post-verità: da un lato, vi sono i sostenitori della libertà di espressione i quali ritengono che la propria libertà di manifestazione del pensiero debba essere garantita anche nella sua estensione *online*, dall'altro, vi sono le posizioni maggiormente garantiste di coloro i quali ritengono che, sebbene la libertà di espressione debba essere tutelata in quanto diritto fondamentale sui cui si basa ogni società democratica, tuttavia, il mezzo con cui vengono diffuse le informazioni

[5] Su tale punto risulta opportuno segnalare il documento annuale prodotto dall'agenzia Eurostat, *Community survey on ICT usage in Households and by Individuals*. Secondo la relazione annuale 2016 dell'AGCOM la televisione rappresenta tuttora il mezzo con la maggiore valenza comunicativa. Al riguardo, una recente indagine condotta da SWG per l'autorità relativa al 2015, ha rilevato come la quasi totalità della popolazione (il 96%) ha avuto accesso alla Tv nella settimana precedente alla rilevazione, visualizzando i contenuti audiovisivi mediante diversi dispositivi. Si vedano inoltre i dati Istat sull'utilizzo dei mass media tradizionali pubblicati su http://dati.istat.it/ che evidenziano come la televisione risulta il mezzo più utilizzato dalla popolazione italiana, mentre la percentuale dell'utilizzo di Internet si colloca a livelli inferiori.

[6] Sul tema del pluralismo informativo si veda F. Donati, *Democrazia, pluralismo delle fonti di informazione e rivoluzione digitale*, in *Federalismi.it*, 20 novembre 2013.

[7] Il dibattito sull'*information overload* comprende posizioni diverse. Sul punto di cui sopra si vedano in particolare J. Ellul, *The Technological Bluff*, Grand Rapids, 1990; N. Postman, *Technopoly: The surrender of Culture to Technology*, New York, 1992. Alcuni autori, tra i quali Wurman e Lewis, hanno inoltre sostenuto come l'*information overload* sia alla base di alcune condizioni di stress derivanti dal dover fronteggiare una quantità eccessiva di dati e informazioni denominando tali forme come *Information Fatigue Sindrome* (IFS) e *Information Anxiety*.

[8] Il tema della trasparenza dei processi decisionali automatizzati risulta il cuore del dibattito sulla regolamentazione degli algoritmi e sulle loro implicazioni sociali. Si veda K. Crawford, *Can an algorithm be agonistic? Ten scenes from life in calculated publics*, in *Science,* in 41(1) *Technology & Human Values* (2016), 77 ss.; D. Neyland, *Bearing accountable witness to the ethical algorithmic system*, in 41(1) *Science, Technology & Human Values* (2016), 50 ss.; A. Raymond, *The dilemma of private justice systems: Big Data sources, the cloud and predictive analytics*, in *Northwestern Journal of International Law & Business*, 2014; M. Turilli - L. Floridi, *The ethics of information transparency*, in 11(2) *Ethics and Information Technology* (2009), 105 ss.; R. Kitchin, *Thinking critically about and researching algorithms*, in 20(1) *Information, Communication & Society* (2016), 14 ss.; L.A. Granka, *The politics of search: A decade retrospective*, in 26(5) *The Information Society* (2010), 364 ss.; A. Rubel - K. Jones, *Student privacy in learning analytics: An information ethics perspective*, SSRN Scholarly Paper, Rochester, NY: Social Science Research Network, 2014 M. Taddeo, *Modelling trust in artificial agents, a first step toward the analysis of e-trust*, in 20(2) *Minds and Machines* (2010), 243 ss.; V. Wiegel - J. van den Berg, *Combining moral theory, modal logic and mas to create well-behaving artificial agents*, in 1(3) *International Journal of Social Robotics*, (2009), 233 ss.; C. Dwork - M. Hardt - T. Pitassi, et al. *Fairness through awareness*, arXiv:1104.3913 [cs], 2011; F.S. Grodzinsky - K.W. Miller - M.J. Wolf, *Developing artificial agents worthy of trust: 'Would you buy a used car from this artificial agent?'*, in 13(1) *Ethics and Information Technology* (2010), 17 ss.

[9] E. Pariser, *The Filter Bubble: What the Internet Is Hiding from You,* New York, 2012.

condiziona il bilanciamento di tale libertà con altri diritti al fine di garantire che le libere opinioni *online* non vengano sopraffatte da pregiudizi e stereotipi costruiti artificialmente e tutelare altri diritti confliggenti come, ad esempio, quello dei soggetti vulnerabili, in particolare dei minori.
In tale contesto, comprendere il ruolo degli attori pubblici e degli attori privati risulta di fondamentale importanza ai fini di individuare ruoli e responsabilità volti a contrastare la diffusione di informazioni false *online*. In particolare, negli ultimi anni alcuni attori privati come Google e Facebook hanno sviluppato tecnologie e nuovi modelli di business tali da acquisire potere e controllo di un enorme quantità di dati degli utenti anche attraverso di tecnologie di analisi basate sugli algoritmi. il ruolo preminente di tali attori privati *online* nel diffondere notizie attraverso piattaforme di *social networking* costituisce uno dei motivi che ha attirato l'attenzione sui profili di responsabilità ai quali sono sottoposti tali piattaforme e sull'opportunità di introdurre misure di regolamentazione emanate da parte di attori pubblici al fine di contrastare tale fenomeno.
Pertanto, nella prima parte dell'elaborato si descriverà l'evoluzione della metafora del *free market place of ideas* al fine di inquadrare l'attuale dibattito sulla post-verità e la libertà di manifestazione del pensiero. Nella seconda parte si analizzeranno le misure di contrasto alle *fake news* implementate dagli attori pubblici in Europa con particolare attenzione alla legge tedesca che entrerà in vigore nell'ottobre 2017 che ha introdotto stringenti obblighi di rimozione alle piattaforme *online* in caso di segnalazione di contenuti illeciti. A seguire verrà delineato il regime di responsabilità delle piattaforme *online* in Europa per poi nell'ultima parte valutare se l'utilizzo da parte dei *social network* di algoritmi al fine del controllo delle notizie costituisca un'attività di controllo sui contenuti tale da stravolgere il quadro di responsabilità di tali piattaforme come stabilito dalla Direttiva e-Commerce.

2 La metafora giuridica del *free market place of ideas*

Tra le metafore giuridiche esistenti quella del *free market place of ideas* è una delle più suggestive[10]. L'espressione, sebbene utilizzata per la prima volta nel caso nel caso *United States v. Rumely* nel 1953 da Justice Douglas[11], tuttavia ha radici storiche ben più profonde.
Alla base delle teorie legate al *free market place of ideas* vi è la radicale convinzione liberista secondo la quale gli individui in quanto razionali sono capaci di discernere i prodotti e i servizi migliori in un mercato libero che tramite il meccanismo concorrenziale produrrà effetti positivi per l'intera società. Come in un mercato concorrenziale dove i migliori prodotti o servizi prevalgono, lo stesso avviene per le informazioni vere e corrette destinate ad essere predilette dal mercato stesso.
Ben prima dello sviluppo del pensiero illuminista, nel XVII secolo, John Milton nel suo scritto *Areopagitica*[12] prende posizione sul tema della libertà di espressione scagliandosi apertamente contro la *Press Ordinance* del 14 giugno 1643, con il quale il Parlamento inglese aveva introdotto un sistema di censura *ex-ante* volto a punire i promotori di idee considerate illecite. In particolare, Milton riteneva che la libertà di espressione non dovesse essere limitata dal momento che la verità avrebbe comunque prevalso grazie ad un incontro libero tra le opinioni senza il bisogno di disporre di misure censorie[13]. In particolare, Milton paragona la verità ad una *streaming fountain* le cui acque vengono inquinate dal pregiudizio quando vengono imposti dei blocchi al continuo fluire delle sue acque[14]. La metafora di Milton esprime il cuore del suo pensiero: l'acqua della fontana costituisce

[10] Per un approfondimento sul concetto di *free market place of ideas* si vv. R. Coase, *Markets for goods and Market for ideas*, in 64(2) *American Economic Review* (1974), 384 ss.; S. L. Winter, *A Clearing in the Forest: Law, Life, and Mind*, Chicago, 2003; B. Gregory, *How Much Does a Belief Cost? Revisiting the Marketplace of Ideas*, in 21(1) *Southern California Interdisciplinary Law Journal* (2011), 2 ss.; J. Blocher, *Institutions in the marketplace of ideas*, in 57(4) *Duke Law Journal* (2008), 820 ss.; P. H. Brietzke, *How and why the marketplace of ideas fails*, in 31(3) *Valparaiso University Law Review* (1997), 951 ss.; M. Gentzkow - J. M. Shapiro, *Competition and Truth in the Market for News*, in 22(2) *Journal of Economic Perspectives* (2008), 133 ss.; D. E. Ho - F. Schauer, *Testing the marketplace of ideas*, in 90 *New York University Law Review* (2015), 1161 ss.; M. N. Browne - J. Rex - D.L. Herrera, *Potential Tension Between a "Free Marketplace of Ideas" and the Fundamental Purpose of Free Speech*, in 3 *Akron Journal of Constitutional Law and Policy* (2012), 56 ss.; E. Volokh, *In defense of the market place of ideas / search for truth as a theory of free speech protection*, in 97(3) *Virginia Law Review* (2011), 591 ss.; D.D. McGeough, *Selling the "Marketplace of Ideas" and Buying Fish, Bollinger, and Baker*, in 10 *Kaleidoscope: A Graduate Journal of Qualitative Communication Research* (2011), 37 ss.; A.I. Goldman - J.C. Cox, *Speech, truth, and the free market for ideas*, Cambridge, 1996.

[11] *United States v. Rumely* 345 U.S. 41 (1953): «*Of necessity I come then to the constitutional questions. Respondent represents a segment of the American press. Some may like what his group publishes; others may disapprove. These tracts may be the essence of wisdom to some; to others their point of view and philosophy may be anathema. To some ears their words may be harsh and repulsive; to others they may carry the hope of the future. We have here a publisher who through books and pamphlets seeks to reach the minds and hearts of the American people. He is different in some respects from other publishers. But the differences are minor. Like the publishers of newspapers, magazines, or books, this publisher bids for the minds of men in the market place of ideas*».

[12] J. Milton, *Aeropagitica*, London, 1644.

[13] Nella suddetta opera Milton sostiene: «*so Truth be in the field, we do injuriously, by licensing and prohibiting, to misdoubt her strength. Let her and Falsehood grapple; who ever knew Truth put to the worse, in a free and open encounter?*»

[14] Ancora nella stessa opera Milton: «*Truth is compared in Scripture to a streaming fountain; if her waters flow not in perpetual progression, they sicken into a muddy pool of conformity and tradition*».

il fluire delle informazioni che libera l'uomo dal pregiudizio dal momento che la verità lo conduce al sommo sapere. In tale ottica, è necessario evitare qualsiasi interferenza al fluire delle informazioni al fine di permettere all'uomo di conoscere la verità.

Lo stretto legame consequenziale sussistente tra il garantire la libertà di espressione e il raggiungimento della verità risulta essere espresso non solo dalle idee di Milton, ma anche da John Stuart Mill nella sua opera On liberty del 1859. In particolare, Mill riteneva che anche le opinioni false potessero essere ipoteticamente vere dal momento che l'uomo non può dare come assodate le proprie verità. Altrimenti, tale assunto equivarrebbe a sostenere che l'uomo ha raggiunto il massimo sapere e, pertanto, il confronto tra le opinioni non avrebbe alcun significato – assunto chiaramente non condivisibile[15]. Da tale osservazione deriva che le opinioni false possano contenere anche una parte di verità che non può essere sacrificata per ragioni censorie dal momento che l'uomo può non conoscere la verità nella sua interezza[16]. Inoltre, anche qualora, un'opinione sia effettivamente falsa e venga censurata, tale attività repressiva pregiudicherebbe comunque il confronto tra le opinioni con il rischio di dogmatizzare la verità corrente impedendo l'evoluzione delle opinioni nella società che considererebbe vere soltanto quelle opinioni che fino a quel momento erano state ritenute tali, senza interrogarsi o confrontarsi con altre posizioni[17]. Secondo Mill, infatti, non esiste un unico concetto di verità ma sussistono diverse opinioni che seppur in parte false o incomplete nel loro confronto possono formare una verità completa o possono contribuire ad arrivare a quest'ultima via via attraverso un processo dialettico che avviene in un libero mercato delle idee.

La portata delle idee liberali appena descritte risulta palesarsi anche nel XX secolo, in particolare nella *dissenting opinion* di Justice Holmes nel caso *Abrams v. United States* del 1919[18], tuttora viene ritenuta come l'essenza costituzionale della libertà di espressione negli Stati Uniti[19]. In particolare, la vicenda riguardava la distribuzione di volantini che incitavano allo sciopero le fabbriche di munizioni al fine di esprimere un chiaro messaggio di resistenza contro l'intervento militare degli Stati Uniti in Russia. Nella sua *dissenting opinion*, Justice Holmes sosteneva che, sebbene l'uomo cerchi di sostenere le proprie posizioni criticando le posizioni opposte, questi non deve illudersi che le proprie opinioni siano certe. Soltanto il confronto libero tra le opinioni confermerà la correttezza delle proprie posizioni[20]. Pertanto, Holmes, riprendendo Mill seppur con alcune differenze, ritiene che al fine di incrementare il livello di verità delle informazioni, bisogna promuovere il confronto tra le idee.

Nonostante il concetto di *free market place of ideas* anche alla luce della summenzionata pronuncia possa affascinare i difensori della libertà di espressione, tuttavia nell'attuale sistema europeo dei diritti fondamentali non è possibile far prevalere incondizionatamente la libertà di espressione sugli altri diritti fondamentali che, in quanto tali, meritano di essere tutelati attraverso un'attività di bilanciamento che avviene ex-ante da parte del legislatore in sede di emanazione delle leggi o ex-post da parte delle Corti.

Alla luce dell'attuale sistema dei diritti in Europa, il concetto di *free market place of ideas* necessita di essere ancora una volta approfondito, analizzando il ruolo degli attori pubblici e degli attori privati nella società dell'informazione – o meglio nel *digital market place of ideas*.

---

15 J. Mill, *On liberty*, London, 1859. In primo luogo, secondo Mill: «*First, if any opinion is compelled to silence, that opinion may, for aught we can certainly know, be true. To deny this is to assume our own infallibility*».

16 In secondo luogo: «*Secondly, though the silenced opinion be an error, it may, and very commonly does, contain a portion of truth; and since the general or prevailing opinion on any subject is rarely or never the whole truth, it is only by the collision of adverse opinions that the remainder of the truth has any chance of being supplied*».

17 Inoltre, Mill aggiunge: «*Thirdly, even if the received opinion be not only true, but the whole truth; unless it is suffered to be, and actually is, vigorously and earnestly contested, it will, by most of those who receive it, be held in the manner of a prejudice, with little comprehension or feeling of its rational grounds. And not only this, but, fourthly, the meaning of the doctrine itself will be in danger of being lost, or enfeebled, and deprived of its vital effect on the character and conduct: the dogma becoming a mere formal profession, inefficacious for good, but cumbering the ground, and preventing the growth of any real and heartfelt conviction, from reason or personal experience*».

18 *Abrams v. United States*, 250 U.S. 616 (1919).

19 S. Novick, *Honorable Justice*, Jefferson City, 1990. Tra gli altri contributi si veda Z. Szajkowsky, *Double Jeopardy - The Abrams Case of 1919*, in 23(1) *The American Jewish Archives* (1971), 6 ss.; R. Polenberg, *Fighting Faiths: The Abrams Case, the Supreme Court and Free Speech*, Ithaca, 1999; M. Ten Cate, *Speech, Truth, and Freedom: An Examination of John Stuart Mill's and Justice Oliver Wendell Holmes's Free Speech Defenses*, in 22(1) *Yale Journal of Law & Humanities* (2013), 35 ss.

20 Nella *dissenting opinion* Justice Holmes sosteneva: «*Persecution for the expression of opinions seems to me perfectly logical. If you have no doubt of your premises or your power and want a certain result with all your heart you naturally express your wishes in law and sweep away all opposition [...] But when men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas. […] The best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out*».

3 Il ruolo degli attori pubblici nella società dell'informazione.

Il moltiplicarsi dei poli d'informazione, in particolare radio, TV, giornali e da ultimo il web, insieme ad un incremento delle modalità di fruizione dei contenuti informativi ormai accessibili in qualsiasi luogo e momento tramite il proprio *device* costituiscono due importanti fattori da tenere in considerazione ai fini di comprendere la rilevanza sociale del fenomeno riguardante la diffusione di informazioni false. Come già espresso, sebbene tale rivoluzione dell'informazione abbia chiari effetti positivi per la società, tuttavia, la mole delle informazioni rende spesso complicato confrontare le notizie, lasciando spesso maggiore spazio ai contenuti più accattivanti, ben presentati o di particolare impatto sociale che riescono ad attrarre l'utente nel poco tempo dedicato ad ogni singola notizia.

Fin qui niente di nuovo. Tuttavia, il problema sorge quando l'informazione *online* contiene fatti non veritieri essendo strumentale al fine di influenzare l'opinione pubblica o perseguire interessi scarsamente trasparenti. Storicamente, lo sfruttamento dei canali di comunicazione è sempre stato funzionale ad influenzare la popolazione veicolando messaggi spesso propagandistici. Basti analizzare l'utilizzo dei canali di comunicazione nei primi anni del XX secolo per accorgersi come l'opinione pubblica si fondava su realtà costruite ad hoc dettate dalla propaganda ideologista. Tuttavia, a differenza dal passato, la quantità di informazioni condivise ogni giorno sulle piattaforme *online* non permette più al pubblico di valutare la qualità delle informazioni. Pertanto ai fini di far fronte a quelli che alcuni commentatori hanno definito come i fallimenti del mercato dell'informazione[21], non può che intervenire l'attore pubblico allo scopo di rimediare alla forte asimmetria informativa garantendo i diritti fondamentali dei cittadini. Ulteriori considerazioni che fanno propendere per un ruolo degli attori pubblici volto al contrasto alle notizie false derivano da alcune considerazioni di carattere costituzionale. In particolare, secondo Haberle[22], lo Stato costituzionale si fonda sulla ricerca della verità non in senso assoluto, ma piuttosto come obiettivo teso a stimolare il dibattito pubblico in cui attraverso il confronto tra idee è ricercata la verità, con la conseguenza che non vi sarebbe spazio per il falso.

Tuttavia, nonostante la rilevanza del fenomeno per l'intera società, non risultano tutt'ora essere presenti interventi legislativi sistematici volti a contrastare il fenomeno delle *fake news*, se non con qualche timida eccezione. Mentre in Inghilterra è stata conclusa un'inchiesta sul tema da parte della Commissione Media[23], in Germania il 30 giugno 2017 è stata approvata una legge – *Network Enforcement Act* (o *NetzDG*) – la quale, accogliendo quanto predisposto nel disegno di legge presentato dal Ministro Maas nel marzo 2017, ha introdotto alcuni obblighi per i *social network* tra i quali, in particolare, la rimozione entro 24 ore dei contenuti illegali diffusi in Germania, come quelli che incitano all'odio o alla diffamazione[24]. In particolare, tale misura legislativa, che entrerà in vigore il primo giorno di ottobre 2017, costituisce uno dei pochi esempi concreti di legislazione contro i contenuti illeciti diffusi *online* e, pertanto, merita di essere analizzata seppur senza alcuna pretesa di esaustività. Focalizzandosi in primo luogo sull'ambito di applicazione soggettivo, la suddetta legge non si rivolge a tutte le piattaforme *online*, ma soltanto ai fornitori di servizi telematici che a scopo di lucro gestiscono una piattaforma *online* che permette agli utenti di scambiare contenuti da loro scelti con altri utenti, condividerli o portarli alla conoscenza del pubblico. Dalla definizione emerge che la suddetta legge si applica soltanto ai fornitori di servizi telematici sulla base delle seguenti condizioni: a) gestione a scopo di lucro di una piattaforma *online*; b) la piattaforma permette lo scambio o la pubblicazione di contenuti scelti dagli utenti. Una volta fornita la definizione di *social network*, la legge precisa l'ambito soggettivo escludendo le piattaforme che offrono contenuti giornalistici o editoriali dalla definizione di *social network* dettata al comma 1. Tale esclusione è motivata dal fatto che i contenuti prodotti dai giornali non sono creati dagli utenti e da loro pubblicati, ma sono sottoposti ad un controllo editoriale del giornale che è pienamente responsabile dei contenuti pubblicati diversamente dal *social network*. Sono inoltre escluse le piattaforme create per permettere la comunicazione individuale o la comunicazione di contenuti specifici come le applicazioni di messaggistica istantanea. Tuttavia, il comma 2 introduce un'ulteriore restrizione all'ambito di applicazione della legge prevedendo che non rientrano nella definizione di *social network* le piattaforme con meno di 2 milioni di utenti registrati in Germania. In questo caso, salvo i *social network* particolarmente rappresentativi e utilizzati dagli utenti, non risulterà sem-

[21] Per un interessante analisi sui fallimenti del mercato delle informazioni si veda T. R. Piety, *Market Failure in the Marketplace of Ideas: Commercial Speech and the Problem that Won't Go Away*, in 41 *Loyola of Los Angeles Law Review* (2007), 181 ss.
[22] P. Haberle, *Wahrheitsprobleme im Wefassungsstaat*, tr. it. *Diritto e verità*, Torino, 2000.
[23] Le informazioni sull'inchiesta sono disponibili *online*.
[24] Il testo della legge è disponibile *online*.

plice verificare il requisito numerico richiesto dall'art. 1 comma 2 a causa di possibili fluttuazioni giornaliere o mensili di utenti registrati, privilegiando quindi *social network* senza meccanismi di registrazione al fine di non essere soggetti ai requisiti imposti da tale legge. Per quanto riguarda invece l'ambito oggettivo di applicazione della legge, l'art. 1 comma 3 definisce i casi in cui i contenuti devono ritenersi illeciti rimandando a specifiche disposizioni del codice penale, tra le quali ad esempio l'istigazione pubblica a commettere reato o la diffamazione, a patto che non sussista una giustificazione a tali condotte[25]. Una volta individuato l'ambito di applicazione della legge, l'art. 2 impone ai *social network* rientranti nella definizione fornita dall'art. 1 di produrre ogni sei mesi dei report in lingua tedesca sulla gestione dei reclami riguardanti i contenuti illeciti pubblicati sulle proprie piattaforme nel caso in cui tali piattaforme abbiano ricevuto più di cento reclami in un anno riguardanti la presenza di contenuti illeciti pubblicati sui propri spazi. Tali report, il cui contenuto è disposto dal comma 2 dell'art. 2[26], saranno pubblicati sulla gazzetta federale e sul sito web del *social network*[27] non più tardi di un mese scaduto il termine per la presentazione del suddetto report.
Venendo al punto più dibattuto, la legge specifica l'*iter* di gestione dei reclami che riguardano contenuti illeciti prevedendo l'obbligo di adottare procedure trasparenti, sempre disponibili, facilmente accessibili e riconoscibili per gli utenti. Il processo di gestione dei reclami si divide in diversi *step*. Una volta ricevuta la comunicazione da parte di un utente, il *social network* è tenuto a prenderne nota e a verificare se il contenuto riportato è illecito e, in quanto tale, suscettibile di rimozione o se l'accesso al contenuto deve essere bloccato. Dopo aver ottemperato al controllo del reclamo e del relativo contenuto, la piattaforma è tenuta a rimuovere o bloccare l'accesso al contenuto che sia manifestamente infondato entro 24 ore dalla ricezione del reclamo. Tuttavia, tale regola non si applica nel caso in cui il *social network* abbia stipulato un accordo con l'autorità competente il quale preveda un periodo più lungo per eliminare o bloccare tali contenuti. Un'altra deroga al termine giornaliero imposto sussiste quando il contenuto non è manifestamente illecito. In quest'ultimo caso, il termine è esteso a 7 giorni dalla ricezione del reclamo. Sono previste comunque delle eccezioni al termine settimanale prevedendo termini più lunghi nel caso in cui la decisione riguardi l'illiceità di contenuti che riportano allegazioni fattuali non veritiere. In tale circostanza, il *social network* può riconoscere all'utente la possibilità di rispondere al reclamo prima della decisione riguardante l'eliminazione o il blocco dell'accesso. Un'ulteriore deroga al termine settimanale si applica nel caso in cui il *social network* decida di rimettere la decisione riguardante il contenuto illecito ad un istituto di autoregolamentazione riconosciuto ai sensi della legge in questione entro 7 giorni dalla ricezione del reclamo, rimettendosi alla decisione di tale istituto.
Nel caso in cui il *social network* disponga la rimozione o il blocco del contenuto è obbligato a conservarlo a fini probatori per un periodo di 10 settimane. Infine, la piattaforma coinvolta è tenuta ad avvisare immediatamente il soggetto proponente il reclamo e l'utente riguardo qualsiasi decisione anche fornendo le ragioni.
Il meccanismo di gestione appena descritto deve essere soggetto a monitoraggio da parte del *social network* richiedendo quindi l'individuazione di risorse destinate a tal fine. Lo scopo è quello di individuare eventuali inefficienze nell'organizzazione del sistema di gestione dei reclami per poter agire prontamente apportando le necessarie modifiche. Inoltre, la legge prevede che l'organo di gestione del *social network* debba predisporre per i soggetti che gestiscono i reclami corsi di formazione e supportare programmi in lingua tedesca su base regolare non meno di una volta ogni

[25] Le condotte indicate dall'art. 1, comma 3, si riferiscono a specifiche previsioni del codice penale tra le quali la diffusione della propaganda di organizzazioni anticostituzionali (art. 86); l'uso di simboli di organizzazioni anticostituzionali (art. 86a); la preparazione di una seria azione sovversiva (art. 89); l'incitamento alla commissione di un reato contro lo Stato (art. 91); la falsificazione (art. 100a); l'istigazione pubblica a commettere atti criminali (art. 111); il disturbo della quiete pubblica (art. 126); la creazione di organizzazioni criminali e terroristiche (art. 129-129b); l'incitamento all'odio (art. 130); la diffusione di immagini violente (art. 133); la ricompensa o l'approvazione di reati (art. 140); la diffamazione nei confronti di professioni religiose, associazioni religiose o ideologiche (art. 166); la distribuzione, acquisizione e possesso di pornografia minorile (art. 184b); gli insulti (art. 185); la diffamazione (art. 186); la diffamazione intenzionale (art. 187); la minaccia di commettere un reato (art. 241); la falsificazione di elementi probatori (art. 269).

[26] Il report deve contenere: 1) osservazioni generali che indichino gli sforzi sostenuti dal provider del *social network* per eliminare attività punibili penalmente dalla piattaforma; b) descrizione dei meccanismi per inviare i reclami in merito ai contenuti illeciti e i criteri applicati ai fini di decidere se eliminare o inibire un contenuto illecito; c) numero dei reclami ricevuti nel periodo relativo al singolo report, ripartiti in base alla provenienza dei reclami (autorità amministrative o utenti) e alle ragioni del reclamo; d) organizzazione, risorse umane, esperienze specialistiche e linguistiche dell'unità responsabile per la gestione dei reclami nonché le attività di formazione e supporto; e) appartenenza ad associazioni industriali specificando se tali associazioni dispongono di un servizio di reclamo; f) numero di reclami nei quali un soggetto esterno è stato consultato ai fini della decisione; g) numero di reclami nel periodo relativo al report che hanno condotto alla cancellazione o il blocco di un contenuto, ripartiti in base alla provenienza dei reclami (autorità amministrative o utenti) e alle ragioni, nel caso in cui il caso rientri nell'ambito di applicazione dell'art. 3, comma 2, n. 3, lett. a) e, in questo caso, se il reclamo è stato inoltrato all'utente, e se la questione è stata rimessa ad un istituto di autoregolamentazione; g) periodo tra la ricezione dei reclami e la rimozione o cancellazione dei contenuti, suddivisi in base alla provenienza dei reclami (autorità amministrative o utenti) e alle ragioni del reclamo, e secondo i periodi "entro 24 ore"/ "entro 48 ore" / "entro una settimana" / "in un periodo successivo"; h) misure introdotte al fine di informare il soggetto che ha inoltrato il reclamo, e l'utente il cui contenuto è stato conservato, riguardo la decisione sul reclamo.

[27] La legge specifica che la pubblicazione di tali report sui siti web dei *social network* deve avvenire in modo da rendere tali pubblicazioni facilmente riconoscibili, direttamente accessibili e sempre disponibili.

sei mesi.
Ulteriore adempimento in capo alle piattaforme individuate dalla legge in questione attiene all'obbligo di nomina immediata da parte del *social network* di una persona incaricata di ricevere le notifiche effettuate nel territorio tedesco dandone informazione sulla propria piattaforma in modo riconoscibile e accessibile per gli utenti. Ciò al fine di poter far notificare a tale soggetto i procedimenti di cui all'art. 4 nonché i procedimenti giudiziali dinanzi le corte tedesche per diffusione di contenuti illeciti. Inoltre, al fine di permettere la ricezione delle richieste di informazioni da parte delle autorità tedesche, i *social network* dovranno nominare una persona in Germania incaricata di ricevere tali richieste, prevedendo che il soggetto in questione è obbligato a rispondere a tali richieste entro 48 ore dalla loro ricezione.
Un altro punto della legge che ha sollevato diverse critiche attiene all'ammontare delle sanzioni imposte per ogni violazione prescritta. L'art. 4 identifica i casi in cui si applica la sanzione ossia quando l'illecito è commesso da qualsiasi soggetto dolosamente o colposamente anche se non è commesso sul territorio tedesco. In particolare i casi riguardano la mancata, incorretta o intempestiva predisposizione del report, delle procedure di reclamo, del loro monitoraggio e rettifica, o la mancata offerta ai soggetti in carica della gestione delle procedure di reclamo di corsi di formazione. Inoltre, le sanzioni si applicano anche nel caso di violazione degli obblighi di nomina o di mancata risposta alla richiesta di informazioni nel caso in cui il soggetto agisca come l'incaricato a ricevere le notifiche. Le violazioni qui descritte comportano l'applicazione di sanzioni da un minimo di 500 mila euro nel caso di mancato rispetto degli obblighi di nomina fino a 5 milioni di euro negli altri casi.
Come già espresso, il dettato della legge appena descritto ha suscitato diversi dubbi riguardo l'opportunità di una misura così incisiva, consistendo principalmente nell'obbligazione per le piattaforme soggette alla suddetta legge di eliminare o bloccare i contenuti illeciti in un termine assai breve. In altre parole, alle piattaforme identificate dalla legge che operano in Germania è stato demandato il compito di decidere all'interno dell'arco di tempo di una giornata, qualora il contenuto sia manifestamente illecito, di bilanciare la libertà di manifestazione del pensiero con i diritti confliggenti di volta in volta individuati. Senza qui soffermarsi sull'opportunità o meno di assegnare tale compito ad un attore privato al di fuori di qualsiasi garanzia pubblicistica, il rischio più evidente riguarda la possibilità per le piattaforme *online* di eliminare tutti i contenuti oggetto di richiesta di cancellazione da parte degli utenti ai fini di non incorrere in sanzioni che, come sottolineato, possono raggiungere la soglia massima di 5 milioni di euro e non essere inferiori a 500 mila euro per ogni violazione. L'associazione tedesca Bitkom aveva già espresso in un articolo riportato sul la propria posizione contraria alle suddette misure, sottolineando, in particolare, come l'obbligo di cancellare i contenuti entro 24 ore non tiene conto del numero di messaggi che vengono caricati ogni giorno sul web con il rischio che le piattaforme *online* siano spinte ad introdurre meccanismi censori al fine di rispettare il dettato normativo[28].
In Francia, l'International Fact-Checking Network (IFCN), una rete che include diverse istituzioni ed enti con il fine di controllare la veridicità dei fatti, ha iniziato a collaborare con Facebook al fine di verificare le notizie sul *social network* segnalando le fonti non attendibili attraverso la dicitura "Disputed"[29]. Inoltre, il meccanismo prevede che, nel caso in cui un utente sia comunque intenzionato a condividere un contenuto recante la summenzionata dicitura, verrà visualizzato un messaggio al fine di sottolineare all'utente che il contenuto non è attendibile. Ai fini comunque di non applicare una censura che tra l'altro in questo caso sarebbe imposta da un attore privato, l'utente sarà libero di condividere il contenuto. Inoltre, gli stessi utenti saranno messi in grado di segnalare le notizie che ritengono false.
In Italia, nel febbraio 2017, è stato presentato il disegno di legge sulle *fake news* e sull'incitamento all'odio[30]. Il testo di legge reca «disposizioni per prevenire la manipolazione dell'informazione *online*, garantire la trasparenza sul web e incentivare l'alfabetizzazione mediatica». In particolare, l'art. 1 del testo stabilisce che chi pubblica o diffonde «notizie false, esagerate o tendenziose attraverso social media o siti, che non siano espressione di giornalismo *online*, è punito con l'ammenda fino a 5 mila euro». Inoltre, tale sanzione potrà essere incrementata nel caso in cui le notizie destino pubblico allarme, o rechino nocumento agli interessi pubblici, prevedendo l'ammenda fino a 5 mila euro e la reclusione non inferiore a dodici mesi.
Occorre inoltre sottolineare che il 21 novembre 2016, l'AGCOM, in occasione dell'audizione del proprio presidente dinanzi alla Commissione "Jo Cox", ha esposto la propria posizione sui temi

[28] Si v. la posizione dell'associazione Bitkom.
[29] Si v. l'articolo del *The Guardian*.
[30] Disegno di legge 2688 (ddl Gambaro). Il testo del disegno di legge è disponibile *online*.

in questione. Da un lato, secondo l'Autorità, l'industria dei media tradizionali dovrebbe impegnarsi responsabilmente, considerata la pervasività dei mezzi, a superare frasi di effetto e considerazioni iperboliche, tentando di stimolare, invece, nel pubblico una visione differente, pur mantenendo libertà di scelta e programmazione dei contenuti. A tal fine, in data 16 settembre 2016, è stata emessa la delibera n. 424/16/CONS indirizzata ai fornitori di servizi media audiovisivi e di radiofonia richiamandoli al rispetto dei principi fondamentali del sistema dei media posti a garanzia degli utenti, ponendo particolare riguardo per i soggetti a rischio di discriminazione al fine di garantire il rispetto della dignità della persona e del principio di non discriminazione. In particolare, i programmi nella diffusione di notizie devono tendere alla verità cercando di limitare connotazioni discriminatorie non pertinenti ai fini di cronaca ed evitando, espressioni d'odio, che incitino alla violenza e offendano la dignità umana. Inoltre, gli stessi fornitori sono invitati alla cautela, in particolare nel corso delle trasmissioni diffuse in diretta, al fine di evitare situazioni suscettibili di degenerazione. Tale attenzione potrà essere rispettata valutando, ad esempio, la predisposizione dell'ordine degli interventi e i possibili rischi legati a particolari soggetti o temi nelle trasmissioni.

Dall'altro lato, per quanto riguarda i *social network*, secondo l'Autorità, il crescente utilizzo dei social media ha contribuito alla creazione di un clima culturale e sociale non rispettoso della dignità umana e del principio di non discriminazione, mettendo a repentaglio categorie deboli tra le quali i minori. Riguardo a questi, l'Autorità ha fatto riferimento in particolare al cyberbullismo sempre più espressione dei sentimenti di odio e discriminazione diffusi in rete. Dalle analisi condotte dall'Autorità risulta come soprattutto la disinformazione contribuisce all'aumento di episodi di violenza o bullismo.

Nonostante il quadro preoccupante, non esiste una normativa che attribuisce all'Autorità un espresso potere di intervento al fine di contrastare tali fenomeni. Alcuni richiami possono essere individuati nella "Dichiarazione dei Diritti in Internet" del 28 luglio 2015, redatta dalla Commissione di studio per i diritti e i doveri in Internet, la quale indica tra i principi garanti della sicurezza in rete la tutela della dignità delle persone da abusi connessi a comportamenti quali l'incitamento all'odio, alla discriminazione e alla violenza. Ulteriore riferimento può essere individuato nel decreto legislativo 9 aprile 2003, n. 70, che espressamente attribuisce all'Autorità amministrativa indipendente del settore (nel caso di specie all'AGCOM) il potere di limitare la libera circolazione di un servizio della società dell'informazione proveniente da un altro Stato membro "per l'opera di prevenzione, investigazione, individuazione e perseguimento di reati, in particolare la tutela dei minori e la lotta contro l'incitamento all'odio razziale, sessuale, religioso o etnico, nonché contro la violazione della dignità umana". Inoltre, il decreto menziona la necessità di garantire la protezione dei minori e della dignità umana nei codici di condotta implementati dai fornitori di servizi *online*. In tale contesto normativo, come già espresso, l'Autorità ha istituito nel 2014 l'Osservatorio sui diritti della persona con la delibera 481/14/CONS. L'Osservatorio ha come obiettivo quello di monitorare e approfondire la conoscenza di fenomeni legati all'*hate speech* coinvolgendo i differenti portatori di interesse. Le attività dell'Osservatorio consistono nella raccolta ed elaborazione sia dei dati relativi al comportamento degli utenti rispetto a Internet e ai *social network* che delle *policy* adottate dagli operatori per la salvaguardia dei valori e degli utenti più sensibili.

Tuttavia, tali interventi come brevemente descritti non tengono conto interamente della portata del fenomeno ben più complesso, cercando, invece, di adattare frettolosamente il quadro normativo attuale sulla base delle richieste sempre più incalzanti da parte dell'opinione pubblica. Difatti, non risulta sufficiente imporre sanzioni nei confronti degli operatori privati al fine di condurli nell'alveo della legge. Né risulta opportuno aggravare le piattaforme *online* di oneri di rimozione generalisti difficilmente gestibili per risorse e competenze i quali rischierebbero di minare lo sviluppo delle piattaforme medio-piccole dotate di minor risorse nonché il proliferare di nuovi modelli di business, imponendo di conseguenza un'evidente riduzione della libertà di iniziativa economica. Sarebbe piuttosto preferibile ridefinire il paradigma di responsabilità degli Internet Service Provider (ISP) *lato sensu* visto il ruolo sempre più dirimente nel contribuire alla diffusione delle notizie false che vengono organizzante e proposte agli utenti al pari delle informazioni veritiere.

Nella società odierna limitarsi a considerare esclusivamente gli attori pubblici come minaccia alla libertà di espressione risulta oggi più che mai anacronistico. Mentre in passato il *marke place of ideas* era ritenuto *free* soltanto quando esente da ingerenze pubblicistiche, bisogna prendere atto che alcuni attori privati esercitano sempre più funzioni para-pubblicistiche, riducendo di fatto la possibilità per l'attore pubblico di poter esercitare il proprio ruolo a tutela delle libertà fondamentali[31]. Sebbene gli attori pubblici mantengano attraverso il meccanismo regolatorio un'influenza di

[31] Tra i commentatori che hanno riconosciuto il ruolo fondamentale degli attori privati nella regolamentazione si veda in particolare A. Murray, *Nodes and gravity in virtual space*, in 5(2) *Legisprudence* (2011).

rilievo sulla possibilità di controllare o censurare come *extrema ratio* i contenuti illeciti, risulta, tuttavia, opportuno notare come l'attore pubblico non è più il solo a condizionare la libertà di espressione *online*. La sempre maggiore diffusione delle tecnologie ha permesso ad alcuni attori privati di acquisire un potere regolatorio rilevante dal momento che questi determinano il funzionamento e le finalità di tali tecnologie il cui impatto sociale risulta dirimente. Utilizzando un linguaggio caro ad alcuni commentatori[32], i grandi operatori privati *online* sarebbero i nuovi *gatekeepers* ossia quei soggetti che influiscono su come gli individui scambiano le loro idee e opinioni sulla rete. In quanto programmatori delle piattaforme *online* e delle tecnologie che li governano, le scelte di tali attori privati risultano sempre più rilevanti per la libertà di espressione e, in particolare, per la formazione dell'opinione pubblica. L'attore pubblico che storicamente ha sempre ricoperto un ruolo più o meno preminente nella regolamentazione dei canali di comunicazione come la radio e la TV, oggi si trova relegato in una posizione marginale rispetto alla rete. In tale contesto, nonostante sia necessario ribadire come l'informazione sia sempre stata connotata dall'influenza editoriale, il rischio è che gli attori privati, non essendo vincolati al perseguimento di un interesse pubblico, possano liberamente influire sui limiti della libertà di espressione senza alcuna garanzia pubblicistica, determinando, ad esempio, le notizie da proporre oppure quelle da segnalare come contenuto non attendibile. Pertanto, risulta necessario che gli attori pubblici valutino le ingerenze degli attori privati che, influenzando in concreto la portata della libertà di espressione, concorrono alla formazione dell'opinione pubblica. Gli algoritmi in questo contesto svolgono un ruolo fondamentale dal momento che questi sulla base di regole prestabilite da attori privati selezionano i contenuti da mostrare agli utenti.
A tal proposito, è opportuno accostarsi ad un'analisi dell'attuale regime di responsabilità al quale sono sottoposti gli ISP in Europa.

4 Il regime di responsabilità delle piattaforme *online*.

Punto di partenza obbligato nella definizione del regime di responsabilità degli ISP in Europa è la direttiva e-Commerce del 2000[33]. In primo luogo, occorre sottolineare come la suddetta direttiva esonera i fornitori di servizi, indipendentemente dalla loro natura (*mere conduit*, prestatori di servizi di *caching* o *hosting*), dall'obbligo generale di sorveglianza sui contenuti pubblicati dagli utenti, approccio giustificato dalla necessità di evitare che le piattaforme *online* risultino oltremodo oberate da un controllo *ex ante* consistente nel monitoraggio dei contenuti caricati da parte degli utenti sulla propria piattaforma[34]. Al contrario, l'obbligo sussiste nel momento in cui ci tali piattaforme vengano a conoscenza della presenza dei contenuti illeciti su segnalazione degli utenti. In questo caso, l'esenzione di responsabilità non trova applicazione e il provider è tenuto ad adoperarsi al fine di rimuovere il contenuto.
A tale proposito, il Considerando 42 della direttiva definisce la ragione fondante delle esenzioni di responsabilità le quali sono destinate ad essere applicate nei casi in cui l'attività del prestatore sia «meramente tecnica, automatica e passiva». In altre parole, è richiesto che l'intermediario in questione non abbia conoscenza dei contenuti né svolga un ruolo di controllo o scelta di questi. Tuttavia, la direttiva prevede un regime di responsabilità per il fornitore di servizi assimilabile a quello del fornitore di contenuti nel caso in cui il primo venga a conoscenza effettiva di fatti o attività illecite commessi dagli utenti dei propri servizi[35]. In questo caso, il fornitore di servizi non potrà invocare l'esenzione da responsabilità stabilita dalla direttiva e, pertanto, si vedrà costretto ad intervenire rimuovendo il contenuto al fine di non incorrere in responsabilità.
Il quadro d'insieme rivela l'intento del legislatore europeo che mira ad evitare che il "provider passivo", ossia il fornitore che non esercita alcun controllo sui contenuti inseriti dagli utenti, sia ritenuto responsabile per illeciti ad esso non imputabili. Infatti, come già espresso, i prestatori di servizi sono equiparatati ai fornitori di contenuti responsabili solo nel caso in cui i primi siano venuti a conoscenza del carattere illecito non potendo quindi ritenersi estranei ai fatti.
In questo contesto, merita un breve accenno la giurisprudenza europea sia della Corte di Giustizia

[32] E. B. Laidlaw, *A framework for identifying Internet information gatekeepers*, in 24(3) *International Review of Law, Computers & Technology* (2010), 266 ss.; P. Drahos - C. Shearing, *Nodal governance*, in 30 *Australian Journal of Legal Philosophy* (2005), 39 ss.
[33] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»). Per un commento sulla direttiva e-Commerce si v. A. Savin, *European Internet Law*, Cheltenham, 2013.
[34] Art. 15, direttiva e-Commerce.
[35] Art. 14, direttiva e-Commerce.

sia della Corte Europea dei Diritti dell'uomo in tema di diffamazione al fine di cogliere quali sono i limiti posti alla libertà di espressione a tutela di altri diritti fondamentali. In particolare, la Corte EDU ha più volte affrontato il tema della pubblicazione dei commenti diffamatori – anche anonimi – su piattaforme *online*[36]. Il primo da sottolineare è sicuramente il caso *Delfi AS c. Estonia*, deciso dalla Grande Camera in data 16 giugno 2015[37]. La vicenda attiene alla pubblicazione di commenti anonimi in un articolo pubblicato su un portale informativo *online*, ritenuti dalla giurisprudenza estone come diffamatori, nonostante il gestore del portale avesse sostenuto la propria estraneità rispetto alle attività compiute dai propri utenti. In questo caso, il peculiare approccio rivolto alla protezione dei diritti fondamentali sanciti dalla CEDU ha spinto i giudici di Strasburgo, a ritenere che nel caso di specie non si era verificata una violazione dell'art. 10 della Convenzione e, pertanto, l'imposizione di una somma a titolo di risarcimento risultava conforme ai criteri enunciati dall'art. 10 comma 2 il quale sancisce: «L'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, alla sicurezza nazionale, all'integrità territoriale o alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario». In altre parole, nel bilanciamento tra diritti fondamentali il diritto alla reputazione ha prevalso su altri diritti fondamentali tra i quali, in primis, la libertà di manifestazione del pensiero. Tuttavia occorre sottolineare la peculiarità della vicenda al fine di non trarre una regola generale da un caso specifico. In particolare, la Corte EDU ha preso in considerazione specifici elementi al fine di sostenere la propria decisione, quali la palese diffamatorietà dei contenuti[38], l'irrisorietà della sanzione[39], il ruolo attivo della piattaforma[40], la necessità di fornire una tutela effettiva al soggetto diffamato[41]. Tali elementi hanno contribuito a ritenere non sproporzionata la sanzione consistente nella somma di 320 euro finalizzata al risarcimento del danno reputazionale subito da un soggetto, in conseguenza di 20 commenti gravemente diffamatori rimasti accessibili per circa 6 settimane. A conferma della peculiarità del suddetto caso, più recentemente nel caso *Magyar Tartalomszolgáltatók Egyesülete e Index.hu Zrt c. Ungheria* deciso il 2 febbraio 2016[42], la Corte Europea ha ritenuto che i gestori dei siti web non sono tenuti ad un obbligo di sorveglianza – e quindi non possono essere ritenuti responsabili – per i commenti pubblicati dagli utenti non sottoposti a preventiva moderazione.

Tale seconda decisione sembra collocarsi maggiormente in linea con la giurisprudenza della Corte di Giustizia, come risulta dal caso *Papasavvas* dell'11 settembre 2014[43]. In tale occasione, il ricorrente lamentava un danno subito a seguito della pubblicazione di alcuni articoli, chiaramente ritenuti da questi diffamatori, sul sito Internet di un quotidiano nazionale. Di particolare interesse risulta la quinta questione pregiudiziale sollevata dal giudice del rinvio il quale chiede se i limiti alla responsabilità previsti agli artt. da 12 a 14 della direttiva e-Commerce siano applicabili ad di una casa editrice che disponga di un sito Internet sul quale sia pubblicata la versione on line di un giornale redatto dal personale del giornale o da giornalisti indipendenti. Nel caso in questione, la Corte non ha fatto altro che confermare l'orientamento derivante dalla lettura del Considerando 42 della direttiva e-Commerce, chiarendo che i limiti di responsabilità previsti dagli artt. 12-14 della

[36] In questa sede è stata scelta l'analisi della giurisprudenza europea in tema di diffamazione visti i punti di contatto tra la diffusione di notizie diffamatorie - spesso false - e le fake news. Più in generale, tra i vari contributi sul regime di responsabilità degli ISP in Europa si veda: M. Husovec, *ECtHR rules on liability of ISPs as a restriction of freedom of speech*, in 9(2) *Journal of Intellectual Property Law & Practice* (2014), 108-109; M. Branka, *Gate Keeper or Trespasser?EU ISP Liability Regime and its Privacy Implications*, in 1 *NIR: Nordiskt immateriellt rättsskydd* (2016), 3 ss.; M. Bassini, *La rilettura giurisprudenziale della disciplina sulla responsabilità degli Internet service provider. Verso un modello di responsabilità "complessa"*, in *Federalismi.it*, 2015.

[37] CEDU, *Delfi AS c. Estonia*, ric. 64649/09 (2015).

[38] Secondo il paragrafo 140: «*The Court notes that it is not disputed that the comments posted by readers in reaction to the news article published on the applicant company's Internet news portal, as presented in the portal's commenting area, were of a clearly unlawful nature*».

[39] Secondo il paragrafo 160: «*The Court notes that the company was obliged to pay the injured person the equivalent of EUR 320 in compensation for non-pecuniary damage. It agrees with the finding of the Chamber that this sum, also taking into account the fact that the applicant company was a professional operator of one of the largest Internet news portals in Estonia, can by no means be considered disproportionate to the breach established by the domestic courts*».

[40] Secondo il paragrafo 144: «*The Court observes that the Supreme Court explicitly referred to the fact that the applicant company had integrated the comment environment into its news portal, inviting visitors to the website to complement the news with their own judgments and opinions (comments). According to the findings of the Supreme Court, in the comment environment, the applicant company actively called for comments on the news items appearing on the portal. The number of visits to the applicant company's portal depended on the number of comments; the revenue earned from advertisements published on the portal, in turn, depended on the number of visits. Thus, the Supreme Court concluded that the applicant company had an economic interest in the posting of comments. In the view of the Supreme Court, the fact that the applicant company was not the writer of the comments did not mean that it had no control over the comment environment*».

[41] Secondo il paragrafo 151: «*The Court also refers, in this context, to the Krone Verlag (no. 4) judgment, where it found that shifting the risk of the defamed person obtaining redress in defamation proceedings to the media company, which was usually in a better financial position than the defamer, was not as such a disproportionate interference with the media company's right to freedom of expression (see Krone Verlags GmbH & Co. KG v. Austria (no. 4), no. 72331/01, § 32,9 November 2006)*».

[42] CEDU, *Magyar Tartalomszolgáltatók Egyesülete e Index.hu Zrt c. Ungheria*, ric. 22947/13 (2016).

[43] CGUE, C-291/13, *Sotiris Papasavvas c. O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi, Giorgos Sertis* (2014).

suddetta direttiva non possono trovare applicazione nel caso in questione dal momento che la casa editrice, avendo pubblicato la versione *online* di un giornale, è a conoscenza delle informazioni pubblicate o esercita comunque un controllo su di esse. In altre parole, la Corte ha ricondotto la casa editrice in questione alla definizione di *content provider*, come tale, soggetto a responsabilità editoriale.
A tal punto, occorre interrogarsi sul regime di responsabilità dei *social network* che sono al centro del dibattito sulle *fake news* al fine di determinare se questi debbano essere o meno ritenuti responsabili al pari di un fornitore di contenuti. Tradizionalmente la loro responsabilità è sempre stata esclusa, da un lato, al fine di promuovere lo sviluppo dei servizi della società dell'informazione, facendo quindi prevalere la libertà di iniziativa economica e, dall'altro, dal momento che tali piattaforme non concorrono all'organizzazione dei contenuti attraverso un progetto editoriale, ma si limitano ad ospitare i contenuti che gli utenti stessi decidono di condividere spontaneamente sulla rete.

5 La responsabilità dei *social network*: attività di selezione e controllo attraverso l'utilizzo di algoritmi.

Nell'ultimo periodo il fenomeno delle *fake news* ha spinto diversi *service provider* a riconsiderare il proprio ruolo e le proprie responsabilità nella società dell'informazione, specie alla luce delle ultime vicende politiche già menzionate. Tale fenomeno ha costretto Mark Zuckerberg, CEO di Facebook, a riconsiderare il ruolo del *social network* come mera piattaforma, presentando diversi piani di azione per combattere la diffusione di notizie false. In particolare, negli ultimi mesi Facebook ha lanciato test negli Stati Uniti, Francia e Germania al fine di introdurre meccanismi efficienti di contrasto al fenomeno basati sulla segnalazione agli utenti di quelle notizie valutate come inattendibili[44]. Lo stesso ha fatto Twitter inasprendo la sua policy contro i contenuti inattendibili e segnalati dagli utenti[45].
Tale attività di controllo è possibile grazie all'impiego di algoritmi ossia di tecnologie che sulla base di un procedimento prestabilito nella loro programmazione sono in grado di analizzare un numero indefinito di dati in modo da produrre un output che nel caso di specie si tradurrebbe nella segnalazione agli utenti di una notizia falsa. In questo contesto gli algoritmi svolgono un ruolo fondamentale identificando le fonti non attendibili o più volte segnalate[46]. Proprio l'impiego di tali tecnologie potrebbe suggerire un ruolo attivo della piattaforma *online* che di fatto esercita un controllo delle notizie sul web, aprendo la via verso un nuovo modello di responsabilità dei fornitori di servizi che, al fine di controllare i propri contenuti, utilizzano tecnologie basate su processi decisionali automatizzati. Secondo il rapporto del relatore speciale delle Nazioni Unite sulla promozione e la protezione del diritto alla libertà di opinione e di espressione: «*search engine algorithms dictate what users see and in what priority, and they may be manipulated to restrict or prioritize content and that platforms deploy algorithmic predictions of user preferences and consequently guide the advertisements individuals might see, how their social media feeds are arranged and the order in which search results appear*»[47].
Il cuore della questione sta nell'interpretazione dell'art. 14 della direttiva e-Commerce, in particolare riguardo ai limiti della definizione di conoscenza e controllo dell'illiceità dei contenuti. In questo caso, sebbene ai sensi dell'art. 15 della suddetta direttiva gli Stati Membri non possano imporre un obbligo di sorveglianza o di ricerca attiva alle piattaforme, l'implementazione spontanea di meccanismi di controllo dei contenuti da parte dei *social network* comporterebbe l'impossibilità di applicare l'esenzione di responsabilità prevista dalla direttiva in quanto tali piattaforme eserciterebbero un controllo sui contenuti ospitati. In altre parole, l'utilizzo di algoritmi atti a controllare le notizie

[44] In particolare, il sito Mashable ha provato ad inserire volontariamente notizie false su Facebook al fine di capire se il meccanismo introdotto fosse funzionante. Alcuni utenti hanno evidenziato la comparsa di un nuovo messaggio quando hanno provato a condividere un articolo di un blog che riferiva una notizia chiaramente falsa (nel caso di specie si trattava di un articolo che sosteneva l'esistenza della tratta degli schiavi irlandesi). In particolare, un'icona rossa segnalava che si trattava di un contenuto che era stato segnalato da due note testate giornalistiche.

[45] L'azione di contrasto di Twitter prevede la cancellazione degli account abusivi, il miglioramento del motore di ricerca in modo da ridurre i risultati meno affidabili, l'eliminazione dei contenuti il cui contenuto è falso o non attendibile.

[46] Diversi commentatori hanno provato a identificare una definizione unitaria di algoritmo in modo da avere una comune base di partenza al fine di indagare l'impatto sociale di tali tecnologie. In primo luogo, guardando agli algoritmi come tecnologie, questi possono essere definiti come processi che esprimono un risultato in uno spazio e tempo limitato e attraverso un preciso linguaggio. Si veda in particolare T. Gillespie, *The Relevance of Algorithms*, in T. Gillespie - P. J. Boczkowski - K. A. Foot (eds.), *Media technologies: Essays on communication, materiality, and society*, Boston, 2014; N. Diakopoulos, *Algorithmic accountability: Journalistic investigation of computational power structures*, in 3(3) *Digital Journalism* (2015), 398 ss.

[47] Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/32/38), disponibile *online*.

potrebbe configurare il fattore determinante al fine di determinare in capo ai *social network* una responsabilità pari a quella dei *content provider*, simile alla responsabilità editoriale tipica dei fornitori di servizi media e audiovisivi. Tale approccio sembrerebbe giustificato dal cambiamento del ruolo dei *social network*. Vista la loro crescita e rilevanza per l'intera società risulta necessaria anche un'assunzione di responsabilità che, comunque. contemperi la necessità di garantire lo sviluppo dei servizi della società dell'informazione. Tuttavia, considerato che gli algoritmi costituiscono la base funzionale di tutte le piattaforme *online*, la suddetta responsabilità non si estenderebbe a tutti i casi di utilizzo di tali tecnologie da parte degli ISP, ma esclusivamente qualora l'impiego degli algoritmi contribuisca sostanzialmente ad un controllo attivo – ed effettivo - dei contenuti caricati dagli utenti.
Tuttavia residua il dubbio se un attore privato senza garanzie pubblicistiche possa essere chiamato a bilanciare diritti fondamentali degli individui decidendo quali contenuti mantenere, segnalare o, addirittura rimuovere, mantenendo un'esenzione da qualsiasi tipo di responsabilità. Paradossalmente, le misure di contrasto alle *fake news* in mancanza di un controllo pubblicistico potrebbero portare a censure *ex ante* di contenuti che, seppur non parzialmente veri, non possono essere considerati come totalmente falsi con un chiaro impatto sulla libertà degli utenti di esprimere le proprie posizioni. Pertanto, in questo caso, dovrebbe essere valorizzato il meccanismo previsto dall'art. 15(2) della direttiva che prevede la possibilità per gli Stati membri di obbligare i prestatori di servizi della società dell'informazione ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati. Tale meccanismo partecipativo tra pubblico e privato garantirebbe la disponibilità di un controllo pubblicistico sull'attività di bilanciamento attuata dai social network in sede di selezione e rimozione delle notizie da segnalare come false o non attendibili. Inoltre, tale cooperazione giustificherebbe l'esenzione di responsabilità soltanto per quelle piattaforme *online* che prontamente comunicheranno all'autorità pubblica i criteri di controllo dei contenuti ospitati e le tecnologie implementate a tal fine. In questo modo da un lato verrebbe garantita la libertà di iniziativa economica e, dall'altro, il diritto alla libertà di espressione sarebbe bilanciato sotto la garanzia dell'attore pubblico chiamato per sua natura a perseguire fini di interesse pubblicistico quali la repressione della circolazione di notizie false nella società.
Alla luce di tale considerazioni, fintanto che l'attore pubblico non deciderà di prendere posizione sul tema della responsabilità delle piattaforme *online*, bisognerà accettare le proposte volontarie dei vari operatori privati che, come già espresso, secondo il dettato della direttiva e-Commerce non sono tenute ad un controllo di vigilanza sui contenuti caricati dagli utenti. Anzi, proprio l'adozione spontanea di misure di controllo pervasive potrebbe esporre i *social network* ad un rischio di estensione della responsabilità nel caso in cui il controllo sul carattere veritiero delle notizie pubblicate dagli utenti venga ritenuta come attività di controllo che qualifica il fornitore dei servizi come responsabile al pari di un *content provider*.

6 Conclusioni.

Risulta, infine, chiaro come le teorie liberali alla base del *free market place of ideas* costituiscano un importante punto di partenza al fine di sancire il diritto di ciascun individuo di esprimere il proprio pensiero in modo libero. La *streaming fountain* di Milton rappresenta il cuore della libertà di espressione e il fondamento dell'attuale società democratica che, al fine di crescere e svilupparsi, non può risultare inquinata dalla falsità e dal pregiudizio. Nella società odierna, tuttavia, la libertà di espressione incontra dei limiti costituiti da altri diritti fondamentali che in quanto tali meritano di ricevere adeguata tutela. Il web costituisce un potente canale di diffusione delle manifestazioni del pensiero, ma non può di certo compromettere le garanzie costituzionali spettanti agli utilizzatori della rete. In tale quadro, l'interesse pubblico volto a garantire il rispetto dei diritti fondamentali impone un'azione positiva da parte degli attori pubblici. Non risulta necessario imporre un controllo diffuso o gravose sanzioni atte rispettivamente a censurare le posizioni espresse nel *digital market place of ideas* o a punire i trasgressori che diffondo notizie false, ma soltanto il recupero di quella funzione pubblicistica di bilanciamento dei diritti tradizionalmente spettante agli attori pubblici.
Tale percorso dovrà basarsi sul dialogo con gli attori principali del *digital market place of ideas* in modo da definire un modello che, da un lato, continui a non imporre un onere sproporzionato sui fornitori dei servizi delle informazioni al fine di garantirne il loro sviluppo e, dall'altro, assicuri la presenza dell'attore pubblico nel meccanismo di bilanciamento dei diritti. Pertanto, rafforzare il

meccanismo di comunicazione tra i *social network* e l'autorità pubblica in relazione all'attività di monitoraggio delle *fake news* sembrerebbe costituire alla luce dell'attuale quadro normativo un primo passo necessario al fine di poter instaurare una cooperazione funzionale all'eliminazione dei contenuti illeciti dalla rete.

Profili evolutivi della responsabilità in Rete: il ruolo degli *Internet Service Provider* tra prevenzione e repressione

The Evolution of the Concept of Liability on the Internet: the Role of Internet Service Providers, between Prevention and Repression

Giuseppe Miceli*
Legal Advisor in Diritto commerciale e Diritto industriale, Università di Camerino

* Le opinioni espresse sono frutto del pensiero dell'autore e non impegna la posizione dell'Amministrazione di appartenenza.

Abstract

Si analizzano ruolo e responsabilità degli attori dell'informazione digitale, nonché l'evoluzione che sta segnando il ruolo degli *ISP* e i profili di responsabilità ad essi imputabili nei confronti dei terzi lesi e danneggiati da condotte riferibili ai clienti utilizzatori del sistema, per loro tramite.
Per scongiurare il rischio di una anarchia virtuale diffusa, con l'alibi di una – apparente – abdicazione dei rimedi giuridici, è avvertita l'esigenza di individuare ed applicare efficaci strumenti di prevenzione e repressione dei reati commessi mediante Internet e delle violazioni di diritti patrimoniali e personali.
Un intervento di tipo interpretativo – prima ancora che legislativo – risulterebbe risolutorio rispetto alla definizione dei profili di responsabilità sulle piattaforme digitali, sia in termini di prevenzione che di repressione delle condotte illecite. Facendo leva sulla teoria dei nuovi diritti, deve evidenziarsi che il diritto di accesso a Internet non è – ancora – un diritto meritevole di tutela costituzionale e, quindi, deve cedere di fronte al rischio che siano compromessi diritti fondamentali, quali: l'onore, la reputazione, la sicurezza pubblica, la riservatezza, la proprietà intellettuale e la protezione dei minori.

The core of the research is based on the possible actions that should be taken to tackle fake news or hate speech and the most common types of illegal activities carried out on the web, along, with the role and responsibilities of the suppliers of information. There is the need to seize ones attention on the evolution that is marking the role of Internet Service Providers (ISP) and the profiles of liability relating to third parties that could be harmed and damaged by customers misbehaviors while using the Internet.
In order to avoid the risk of a widespread virtual anarchy, due to the alibi of an apparent abdication of legal remedies, it is necessary to identify and apply effective tools to prevent and prosecute the crimes committed on the Internet and the infringement of property and personal rights.
This research should consider the "principle requiring the legal issues linked to the Internet being regulated by applying the laws in force in similar fields and proper adjustments to the peculiarities, if needed".
This analysis is aimed at showing that an interpretative intervention rather than a legislative one can be a means to define profiles in compliance with the responsibilities of digital platforms, based on the prevention and repression of illegal conduct.

Sommario

responsabilità del provider
Internet Service Provider
modello 231
direttiva e-commerce
ISP

1 Premessa. Analisi di contesto.

Non v'è dubbio che il peculiare e caratterizzante connotato di internet, quale moltiplicatore esponenziale di opportunità di comunicazione fra una moltitudine di utenti, abbia reso la Rete un eccezionale volano per la commissione e diffusione di illeciti la cui gamma risulta notevolmente ampliata, così come il numero degli autori[1].

La grande facilità di diffusione di messaggi, immagini e filmati, la potente capacità di divulgazione di ogni altro tipo di comunicazioni unite al carattere naturalmente ubiquo di internet complicano l'opera di regolamentazione giuridica e rendono estremamente difficile individuare i soggetti responsabili[2] delle azioni illecite commesse in questo *infinito non luogo*[3]. Tant'è che non sempre le più evolute tecnologie utilizzate per gestire una rete telematica consentono di identificare realmente l'utente che si sia reso autore di una violazione[4].

La risonanza degli illeciti che vengono commessi attraverso internet e i preoccupanti effetti che ne scaturiscono rendono quanto mai urgente l'adozione di uno strumento capace di individuare i ruoli e differenziare le responsabilità di coloro che agiscono in Rete.

Gli studiosi del diritto sono impegnati nella ricerca di una formale tipizzazione delle diverse condotte che, a vario titolo, trovano configurazione in internet.

Anche tale ricerca dovrà tener conto del «principio secondo il quale le questioni giuridiche riguardanti internet devono essere regolate applicando il diritto vigente in settori analoghi, premessi, se necessari, gli opportuni adattamenti alle peculiarità della Rete»[5].

Proprio su tale principio si basa la presente analisi con la quale si mira a dimostrare che un intervento di tipo interpretativo – prima ancora che legislativo – possa risultare risolutorio rispetto alla definizione dei profili di responsabilità sulle piattaforme digitali, sia in termini di prevenzione che di repressione delle condotte illecite.

Al centro di questa riflessione sulle possibili azioni di contrasto alle più diffuse tipologie di attività illecite realizzate sul web, nonché, sul ruolo e le responsabilità degli attori dell'informazione digitale, si pone l'attenzione verso l'evoluzione che sta segnando il ruolo degli *Internet Service Provider* (ISP)[6] e i profili di responsabilità ad essi imputabili nei confronti dei terzi lesi e danneggiati da condotte riferibili ai clienti utilizzatori del sistema, per loro tramite[7].

Periodicamente – per lo più, in concomitanza con le tragiche conseguenze che scaturiscono dalla pubblicazione e diffusione *online* di video privati, come nei casi di *revenge porn* o di *cyberbullismo* – si riaccende il dibattito sull'opportunità di attribuire una responsabilità oggettiva in capo all'ISP.

In tale scenario, al fine di scongiurare il rischio di una *anarchia virtuale* diffusa, con l'alibi di una

---

[1] Si tratta dei "*reati di massa*". C.E. Paliero, *Minima non curat praetor. Ipertrofia del diritto penale e decriminalizzazione dei reati bagatellari,* Padova, 1985, 181 ss.

[2] Affermazione mutuata da T. Ballarino, *Internet nel mondo della legge*, Padova, 1998, nonché, A. Sirotti Gaudenzi, *Trattato breve di diritto della rete*, Rimini, 2001. Si tratta di una convinzione su cui saranno basate le considerazioni conclusive e le proposte risolutive sul tema della responsabilità degli ISP.

[3] Non si ritiene di poter condividere il pensiero di quanti identificano il fenomeno Internet come un "ambiente", ovvero, un luogo fisico, tanto da definirlo con l'espressione, di matrice fantascientifica, cd *cyberspace*. Parte, autorevole, della dottrina (C. Giurdanella, *Problemi di giurisdizione,* in Aa. Vv., *Internet. Nuovi problemi e questioni controverse*, Milano, 2001, 373 ss.) come pure alcuni pronunciamenti giurisprudenziali nazionali (ad es.: Trib. Firenze, 7 giugno 2001, n. 3155, consultabile in *Interlex*) in effetti, fanno riferimento a quella espressione che fu utilizzata per la prima volata da W. Gibson, nel suo *Neuromancer*, New York, 1984 descrivendo la *Rete* come un "nuovo ordinamento" caratterizzato da proprie peculiarità.

Si ritiene, piuttosto, di condividere il pensiero che nel 1996, J. Perry Barlow ha espresso nella sua *Dichiarazione di indipendenza del Cyberspazio* ovvero: «Il Cyberspazio è fatto di transazioni, di relazioni e di pensiero puro disposti come un'onda permanete nella ragnatela delle nostre comunicazioni. Il nostro è un mondo che si trova contemporaneamente dappertutto e da nessuna parte, ma non è dove vivono i nostri corpi».

[4] L'accesso alla Rete avviene mediante una procedura di login, con un nome di accesso, o username e una password. Tecnicamente, salvo i casi di navigazione segreta in Internet - il cd *dark web* - è sempre possibile identificare il nome d'accesso dell'utente che ha commesso la violazione attraverso quello che viene chiamato il log file, contenente l'identificazione dell'utente che ha effettuato il login e i tempi di accesso di ogni utente, tuttavia nulla vieta che tale nome possa essere stato in precedenza sottratto, insieme alla sua password ed utilizzato fraudolentemente da terzi al fine di evitare ogni possibile conseguenza. La stessa difficoltà di individuazione si ha quando uno stesso nome di accesso alla rete è utilizzato da più persone contemporaneamente. Analogo discorso vale per indirizzo numerico IP che viene assegnato ai computer e a tutti gli altri dispositivi connessi a Internet per identificarli e consentirgli di interagire l'uno con l'altro, rappresentando una vera e propria impronta digitale del dispositivo utilizzato.

[5] Così A. Gili, *Abuso del diritto di cronaca e diffamazione online,* disponibile *online*.

[6] In informatica e telecomunicazioni un *Internet Service Provider* (ISP), termine mutuato dalla lingua inglese, letteralmente "*fornitore di servizi Internet*", è una struttura di natura imprenditoriale e che offre agli utenti, dietro la stipulazione di un contratto commerciale di fornitura, servizi inerenti a Internet. L'ISP è assegnatario di indirizzi IP e fornisce il collegamento con la rete telematica, direttamente o tramite un provider collocato ad un livello più alto. È rilevante rappresentare che già da alcuni anni i costi del servizio di connessione sono tendenti allo zero, tanto che ai provider risulta molto più proficuo offrire sul mercato l'utilizzo di pagine web pubblicitarie e di promozione commerciale (i cd. *banner*) registrando, così, interessanti livelli di introiti economici.

[7] Altri ordinamenti hanno definito i profili di responsabilità degli ISP, tra questi: la Germania, che per prima si è dotata di un sistema fondato sulla Legge Federale del 2 luglio 1997; Gran Bretagna, che prevede la responsabilità degli ISP nei casi di diffamazione in Rete. Sul piano giurisprudenziale, si segnale che in Olanda un ISP è stato condannato per essere stato responsabile della violazione per negligenza, non avendo impedito il comportamento illecito di suoi utenti che avevano violato la normativa sul copyright (Trib. Rotterdam, 1995). In Francia con sentenza del 10 febbraio 1999, la Corte d'Appello di Parigi ha ritenuto configurata la responsabile extracontrattuale dell'ISP per il contenuto illecito presente in siti "ospitati". La sentenza dell'8 dicembre 1999 del Trib. Nanterre attribuisce responsabilità all'ISP in considerazione di un obbligo di prudenza e diligenza che grava in capo ai *Provider*. In Italia: Ordinanza Trib. Napoli, 8 agosto 1996; Trib. Catania, 25-29 giugno 2004, n. 2286; Trib. Milano, ord. 24 marzo 2011 e, ancora, sent. 9 settembre 2011, n. 10893. Ancora, una serie di pronunce della Corte di giustizia dell'Unione europea e – come se non bastasse – significative sono le Conclusioni del 26 novembre 2013, causa C-314/12, dell'Avvocato Generale.

– apparente – abdicazione dei rimedi giuridici, è avvertita l'esigenza di individuare ed applicare efficaci strumenti di prevenzione e repressione dei i reati commessi mediante internet e delle violazioni di diritti patrimoniali e personali.

2 Internet Service Provider: ruolo e funzioni.

Volendo incentrare l'attenzione sul dibattito circa l'opportunità di attribuire una responsabilità oggettiva in capo all'ISP nell'ambito di quella che è già stata definita la ricerca di una formale tipizzazione delle diverse condotte che, a vario titolo, trovano configurazione in internet, giova il riferimento alla distinzione operata dalla direttiva n. 2000/31/CE sul commercio elettronico, in ragione della capacità degli stessi ISP di immagazzinare, modificare e trasmettere una, più o meno, ampia mole di informazioni, anche in via permanente, nelle piattaforme informatiche e di garantire un'agevole condivisione di tali dati tra gli utenti[8].

Il legislatore nazionale, con la legge delega 1 marzo 2002, n. 39 e il d. lgs. 9 aprile 2003, n. 70, ha dato attuazione alla direttiva 2000/31/CE sul commercio elettronico, iniziando l'opera di armonizzazione del regime di responsabilità civile dei cd prestatori intermediari, i *provider*, nei confronti dei terzi[9].

In altre parole, il legislatore italiano, al pari di quello comunitario, applica il principio della distinzione dei *provider*, a seconda che questi svolgano funzioni di "semplice trasporto" (*mere conduit*), di "memorizzazione temporanea" (*caching*) e di "*hosting*".

A ben vedere, il d. lgs. 70/2003, si limita a riprodurre la direttiva 2000/31/CE, travasandone il contenuto nel nostro ordinamento giuridico. Nelle tre disposizioni (artt. 14, 15 e 16) corrispondenti a diversi menzionati profili di *provider*, emerge soltanto che i fornitori di servizi non sono responsabili dei contenuti per loro tramite veicolati purché non intervengano su di essi, confermando una *ratio iuris* già presente nel nostro impianto normativo.

La direttiva, inoltre, agli artt. 12, comma. 3, 13, comma 2, e 14, comma 3, con riguardo alle tre diverse attività di *provider* lascia aperta la possibilità per gli Stati membri di disporre che un organo giurisdizionale o un'autorità amministrativa ordini al prestatore di porre fine alla violazione e con riguardo alla sola attività di *hosting*, nella seconda parte dell'art. 14, comma 3, prevede la possibilità in sede di recepimento di «definire procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime».

L'assetto normativo sin qui analizzato deve essere letto con il dettato dell'art. 17, il quale esclude che il *provider* possa essere assoggettato a un generale obbligo di sorveglianza sulle informazioni che trasmette o memorizza, ovvero ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.

Tuttavia, la direttiva, all'art. 15, comma 2, prevede che gli Stati membri possano «stabilire che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati»[10].

Gli Stati membri hanno facoltà di prescrivere *standard* di diligenza a carico degli intermediari *online,* idonei a individuare in via preventiva i contenuti lesivi, ma senza che questi vadano a costituire un vero e proprio dovere di ricercarli attivamente.

Parafrasando quanto acutamente osserva Oreste Pollicino[11], è necessario distinguere in maniera adeguata il piano della responsabilità del *provider* fondata sull'esercizio, da parte dello stesso, di un'attività editoriale che lo escluderebbe dalle esenzione di responsabilità e quello della responsabilità che scaturisce dall'inerzia del *provider* quando ricorrano le condizioni per le quali l'art. 16 del d. lgs. 70/2003 sarebbe doveroso un intervento dello stesso volto alla rimozione dei contenuti.

---

[8] Gli ISP dispongono di propri *data center* e di proprie apparecchiature che consentono l'interfacciamento con la rete Internet; tuttavia, vi sono anche alcuni ISP virtuali capaci di offrire abbonamenti ai loro servizi senza possedere un'infrastruttura di Rete propria, si servono, cioè, di un altro provider cosiddetto *wholesale*, fornitore di servizi per rivenditori.

[9] La direttiva sul commercio elettronico è applicata ai settori *online*, come i servizi di informazione (giornali, riviste); pubblicità; commercio; servizi professionali (avvocati e medici); servizi finanziari e di accesso alla Rete. Non viene applicata a settori come quello tributario, ai servizi sulla privacy della società dell'informazione; attività di notai o figure professionali equivalenti che esercitano pubblici poteri e i giochi d'azzardo (inclusi lotteria e scommesse).

[10] A ciò si deve aggiungere quanto previsto dal Considerando 48, ovvero, la possibilità per gli Stati membri «di chiedere ai prestatori di servizi, che detengono informazioni fornite dai destinatari del loro servizio, di adempiere al dovere di diligenza che è ragionevole attendersi da loro ed è previsto dal diritto nazionale, al fine di individuare e prevenire taluni tipi di attività illecite». Il Considerando 48 costituisce il fondamento di un'obbligazione di mezzi e non di risultato. G. M. Riccio, *La responsabilità civile degli internet providers,* Torino, 2002, 213.

[11] O. Pollicino, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider*, in *ConsultaOnline,* 2014.

Tuttavia, anche nel primo caso, per effetto di un eventuale accertamento della natura di *hosting* non passivo, ovvero non neutro, bensì di un ruolo "attivo", si giustificherebbe l'addebito di responsabilità, proprio per non essere il *provider* del tutto estraneo alla gestione dei contenuti[12].
Ecco quindi che l'elemento significativo ai fini della configurazione di una responsabilità del *provider* è rappresentato dalla sua neutralità ma – risiede proprio qui il problema, visto che - in mancanza di un intervento legislativo chiarificatore, sarà il giudice a doversi fare carico di individuare il confine tra *hosting* attivo e *hosting* passivo[13].
Si è giunti così, a compiere talora una forzatura del dato legislativo per coniare una nuova figura per così dire "ibrida", diversa dal mero *provider* passivo, l'*hosting* cosiddetto attivo, concepito come un *provider* non neutrale nella prestazione di servizi, così da attrarne la responsabilità in concorso con gli autori degli illeciti di volta in volta contestati.
Tale circostanza, in effetti, non manca di generare profili altamente problematici proprio per l'elevato rischio di abuso connesso alla variegata platea di fruitori dei servizi offerti dagli stessi ISP.
A dirimere la questione risulterebbe utile la corretta individuazione e puntuale applicazione dei cd *standard* di diligenza previsti dalla direttiva sul commercio elettronico.

3 La funzione degli standard di diligenza.

In effetti, rispetto alla prevista facoltà riconosciuta agli Stati membri di prescrivere *standard* di diligenza a carico degli intermediari *online,* capaci di individuare in via preventiva i contenuti lesivi, ma senza che questi vadano a costituire un vero e proprio dovere di ricercarli attivamente, si ritiene auspicabile un caso particolare di messa in sicurezza delle Reti che può ravvisarsi nell'azione di stimolo per l'adozione "spontanea" da parte degli ISP di "programmi di collaborazione" e, ove non bastasse, l'onere di applicare il Modello organizzativo previsto dal d. lgs. 231/2001[14].
Come è noto, proprio in ragione della continua evoluzione degli ordinamenti giuridici, emerge, sia a livello nazionale che internazionale, una chiara apertura verso alternative forme di regolamentazione, complementari alla classica elaborazione dottrinale del *"diritto"*[15].
Tali forme alternative di elaborazione del diritto trovano configurazione nel cosiddetto *soft law*[16] che rappresenta quell'insieme di tecniche e strumenti di produzione normativa idonee a gestire e dirigere le attuali vicende statali, internazionali e comunitarie. In altre parole, tale forma di diritto è una manifestazione di *ius publicum*, quale diritto prodotto, o quanto meno indirizzato, orientato e controllato da parte delle istituzioni pubbliche dei differenti ordinamenti, anche laddove gli attori protagonisti della concreta ed effettiva elaborazione regolamentare siano soggetti di natura chiaramente privata.
Il *soft law* potrebbe trovare valida applicazione anche per ciò che attiene la corretta definizione dei profili di responsabilità degli *internet Service Provider*, per colmare l'evidenziata lacuna con l'emanazione di un Codice di regolamentazione dell'attività dei *provider* relativamente ai profili di responsabilità che ne possono scaturire.
Nel caso in cui non dovesse registrarsi una spontanea adesione a tale soluzione, si potrebbe efficacemente ricorrere ad una più incisiva richiesta di assunzione di responsabilità da parte dei *provider*, assoggettandoli all'onere di adottare ed efficacemente attuare il «Modello di organizzazione, gestione e controllo» previsto dal d. lgs. 231/2001 sulla responsabilità amministrativa degli enti.[17]
Ciò che si propone, dunque, è "vincolare" il regime autorizzatorio dei *provider* all'onere di redigere ed

[12] Come si evince da G. Cassano - A. Contaldo, *La natura giuridica e la responsabilità civile degli Internet Service Providers (*ISP*): il punto sulla giurisprudenza*, in *Corriere giuridico,* 9/2009, 1210, «Un orientamento riconosce la responsabilità del provider per l'illecito commesso anche da colui che si serva di strumenti forniti dal prestatore, richiamando l'equiparazione tra provider e direttore di giornale, o sottolineando la portata di Internet e quindi la strumentalità del sito del provider nel consolidare l'illecito, con la conseguente copertura da parte del provider riguardo l'anonimato dell'utente. Un altro orientamento nega che il provider possa essere responsabile per il semplice fatto di offrire l'accesso alla rete o lo spazio sul proprio server, dubitando dell'assimilabilità del sito internet alla testata giornalistica (Trib. di Cuneo, sez. I civ., sentenza 23 giugno 1997; Trib. Roma, sez. I civ., 4 luglio 1998, ord.)».

[13] A tal proposito, un esame delle più importanti decisioni in tema di responsabilità degli ISP - soprattutto nell'ambito di asserite violazioni del diritto d'autore, della *privacy* o di altri beni giuridicamente tutelati (l'onore e la reputazione, per esempio, nei casi di diffamazione *online*) - documenta come i giudici abbiano spesso faticato a qualificare il ruolo effettivamente esercitato dai *provider* di volta in volta interessati entro i limiti normativi che sono configurati dagli artt. 14, 15 e 16 del d. lgs. 70/2003.

[14] Decreto legislativo 8 giugno 2001, n. 231 "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300".

[15] La stessa direttiva 2000/31/CE demanda all'importanza di una autoregolamentazione.

[16] Il primo a teorizzare il concetto di *soft law* (ovvero, in Italia diritto attenuato e in Francia *droit mou*) agli inizi degli anni settanta, fu il Professor Dupuy; R.J. Dupuy, *Droit déclaratorie et droit programmatoire: de la coutume sauvage à la soft law*, in *L'élaboriation du droit international public*, Colloque de Toulouse, *Société Française de Droit International*, Paris, 1975, 132 ss.

[17] Peraltro, il catalogo dei cd reati presupposto in materia di 231 comprende già «I delitti in materia di violazione del diritto d'autore» *ex* l. 99/2009.

attuare un documento che contenga le regole e le procedure organizzative dell'ente[18] volte a prevenire la commissione dei reati specifici.[19] Nemmeno, il d. lgs. 231/2001 sancisce l'obbligatorietà riguardo alla sua adozione[20], tuttavia, l'approvazione di un Modello idoneo a prevenire i reati costituisce causa di esclusione o limitazione della responsabilità dell'ente ai sensi del d. lgs. 231/2001[21]. Ecco quindi che tale strumento costituirebbe uno *standard* di diligenza i cui effetti avrebbero riverbero rispetto a quanto si dirà nel prosieguo di questa analisi a proposito dell'auspicata applicazione del regime di responsabilità oggettiva (*ex* art. 2050 c.c.) e della conseguente inversione dell'onere della prova.
Ciò significa – volendo anticipare l'evidenza dell'effetto – che l'ISP sul quale graverebbe la responsabilità oggettiva per il danno causato suo tramite, sarebbe responsabile «se non prova di avere adottato tutte le misure idonee a evitare il danno» e – al contrario - sarebbe esente da responsabilità ove dimostrasse di avere adottato tutte le misure idonee a evitare il danno, ovvero, come testualmente recita l'art. 6 del d. lgs. 231/01, che «l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi».

4 Profili evolutivi e prospettive di contrasto.

Si deve evidenziare che prima dell'entrata in vigore del decreto legislativo che ha recepito la direttiva sul commercio elettronico, la responsabilità civile dell'*Internet Service Provider,* per gli atti pregiudizievoli compiuti dal proprio cliente, trovava fondamento e regola nell'art. 2043 c.c. che sancisce: «qualunque fatto doloso o colposo che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno». Si tratta della responsabilità extracontrattuale, ovvero, la situazione di soggezione alle conseguenze di una condotta umana illecita (attiva o omissiva) che abbia determinato in capo ad un terzo un danno ingiusto. Tuttavia, nel corso degli anni, la giurisprudenza che si è occupata di tali questioni non sembra aver assunto posizioni univoche. Secondo un iniziale orientamento giurisprudenziale, il *provider* non risultava tenuto ad accertare la liceità delle comunicazioni e dei messaggi che, per suo tramite, fossero stati trasmessi *on line*; vi sarebbe stata responsabilità solo nel caso in cui il medesimo avesse fornito, con dolo o colpa, un cosciente apporto causale, contribuendo così alla determinazione del danno, secondo quanto stabilito, in via generale, dall'art. 2043 c.c.[22].
Tale orientamento escludeva, già, la presenza di un dovere di vigilanza che imponesse al *provider* di verificare la liceità delle informazioni circolanti *on line* per suo tramite[23].
In evidente antitesi, un successivo orientamento giurisprudenziale ha ritenuto dover constatare una responsabilità oggettiva del *provider* per l'illecito contenuto delle informazioni immesse in *Rete* "per conto terzi"[24].

[18] Analogamente a quanto disposto dalla Regione Calabria che, con l. 60 del 4 dicembre 2012, ha reso obbligatoria l'adozione dei modelli di organizzazione, gestione e controllo *ex* d. lgs. 231/2001 per alcune categorie di enti.

[19] Peraltro, la gran parte di tali illeciti è già prevista tra le fattispecie di reato rilevanti in base al d. lgs. 231/2001 e s.i.

[20] Nonostante ciò, si registrano i primi esempi di "vincolo", come nel caso della la Regione Lombardia e la Regione Calabria.

[21] Si tratta della circostanza esimente prevista dal d. lgs. 231/2001, art. 6 "Soggetti in posizione apicale e modelli di organizzazione dell'ente".

[22] Prima dell'entrata in vigore del d. lgs. 9 aprile 2003, n. 70 , la responsabilità civile dell' internet service provider per gli atti pregiudizievoli compiuti dal proprio cliente trovava fondamento e regola nell'art. 2043 c.c.: «qualunque fatto doloso o colposo che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno», prevede e disciplina la fattispecie della responsabilità extracontrattuale e, cioè, la situazione di soggezione alle conseguenze di una condotta umana (attiva o omissiva) illecita che abbia determinato in capo ad un terzo un danno ingiusto. Tuttavia, la giurisprudenza che si era occupata di tale questione aveva assunto posizioni contrapposte. Da un lato talune pronunce sostenevano che il provider non potesse reputarsi tenuto ad accertare la liceità delle comunicazioni e dei messaggi che, per suo tramite, venivano trasmessi on line. La sua responsabilità era pertanto ravvisabile solo laddove il medesimo avesse fornito, con dolo o colpa, un cosciente apporto causale, contribuendo così alla determinazione del danno, secondo quanto stabilito, in via generale, dall'art. 2043 c.c.
Tale orientamento escludeva, dunque, la presenza di un dovere di vigilanza che imponesse al provider di verificare la liceità delle informazioni circolanti on line per suo tramite. In antitesi si registrava un'opposta opinione, che ipotizzava una responsabilità oggettiva del provider per l'illecito contenuto delle informazioni immesse in rete "per conto terzi". Così: Trib. Napoli, 8 agosto 1997. Ad analoga conclusione giunge il Trib. Roma, 22 marzo 1999.

[23] Tale assetto, tuttavia, iniziava a lasciare il campo a un opposto orientamento giurisprudenziale che ammetteva la configurabilità di una responsabilità oggettiva del *provider* per l'illecito contenuto delle informazioni immesse in Rete "per conto terzi". L'entrata in vigore del d. lgs. 9 aprile 2003, n. 70, coerentemente con quanto stabilito dalla direttiva 2000/31/CE, sancisce la responsabilità del *provider* sulla base del tipo di attività concretamente svolta.

[24] Il proprietario di un "sito" Internet ha obblighi precisi di vigilanza sul compimento di atti di concorrenza sleale eventualmente perpetrati attraverso la pubblicazione di messaggi pubblicitari. La colposa o dolosa inottemperanza a questi obblighi comporta la sua corresponsabilità nell'illecito concorrenziale. Trib. Napoli, 8 agosto 1997, in *Diritto e giurisprudneza,* 1997, 472 ss. nota di Catalano
Il *provider* che effettua il collegamento in rete non è tenuto ad accertarsi del contenuto illecito delle comunicazioni e dei messaggi che vengono immessi in un sito: tuttavia, sussiste la sua responsabilità per colpa se il contenuto delle dette comunicazioni da trasmettere appaia all'evidenza illecito; in questo caso, il *provider*, dando corso al collegamento concorre nel fatto illecito in quanto dà un apporto causale alla commissione dello stesso. Nella specie, il *provider* ha concorso nell'illecito consistente in un atto di concorrenza sleale per non aver rilevato, secondo l'ordinaria diligenza, l'uso di un noto acronimo da parte di un soggetto non autorizzato. Trib. Roma, 22 marzo 1999, in *Diritto dell'informazione e dell'informatica*, 2000, 66 con nota di Sammarco; *Rivista del diritto commerciale,* 2/1999, 273 ss., con nota di Visconti.

Come puntualmente osservato, «tra i fattori che hanno contribuito allo sviluppo di internet nel nostro paese, va senz'altro considerata la presenza dei c.d. *Internet Service Provider* (ISP), la cui funzione consiste appunto nel fornire agli utilizzatori l'accesso alla Rete, essendo l'interfaccia fra l'utenza e il *Network Service Provider* (NSP), che si appoggiano a loro volta agli operatori di telecomunicazioni». Gli stessi citati autori rilevano, pure, che «l'attività dell'ISP presenta le caratteristiche di una vera e propria attività commerciale»[25].

Il legislatore nazionale non ha definito un apposito regime amministrativo per i *provider* su internet, per cui il regime autorizzatorio vigente per i fornitori di servizi in materia di telecomunicazioni costituisce anche il quadro normativo di regolamentazione delle comunicazioni di dati via internet, finendo per rendere l'ISP un mero «fornitore di servizi pubblici di telecomunicazioni»[26]. Sul piano amministrativo, in virtù di tale quadro normativo, il rivenditore di servizi pubblici di telecomunicazioni (tra cui i *provider*), per poter attivare la fornitura dei servizi offerti, deve essere autorizzato dal Ministero dello Sviluppo Economico[27]. Ne consegue che per effetto della normativa in questione si è giunti ad assicurare le basi per uno statuto giuridico di tale figura che, se esercitata professionalmente, attiene ad una vera e propria attività d'impresa.

Pertanto, se è vero - com'è vero - che l'ISP svolge un ruolo fondamentale per il funzionamento di internet, è altrettanto vero che tale attività non possa non tener conto di un continuo ed equo bilanciamento tra contrapposti diritti: da una parte il diritto di accesso a internet e dall'altra l'onore, la reputazione, la sicurezza pubblica, la riservatezza, la proprietà intellettuale e la protezione dei minori. L'assenza di una previsione normativa, sia europea, sia nazionale, in relazione ad un obbligo di sorveglianza – non generale - in capo agli ISP, non ha impedito, nel tempo, pronunce giurisprudenziali circa uno specifico obbligo degli stessi[28].

Ecco perché, l'individuazione di una responsabilità in capo all'ISP e la scelta dell'*an* e del *quomodo* della responsabilità dell'ISP comportano attente e propedeutiche valutazioni per le delicate scelte di contrasto alla criminalità specifica che si potranno realizzare.

Forti del pensiero di Vittorio Frosini, condiviso anche da Aldo Loiodice, facendo leva sulla teoria dei nuovi diritti, deve evidenziarsi che il diritto di accesso a internet non è – ancora – un diritto meritevole di tutela costituzionale[29]. Dai risultati della attenta analisi compiuta dagli autorevoli autori emerge che l'art. 2 Cost. è – certamente - interpretabile come norma aperta e, come tale, consente il riconoscimento di nuovi diritti fondamentali, rispetto a quelli specificamente individuati dalla Carta costituzionale. Tuttavia, Frosini e Loiodice, mentre affermano che la libertà informatica è desumibile anche dalla definizione di alcune altre libertà[30] ed è, quindi, meritevole di tutela costituzionale tanto da essere riconosciuta come nuovo diritto costituzionale; con altrettanta convinzione sostengono che lo stesso non possa dirsi per il diritto di accesso a internet che resta privo di altri riferimenti costituzionali.

---

[25] G. Cassano - A. Contaldo, *La natura giuridica e la responsabilità civile degli Internet Service Providers (ISP): il punto sulla giurisprudenza*, cit.

[26] Secondo quanto già previsto nel d. lgs. 17 marzo 1995, n. 103 e nel d.P.R. 14 settembre 1995, n. 420, non essendovi un esplicito riferimento ai casi di fornitura di servizi telematici su Internet, l'ISP è considerato un mero "fornitore di servizi pubblici di telecomunicazioni".

[27] Sempre ai sensi del d. lgs. 17 marzo 1995, n. 103 e del d.P.R. 14 settembre 1995, n. 425.

[28] Trib. Milano, ord. 21/25 gennaio 2011 e ord. 24 marzo 2011. Secondo il Tribunale, dal momento che «l'associazione tra il nome del ricorrente e le parole 'truffa' e 'truffatore' è opera del software messo a punto appositamente e adottato da Google per ottimizzare l'accesso alla sua banca dati operando con le modalità […] volutamente individuate e prescelte per consentirne l'operatività allo scopo voluto […] non può che conseguirne la diretta addebitabilità alla società, a titolo di responsabilità extracontrattuale, degli eventuali effetti negativi che l'applicazione di tale sistema può determinare». Trib. Pinerolo, ord. 30 aprile 2012; Trib. Milano, ord. 25 marzo 2013. Precisa il giudice che «le associazioni, tuttora visibili su Autocomplete e Ricerche Correlate, ai nomi dei ricorrenti […] dei termini setta e plagio di cui gli stessi si dolgono non costituiscono una frase di senso compiuto né una manifestazione di pensiero, né dunque 'quello che Google pensa', né un pensiero, né un pensiero attribuibile a Google, ma esclusivamente il risultato delle ricerche più popolari effettuate dagli utenti, ovvero la visualizzazione dei termini ricorrenti nelle pagine web incluse tra i risultati di ricerca di una determinata *query*, entrambi resi disponibili agli utenti come strumenti di aiuto alla ricerca»; in prospettiva comparata: Corte d'Appello di Parigi, 14 dicembre 2011. Cfr.: O. Pollicino, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider,* cit. La responsabilità del *provider* si configurava alla stregua di una responsabilità soggettiva: colposa, quando il fornitore del servizio, consapevole della presenza sul sito di materiale sospetto, si astenga dall'accertarne l'illiceità e, al tempo stesso, dal rimuoverlo; dolosa, quando egli sia consapevole anche della antigiuridicità della condotta dell'utente e ometta di intervenire. I sopracitati orientamenti giurisprudenziali trovano ulteriore conferma anche in Trib. Torino, sez. I impresa, ord. 23 giugno 2015.

[29] Come ha osservato Vittorio Frosini, il cui pensiero è stato condiviso anche da Aldo Loiodice, l'art. 21 Cost. non statuisce – per esempio - un autonomo diritto di stampa o di accesso alla stessa, ma – soltanto - di stampa come *species del genus* "mezzo di diffusione", funzionale all'unico diritto testualmente previsto e tutelato, ossia quello di manifestazione del pensiero. di trasmissione del pensiero *in certam personam*, qualunque sia la "forma" prescelta per tale trasmissione. Cfr.: V. Frosini, *L'orizzonte giuridico dell'Internet*, in *Diritto dell'informazione e dell'informatica*, 2002, 275 ss.; T.E. Frosini, *Il diritto costituzionale di accesso ad Internet*, in M. Pietrangelo (a cura di), *Il diritto di accesso ad Internet*, Napoli, 2011, 32 ss.; A. Valastro, *Le garanzie di effettività del diritto di accesso ad Internet e la timidezza del legislatore italiano, ivi*, 47 ss.; A. Loiodice, *Informazione e partecipazione nella società tecnologica*, Roma-Reggio Calabria, 1974. Sul fronte opposto, si deve, tuttavia, considerare che la Legge Stanca del 9 gennaio 2004, relativa alle disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici, riconosce e tutela il diritto di ogni persona ad accedere a tutte le fonti di informazione ed ai relativi servizi, compresi quelli che si articolano attraverso gli strumenti informatici e telematici. L'art. 1 della menzionata legge fonda il diritto di accesso ad Internet sul principio di eguaglianza *ex* art. 3 della Costituzione, qualificandolo come uno strumento di realizzazione dell'eguaglianza sostanziale dei cittadini. Ma si può obiettare che Il mancato accesso alla rete di molti individui comporta l'esclusione dell'accesso ad Internet come diritto universale e consente, invece, di inquadrarlo come una libertà negativa, intesa come possibilità di utilizzare il mezzo informatico senza interferenze esterne.

[30] In particolare, la libertà di espressione, anche a mezzo Internet, consente diverse modalità e finalità di comunicazione, quindi, oltre agli artt. 15 e 21 Cost., si potrebbe fare richiamo agli artt. 19, 33, comma 1, e 34 Cost.

5 La responsabilità per l'esercizio di attività pericolose ex art. 2050 c.c.

Orbene, avendo così chiarito i termini oggetto di una inevitabile opera di bilanciamento dei contrapposti diritti in campo ed evidenziando che su un "piatto della bilancia" viene riposto il diritto di accesso, in ordine al quale gli ISP ne rivendicano il riconoscimento e la connessa tutale di rango costituzionale e, sullo stesso "piatto" si pone pure il diritto di iniziativa economica (questo si, di rango costituzionale) mentre sull'altro "piatto della bilancia" la collettività – non solo degli utenti della Rete –ripongono una serie di diritti fondamentali, tutti degni di tutela costituzionale[31], non resta che interpretare la normativa vigente e dimostrare l'applicabilità all'*Internet Service Provider* della responsabilità oggettiva *ex* art. 2050 c.c., fermo restando il dover garantire la *«assenza dell'obbligo generale di sorveglianza» ex* art. 17 del d. lgs. 70/2003.

In effetti, da una attenta lettura dell'art. 17 emerge, da un lato l'assenza di un generale obbligo di sorveglianza, dall'altro, una serie di adempimenti da parte del *provider* che consente la concretizzazione di un'attività di monitoraggio[32].

Dato che l'art. 2050 c.c. fa riferimento, oltre che alle attività pericolose tipizzate, nel codice o in leggi speciali, a quelle che, per la loro attitudine a produrre un rischio, si considerano attività pericolose atipiche e considerato che la giurisprudenza è unanime nel definire le "attività pericolose" in modo piuttosto ampio, comprendendo nella definizione non solo le attività qualificate pericolose dagli artt. 46 ss. T.U.L.P.S. o da altre leggi speciali, ma più in generale anche quelle che comportano la rilevante possibilità del verificarsi del danno per la loro stessa natura e per le caratteristiche dei mezzi usati; si vuole sostenere che nel caso di specie, l'oggettiva pericolosità emerge da una potenzialità lesiva, rilevabile attraverso dati statistici, elementi tecnici e di comune esperienza, notevolmente superiore al normale[33].

Proprio in considerazione di tale specificità, si ritiene poter sostenere l'ipotesi di incardinare l'attività svolta dall'ISP, caratterizzata da un potenziale elevato livello di pericolosità, nella fattispecie prevista e disciplinata dall'art. 2050 c.c.[34].

Incardinare l'attività dell'ISP all'interno del *genus* delle attività pericolose significa prescrivere l'adozione di condizioni di massima sicurezza e di ogni accorgimento utile a prevenire l'evento dannoso che, in tal modo, lo qualifica come inevitabile e, quindi, non in rapporto causale con l'attività stessa.

Come anticipato, si procederà – ancora una volta - in virtù del «principio secondo il quale le questioni giuridiche riguardanti Internet devono essere regolate applicando il diritto vigente in settori analoghi, premessi, se necessari, gli opportuni adattamenti alle peculiarità della Rete».

Ecco quindi che l'ipotesi prospettata trova analogia nel caso della navigazione aerea che, pur non essendo *ex se* attività pericolosa è ritenuta tale, per la sua natura e/o le caratteristiche dei mezzi adoperati, in relazione alle possibili conseguenze dannose che ne possono scaturire. In altre parole, vi è pericolosità ogni qual volta la navigazione aerea non rientri nella normalità delle condizioni previste dai piani di volo, dalle condizioni di sicurezza, dalle ordinarie condizioni atmosferiche, ovvero, nei casi in cui la stessa sia esercitata in condizioni di anormalità o di pericolo, con conseguente applicabilità della disposizione dell'art. 2050 c.c.

Ulteriore analogia è data dal trasporto marittimo, in cui le condizioni di pericolosità dipendono dalla natura del bene trasportato, materiale infiammabile o produttivo di gas esplosivi. In questo caso, a nessuno sfugge il riferimento alla natura del "bene trasportato" dal flusso telematico che denota un carattere di pericolosità nei casi in cui consista di dati falsi e calunniosi, video appartenenti alla

[31] Basti pensare a diritti quali: l'onore, la reputazione, la sicurezza pubblica, la riservatezza, la proprietà intellettuale e la protezione dei minori, il diritto di espressione e il diritto di informazione. Si tratta di tutti quei diritti di rango costituzionale che rischiano di essere lesi o, quantomeno, minacciati da condotte illecite perpetrate in rete

[32] Trib. Catania, sez. II civ., 29 giugno 2004, n. 2286.

[33] In tal senso: Cass. civ., sez. III, 6 aprile 2006, n. 8095, in *Responsabilità Civile, 7/*2006, 662 ss., con nota di Facci; Cass. civ., sez. I, 27 gennaio 2006, n. 1755; Cass. civ., sez. III, 21 ottobre 2005, n. 20359; Cass. civ., sez. III, 21 ottobre 2005, n. 20357; Cass. civ., sez. III, 27 maggio 2005, n. 11275; Cass. civ., sez. III, 15 ottobre 2004, n. 20334; Cass. civ., sez. III, 26 aprile 2004, n. 7916; Cass. pen., sez. IV, 27 maggio 2003, n. 34620; Cass. civ., sez. III, 10 febbraio 2003, n. 1954; Cass. civ., sez. III, 19 luglio 2002, n. 10551, in *Danno e Resp*., 12/2002, 1214 ss., con nota di Agnino; Cass. civ., sez. III, 5 giugno 2002, n. 8148; Cass. civ., sez. III, 29 maggio 1998, n. 5341; Cass. civ., sez. III, 2 dicembre 1997, n. 12193, in *Danno e Responsabilità*., 6/1998, 567 ss., con nota di Laghezza; Cass. civ., sez. I, 9 dicembre 1996, n. 10951; Cass. civ., sez. III, 8 novembre 1996, n. 9743; Cass. civ., sez. III, 16 febbraio 1996, n. 1192, in *Diritto dei Trasporti*, 1998, 465 ss., con nota di La Torre; Cass. civ., sez. III, 1 aprile 1995, n. 3829; Cass. civ., sez. II, 21 dicembre 1992, n. 13530; Cass. civ., sez. III, 17 dicembre 1991, n. 13564; Cass. civ., sez. III, 27 luglio 1990, n. 7571; Cass. civ., sez. III, 29 maggio 1989, n. 2584; Cass. civ., sez. II, 12 dicembre 1988, n. 6739; Cass. civ., sez. III, 11 novembre 1987, n. 8304; Cass. civ., sez. III, 15 luglio 1987, n. 6241, in *Foro Italiano*, 1988, I, con nota di Caruso; Cass. civ., sez. III, 1 luglio 1987, n. 5764; Cass. civ., sez. III, 27 febbraio 1985, n. 1733; Cass. Civ., sez. III, 27 febbraio 1984, n. 1393; Cass. civ., sez. III, 23 febbraio 1983, n. 1394; Cass. civ., sez. III, 2 febbraio 1983, n. 908; Cass. civ., sez. III, 27 gennaio 1982, n. 542; App. Genova, sez. II, 8 maggio 2006; App. Bari, sez. III, 7 aprile 2006; Trib. Gallarate, 18 marzo 2005; Trib. Busto Arsizio, 1 febbraio 2005; App. Milano, 18 maggio 2001, in *Foro Padano*, 2002, I, 205 ss., con nota di Curti; Trib. Monza, 7 febbraio 2000; Trib. Pescara, 10 luglio 1999; Trib. Milano, 5 giugno 1995; Trib. Milano, 17 novembre 1994; App. Roma, 16 gennaio 1986; App. Milano, 17 marzo 1972.

[34] L'art. 2050, c.c. recita «Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno». Si veda: S. Sica, *Il commercio elettronico. Profili giuridici*, Torino, 2001.

sfera privata, informazioni tutelate da brevetto o, ancora, opere appartenenti al diritto d'autore.
Anche il trasporto ferroviario, di per sé, non è catalogabile come attività pericolosa, ma lo diventa al verificarsi di circostanze che eccedano il normale rischio e che richiedano, quindi, l'adozione di cautele preventive[35].
Se quindi la *Rete* viene vista come una sorta di autostrada virtuale, ove le merci o i passeggeri sono le informazioni, ovvero i dati, possiamo affermare che *ex* art. 2050 c.c. il *provider* – al pari del vettore – abbia l'obbligo di adottare ogni possibile precauzione e cautela idonea ad evitare l'evento dannoso.
Stesso discorso vale anche nel caso in cui il servizio fornito dal *provider* sia utilizzato da terzi, in forma attiva, mediante il cosiddetto *uploading* e *downloading.* In questi casi caricare o scaricare contenuti digitali può essere paragonato, ad esempio, alle attività di carico e scarico merci che si svolgono in ambito portuale. È evidente che differente potrà essere la natura danno che ne potrà scaturire ma, altrettanto evidente è che, in ogni caso il bene giuridico protetto assume rilievo costituzionale[36] e che, per ciò, anche in tale contesto le Autorità portuali – dunque, analogamente, gli ISP - al fine di garantire la sicurezza delle operazioni, debbano adottare ogni idonea misura per evitare eventi pericolosi.
Gli esempi di attività alle quali si applica quanto disposto dall'art. 2050 c.c. sono numerosi[37] e sono conseguenza di provvedimenti giurisprudenziali[38].
Si ritiene che l'ISP nell'offrire i servizi di accesso alla *Rete* ed, in generale, di trasferimento di *file* multimediali svolga un'attività pericolosa rientrante nella vasta casistica che nel tempo la giurisprudenza consolidata ha individuato e per la quale si configura la responsabilità ai sensi dell'art. 2050.
Ove non bastasse, per dirimere eventuali divergenze interpretative circa la plausibilità di tale tesi, giova il parallelismo con le norme che disciplinano il trattamento dei dati personali contenute nel d. lgs. 30 giugno 2003, n. 196. In particolare, l'art. 15, comma 1, del menzionato Codice della privacy sancisce che: «chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile»[39].
Parte della dottrina sostiene che il legislatore abbia inteso, così, qualificare il trattamento dei dati personali, *ipso iure,* in termini di attività pericolosa.[40] In effetti, è possibile considerare pericolosa l'attività di trattamento dei dati personali per sua natura, ovvero, «in relazione al rischio che essa presenta di ledere i diritti fondamentali dell'interessato»[41], considerando le finalità della legge, consistenti «nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale». Ecco quindi che se il rischio tipico dell'attività di trattamento di dati personali è quello di ledere posizioni particolari e qualificate, dell'interessato, rischio che sussiste anche al di fuori dell'ipotesi di trattamento concernente dati sensibili, prende corpo il parallelismo con l'attività svolta dagli ISP[42].
Il rinvio all'art. 2050 c.c. si dovrà collegare all'applicabilità del regime relativo alla prova liberatoria prevista in materia di attività pericolose.[43]
In tal senso, l'estensione dell'applicabilità dell'art. 2050 c.c. all'attività degli ISP comporterebbe l'inversione dell'onere probatorio che opera solo in relazione alla prova dell'elemento soggettivo della colpevolezza; a quel punto, il preteso responsabile (ISP) dovrà dimostrare di avere adottato ogni cautela idonea ad evitare l'evento dannoso, mentre, permarrebbe sull'attore (danneggiato) l'onere

[35] Cfr. Cass. civ., sez. III, 1 aprile 1995, n. 3829.
[36] Nel caso di carico e scarico merci il bene giuridico che si intende tutelare è la salute e la vita dell'individuo mentre nel caso del carico e scarico di file o dati, il bene giuridico protetto è la dignità, la privacy, la reputazione, la proprietà intellettuale dell'individuo che potrà – anche in questi casi – essere vittima degli effetti di un'attività pericolosa.
[37] Ad esempio, anche nel caso della raccolta di gas in bombola, qualora non vengano effettuate corrette operazioni di bonifica, si configura a carico del distributore, ai sensi dell'art. 2050 c.c., la responsabilità per il danno causato dallo scoppio di una bombola consegnata ad un terzo. Così Cass. civ., sez. III, 13 gennaio 1981, n. 294.
[38] La giurisprudenza ha giudicato la fangoterapia come attività pericolosa in considerazione della «frequenza con cui verificano degli incidenti ai clienti che utilizzano impianti»: Trib. Perugia, 04 ottobre 1991; lo spettacolo di un gruppo di sbandieratori è considerato attività pericolosa (Cass. civ., sez. III, 2 dicembre 1997, n. 12193); anche l'attività di giostraio (App. Cagliari, 26 febbraio 2000) di gestione dei parchi divertimento (Cass. civ., sez. III, 27 luglio 1990, n. 7571), l'attività di pastificazione, per i mezzi impiegati (Cass. civ., sez. III, 5 giugno 2002, n. 8148), l'insegnamento delle tecniche per il conseguimento del titolo di guida alpina (Trib. Verbania, 17 febbraio 1994, in *Rivista di diritto sportivo*, 1999, 545 ss., con nota di Lanotte) e l'attività di caccia, per la quale è obbligatoria l'assicurazione per responsabilità civile (l. 11 febbraio 1992, n. 157).
[39] L'art. 15 del Codice Privacy disciplina il risarcimento del danno che precedentemente era disciplinato da due distinte norme: il danno patrimoniale dall'art. 18, quello non patrimoniale dall'art. 29 comma 9.
[40] In tal senso: V. Zeno-Zencovich, *Commentario alla legge 31 dicembre 1996, n. 675*, Padova, 1997; P. Ziviz, *Trattamento dei dati personali e responsabilità civile: il regime previsto dalla l. 675/96*, in *Responsabilità civile*, 1997, 1300 ss.
[41] *Ibidem.*
[42] La disciplina di cui all'art. 2050 c.c. risulterebbe applicabile solo in caso di lesione di diritti fondamentali dell'interessato e non per eventuali altri pregiudizi che ricadrebbero, invece, sotto la disciplina dell'art. 2043 c.c.
[43] Condividendo tale soluzione, si giunge a considerare il regime della prova liberatoria *ex* art. 2050 c.c. sempre applicabile, anche quindi se il danno non sia collegato alla lesione di un diritto fondamentale. M. Granieri, *Una proposta di lettura sulla tutela risarcitoria nella vicenda del trattamento di dati personali*, in *Danno e responsabilità,* 3/1998, 222; G. Visintini, *Trattato breve della responsabilità civile*, Padova, 1999, 404. In questo senso anche Trib. Orvieto 23 novembre 2002, in *Diritto dell'informazione e dell'informatica*, 2/2003, 337 ss.

di provare il nesso causale tra condotta ed evento lesivo.
In virtù di tale linea interpretativa, l'ISP sarebbe sollevato da responsabilità nel caso in cui riuscisse a dimostrare la mancanza di colpa e di aver agito con prudenza, diligenza e perizia, ovvero, di aver applicato lo standard di diligenza che – come si sostiene in questa analisi – sarebbe rappresentato, ai sensi dell'art. 6 del d. lgs. 231/2001, dall'aver «adottato ed efficacemente attuato [...] modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi».
L'analisi e la valutazione - sin qui proposta - dei mezzi di prevenzione e repressione applicabili alle condotte illecite che si realizzano in Rete, dimostra che l'abdicazione dei rimedi giuridici è solo apparente e che – evidentemente - ove non trovasse riscontro l'iniziativa dei *Provider* volta all'autoregolamentazione, vi sarebbero già i presupposti per l'applicazione di una tutela che, in *extrema ratio*, potrebbe giungere a rivestire carattere penale. Ciò che si vuole rilevare è che - come ha autorevolmente dimostrato Antolisei - l'illecito civile costituisce il c.d. "delitto nano" che identifica una condotta illecita priva di una sanzione penale.[44]
L'illecito civile e l'illecito penale sorgono, storicamente, per il conseguimento di distinti obiettivi: in relazione all'illecito civile, si evidenzia la volontà dell'ordinamento di assicurare – attraverso il perseguimento dell'illecito civile, stesso – la riparazione complessiva del danno subito da interessi privati; rispetto all'illecito penale vengono, invece, perseguite quelle violazioni dell'ordine generale di gravità tale da richiedere l'intervento statale per la punizione del colpevole.[45]
Pur operando in settori differenti, ambito civile e ambito penale, i due istituti condividono la struttura tripartita[46] che li caratterizza: entrambi possono esser, infatti, ontologicamente scomposti in fatto materiale (od oggettivo: nel diritto penale, il c.d. fatto tipico), antigiuridicità e colpevolezza[47].
Pertanto un intervento da parte del legislatore potrebbe spostare la competenza sul piano penale e l'accertamento dei profili di responsabilità degli ISP a favore del rito penale.
Si tratterebbe di attribuire rilievo penale alla fattispecie di illecito oggettivamente imputabile all'ISP che non abbia fornito la prova liberatoria rispetto all'autonoma ipotesi di reato colposo, strutturata in forma omissiva, che troverebbe così disciplina analoga a quella che l'art. 57, al direttore responsabile di stampa periodica.

[44] Come sostiene Antolisei «Il fallimento delle teorie che sono state enunciate per distinguere il torto penale da quello civile, induce a concludere che una diversità sostanziale non esiste. La distinzione è puramente estrinseca e legale: il reato è il torto sanzionato mediante la pena; l'illecito civile è quello che ha per conseguenza le sanzioni civili (risarcimento, restituzioni, ecc.). Insomma, è la natura della *sancito juris* quella che consente di stabilire se ci troviamo di fronte all'una o all'altra specie di torto. Ciò non significa che la distinzione dipenda esclusivamente dall'arbitrio del legislatore. La scelta della sanzione, infatti, non avviene per puro capriccio, ma in base al criterio che più sopra abbiamo enunciato: la pena, essendo una sanzione onerosa anche per la comunità sociale, non viene adottata, se non quando i reggitori dello Stato ritengono che non se ne possa fare a meno; mentre, come già osservato, rispetto al risarcimento del danno essa presenta i caratteri della personalità, della necessaria determinatezza del precetto e della riserva di legge». F. Antolisei, *Manuale di diritto penale. Parte generale,* Milano, 2000, 98.
[45] Parafrasando, R. Mazzon, *La Responsabilità Civile - Responsabilità oggettiva e semioggetiva*, Torino, 2012, 2.
[46] «*La teoria tripartita succede storicamente alla teoria bipartita classica. Sviluppatasi in Germania all'inizio del secolo, fu recepita in Italia negli anni trenta (soprattutto ad opera di G.* Delitalia). Essa distingue nel reato tre componenti fondamentali: il fatto tipico, l'antigiuridicità obiettiva e la colpevolezza»: così T. Padovani, *Diritto Penale*, Milano, 2006.
[47] «Modernamente si usa distinguere nell'analisi dell'atto illecito il fatto materiale, l'antigiuridicità e la colpevolezza…»*: Ibidem.*

Diritto all'oblio, verità, design tecnologico: una prospettiva di ricerca

Right to Be Forgotten, Truth and Technological Design

Stefano Leucci
Fellow del Nexa Center for Internet & Society

Abstract

Come cambia il concetto di memoria nell'ambiente digitale? Quali forme e contorni presenta il nuovo diritto all'oblio dopo il caso *Google Spain* e il nuovo Regolamento europeo sulla protezione dei dati personali? Quanto pesa la veridicità o la falsità di una fonte informativa sul bilanciamento necessario al *de-listing* dagli indici di un motore di ricerca? Gli stessi algoritmi che contribuiscono ad invadere sempre più la nostra sfera privata possono essere utilizzati anche quale rimedio alla loro stessa invasività?

Questi sono i principali quesiti di un possibile percorso di ricerca che il contributo mira a disegnare. Domande non semplici, che necessitano dell'unione trans-disciplinare di intelligenze diverse e complesse. Il punto di partenza è l'analisi del caso *Google Spain*, in cui la Corte di giustizia dell'Unione europea ha definito una nuova forma di diritto all'oblio, sviscerandone i meccanismi, i contenuti e i pesi da sistemare sulla complessa bilancia della giustizia. La precisazione degli aspetti legali ed etici precede la traduzione degli stessi in ambiente digitale sotto forma di requisiti e scelte operate direttamente dall'utente. Successivamente, la tensione tra i concetti di veridicità dell'informazione ("esattezza" del dato personale) e i principi di *Privacy by Design* e by *Default* - previsti al nuovo Regolamento Europeo sulla protezione dei dati personali - permettono di disegnare un possibile cammino di studio ed approfondimento da cui potrebbero emergere risposte ai quesiti sopra rappresentati, utili a rendere maggiormente efficaci i sofisticati meccanismi giuridici introdotti dall'Unione Europea. Rimane fisso un solo elemento: la nuova legge del memorizzare e del dimenticare è l'algoritmo. Spetta a noi conoscerlo e governarlo, prevedendo sempre uno spazio di decisione umana nei giudizi di bilanciamento necessari a fronte della pluralità di interessi che insistono nell'ambiente digitale.

How does the concept of memory change in the digital environment? What shapes and contours presents the new right to be forgotten after the case of *Google Spain* and the new European Regulation on the protection of personal data? How important are truth and falsehood of an information source on the balancing act required for de-listing a link from indexes of a search engine? May the same algorithms that contribute to invade our private sphere also be used as a remedy to their own invasiveness?

These are the main questions of a possible research path that this paper aims to draw. Questions are not simple, and they require a trans-disciplinary approach. The starting point of this paper is the analysis of the *Google Spain* case, where the European Court of Justice has reshaped the right to be forgotten, setting up new mechanisms, contents and weights that need to be carefully balanced. The clarification of the legal and ethical aspects precedes the translation of them in the form of requirements and user-made choices. Subsequently, the tension between the concepts of truthfulness of information ("accuracy" of personal data) and the principles of Privacy by Design and by Default - as stated by the new European Regulation on the protection of personal data - allow to draw a possible path of investigation. The final aim is to find answers to the questions asked above, increasing the effectiveness of the sophisticated legal mechanisms introduced by the upcoming General Data Protection Regulation. Only one element remain fixed: algorithm is the new law of our digital memory. Our responsibility is to govern its intelligence, safeguarding spaces for human decisions for balancing different interests that insist in the digital environment.

Sommario

diritto all'oblio
design
esattezza
intelligenza artificiale
trasparenza algoritmica

1 Memoria e motori di ricerca

Dimenticare è «perdere la memoria di qualcosa», ricorda il Sabatini-Colletti. Il noto dizionario è solo uno dei tanti strumenti che l'umanità ha prodotto nel corso dei secoli per supplire a quel misterioso atto mentale volto a rimuovere inconsciamente fatti, pensieri e valutazioni che, in uno spazio temporale variabile, non consideriamo più utili. Biblioteche e archivi da sempre sopperiscono alla volatilità della nostra memoria, costruendo quella conoscenza collettiva poi custodita e catalogata dai "sacerdoti dell'informazione" che erano e sono archivisti e bibliotecari.
Ma quando le informazioni che raccogliamo ed accumuliamo nella quotidianità riguardano persone fisiche, l'impatto sulla reputazione di queste è immediato e persistente nel tempo, e può generare pesante pregiudizio. Dimenticare permette, dunque, di "ripulire" la reputazione delle persone da fatti - veri, verificati o anche totalmente falsi - che potrebbero comportare detrimento. In altre parole, dimenticare corrisponde a riabilitare la persona alla piena dignità[1]. Ma se dimenticare è fatto mentale, e dunque difficilmente controllabile in quanto umano, inconscio ed inconsapevole, cosa succede a sostituire le sinapsi o gli strumenti cartacei un con bit e hardware?
"*Internet never forgets*", recita un adagio ad oggi molto in voga. Effettivamente, la Rete è stata progettata in modo entropico[2]. Ciò significa che l'informazione molecolare collegata in conoscenza collettiva può solo aumentare, e le operazioni per cancellare (de-collegare) un'evidenza sono molto costose e faticose, a volte del tutto inutili. La differenza tra biblioteche e internet risiede nell'automazione: la faticosa attività degli archivisti è stata lentamente riprodotta[3] e poi interamente sostituita dai *crawler* dei motori di ricerca che scandagliano il web senza sosta, organizzando e catalogando quelle molecole informative di cui è composto. Dunque, i motori di ricerca diventano meta-strumenti della conoscenza digitale, misteriosi intermediari dell'informazione, con la capacità di mostrare le evidenze più appropriate ogni qual volta una parola è inserita nel campo di ricerca. E quando quella parola corrisponde al nome proprio di una persona, tutti i siti web e i documenti in cui quel nome è contenuto appaiono sullo schermo in ordine metodico.
Come ricorda elegantemente il prof. Solove[4], il vero problema non è ciò che riveliamo di noi in rete, più o meno consapevolmente. I rischi più grandi per la nostra *privacy* «derivano da quello che rivelano pubblicamente di noi i nostri amici e i nostri nemici, coniugi e amanti, impiegati e datori di lavoro, professori e studenti». Piccoli dettagli insignificanti della nostra vita *online* si uniscono costruendo profili onnicomprensivi del nostro essere ed avere. La peculiarità dei nostri tempi è poter sopperire alla frammentarietà dell'informazione tramite l'immenso potere di aggregazione degli algoritmi di ricerca, sempre più performanti e sempre più raffinati.
Ma quanto possiamo fidarci di questi "aggregati informativi" composti in maniera automatica da un – pur raffinatissimo – motore di ricerca? Come possiamo controllarne il funzionamento e governarne le funzionalità a nostro favore - e non a scapito - dei nostri diritti più intimi?

2 Caso *Google Spain*: il nuovo diritto all'oblio

Può capitare che fatti lesivi della dignità "tornino a galla" molto tempo dopo, in seguito ad una semplice ricerca *online*. Ed è proprio questo che è successo al signor Costeja González, che per proteggere la sua *privacy* ha adito prima l'*Agencia Española de Protecciòn de Datos* e poi la Corte di

[1] L. Floridi, *On Human Dignity as a Foundation for the Right to Privacy. Philosophy and Technology*, Berlino, 2016.
[2] Come il padre del web semantico ricordava in uno dei suoi articoli più importanti, un'area particolarmente problematica dell'aggregazione di dati provenienti da diverse sorgenti riguarda proprio la tutela della privacy. Il mondo accademico lavora ancora oggi alla ricerca di proposte sostenibili alla soluzione di questo problema, oramai assimilato ad un paradosso. Si veda C. Bizer - T. Heath - T. Berners-Lee, *Linked data: the story so far*, in *Special issue on linked data. International Journal on Semantic Web and Information Systems*, 2009.
[3] La ricerca riassunta in questo articolo ha reso possibile il cambiamento di paradigma nella catalogazione automatica delle informazioni. Le tecnologie derivate hanno permesso la nascita del più importante motore di ricerca ad oggi esistente (Google): S. Brin - L. Page, The anatomy of a large-scale hypertextual Web search engine, in Computer Networks and ISDN Systems archive, 30/1998.
[4] D. Solove, *The future of reputation*, New Haven, 2007.

giustizia dell'Unione Europea[5], ri-aprendo un enorme dibattito[6] destinato ad avere nuove e continue ripercussioni sul modo e sulle precauzioni con cui gestiamo (e vediamo gestite) le informazioni che ci riguardano, diffuse nell'ambiente digitale.

Infatti, introducendo il proprio nome in *Google*, venivano mostrate notizie pubblicate due anni prima sul quotidiano *La Vanguardia*, che narravano di una vendita all'asta di immobili connessa ad un pignoramento effettuato per la riscossione coattiva di crediti previdenziali. Il sig. Costeja González affermava che «il pignoramento, che era stato effettuato nei suoi confronti, era stato interamente definito da svariati anni e che la menzione dello stesso era ormai priva di qualsiasi rilevanza»[7].

Evidente è il rischio di reperire queste informazioni. Si pensi a un istituto bancario che, nella millimetrica cautela tipica delle decisioni in tema di benefici finanziari, decida di non concedere un prestito proprio a causa dell'evidente insolvenza, semplicemente immettendo il nome del possibile futuro debitore. Immaginiamo, ancora, la lesività di queste informazioni se unite a dettagli lavorativi, orientamenti sessuali o politici del soggetto. Come rilevato anche dalla sentenza in commento, da una semplice ricerca del nome di una persona, è possibile ricostruire «una visione complessiva strutturata delle informazioni relative a questa persona reperibili su internet, che consente di stabilire un profilo più o meno dettagliato di quest'ultima».[8]

Non si dubita, in questo caso, dell'applicabilità della direttiva 95/46[9], nonostante si tratti esclusivamente di operazioni atte a non modificare, bensì ad organizzare e aggregare dati pubblicati precedentemente. Come afferma graniticamente l'estensore, non considerare trattamento di dati personali tutti quei trattamenti ulteriori e successivi di dati personali già diffusi in rete «priverebbe in larga parte del suo significato tale direttiva»[10]. Il trattamento in questione «si distingue da e si aggiunge a»[11] quello effettuato dagli editori nel web, e proprio per questo è il gestore del motore di ricerca - in qualità di responsabile del trattamento - a dover assicurare il rispetto dei dogmi della normativa in materia di protezione dei dati personali affinché le garanzie previste da quest'ultima possano sviluppare pienamente i loro effetti. Considerando la ricerca di una tutela efficace e completa come faro-guida di tutta l'applicazione della normativa in materia, non sarebbe possibile raggiungere pienamente questi risultati se si dovessero preventivamente rimuovere le informazioni che riguardano la persona interessata dai siti web degli editori.

Oltretutto, nemmeno si dubiterebbe dell'applicabilità agli editori web delle maggiori deroghe previste a tutela della libertà d'espressione. L'art. 9 della direttiva[12] sposta infatti il peso verso l'interesse pubblico alla conoscenza, richiedendo attenti bilanciamenti tra il diritto alla vita privata e le norme sulla libertà d'espressione[13]. Nel caso di specie, è necessario tenere in considerazione la maggior ingerenza nel diritto fondamentale al rispetto della vita privata della persona interessata nel caso dell'inclusione all'interno dell'elenco dei risultati a fronte della semplice pubblicazione di una pagina web. Come spiega la sentenza, «l'inclusione nell'elenco dei risultati facilita notevolmente l'accessibilità di tali informazione a qualsiasi utente di internet che effettui una ricerca sulla persona di cui trattasi»[14].

Con questi presupposti è chiaro l'arduo compito del gestore del motore di ricerca, a cui spetta garantire che i dati personali siano trattati lecitamente, per finalità determinate esplicite e legittime, che siano adeguati pertinenti e non eccedenti rispetto alle suddette finalità, che siano esatti ed

[5] Il presente contributo mira ad analizzare il solo piano giuridico e giurisdizionale europeo. Non verranno, perciò, commentate normative e pronunce nazionali, se non marginalmente.

[6] Il tema è, infatti, da molto tempo dibattuto nelle corti nazionali di tutta Europa, ma anche in ambiti istituzionali e accademici. In Italia, oltre ad alcuni precedenti provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali, l'orientamento che ha preceduto la Corte europea è stato espresso in Cass. civ., sez. III,, sent. 5525/2012. Il caso di specie presenta solo alcuni tratti di similitudine con il giudicato della Corte europea, trattandosi della richiesta di blocco del trattamento dei dati personali rivolto all'archivio storico digitale di una nota testata giornalistica. A commento di questa sentenza, si veda: A. Mantelero, *Right to be forgotten ed archivi storici dei giornali: la Cassazione travisa il diritto all'oblio*, in *La nuova giurisprudenza civile commentata*, 28/2012, 543 ss. Per una vista comparativa si veda O. Pollicino – M. Bassini, *Diritto all'oblio: i più recenti spunti ricostruttivi nella dimensione comparata ed europea*, in F. Pizzetti (a cura di), *Il caso del diritto all'oblio*, Torino, 2013, 185 ss. Per un approfondimento storico si veda invece G. Zanfir, *Tracing the Right to be Forgotten in the Short History of Data Protection Law: the "New Clothes" of an Old Right*, in *Computers, Privacy and Data Protection Conference*, 2014.

[7] Paragrafo 15, Corte di giustizia dell'Unione Europea, Grande Camera, Causa C-131/12, da subito ribattezzata "Sentenza *Google Spain*".

[8] Paragrafo 37, sentenza *Google Spain*.

[9] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Le nuove tensioni a fronte del rinnovato contesto giuridico che segue l'emanazione del Regolamento Europeo sulla Protezione dei Dati (Regolamento (UE) 2016/679) verranno esaminate nei paragrafi successivi.

[10] Paragrafo 30, sentenza *Google Spain*.

[11] Paragrafo 35, sentenza *Google Spain*.

[12] Art. 9, direttiva 95/46/CE, rubricato "Trattamento di dati personali e libertà d'espressione", che recita quanto segue: «Gli Stati membri prevedono, per il trattamento di dati personali effettuato esclusivamente a scopi giornalistici o di espressione artistica o letteraria, le esenzioni o le deroghe alle disposizioni del presente capo e dei capi IV e VI solo qualora si rivelino necessarie per conciliare il diritto alla vita privata con le norme sulla libertà d'espressione».

[13] Si veda, sul tema, l'Allegato A1 (Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica) al decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).

[14] Paragrafo 87, sentenza *Google Spain*.

aggiornati e che siano conservati per un arco di tempo non superiore a quello necessario al conseguimento delle suddette finalità. Proprio le informazioni riguardanti il sig. Costeja González, indicizzate e diffuse dal motore di ricerca, sono state considerate non più pertinenti, ovvero eccessive in rapporto alle finalità del trattamento in questione. Vari sono i pesi che devono essere sistemati sulla complessa bilancia della giustizia. Di primaria importanza sono gli articoli 7[15] e 8[16] della Carta dei diritti fondamentali dell'Unione europea, che «prevalgono non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse del pubblico a trovare l'informazione suddetta[17] in occasione di una ricerca concernente il nome di questa persona»[18]. È necessario però precisare il parametro fondamentale di questa decisione: il «ruolo ricoperto da tale persona nella vita pubblica»[19], che potrebbe anche giustificare l'ingerenza dell'interesse preponderante del pubblico nei suoi diritti fondamentali, nel pieno rispetto del principio di proporzionalità[20]. Il signor Costeja González - comune cittadino senza alcuna particolare rilevanza pubblica né sociale - ha così potuto attivare le tutele previste dalla Direttiva: la possibilità di operare rettifica, cancellazione o congelamento dei dati che lo riguardano[21], e il diritto di opporsi al trattamento di tali dati[22].

3 Il "peso" della verità

Ad oggi, dopo l'assorbimento dei nuovi meccanismi operativi del diritto all'oblio da parte delle Corti nazionali e nel nuovo Regolamento Generale sulla Protezione dei Dati[23], non tanto è poi cambiato. Importanti precisazioni sono state recentemente stilate da un secondo intervento della Corte di Giustizia dell'Unione Europea[24] (ribattezzato "caso *Manni*") che ha permesso di svelare i rapporti tra i tempi di conservazione e di cancellazione dei dati. Nonostante il caso di specie sia lontano dalle tipicità dei trattamenti operati dai motori di ricerca, quest'ultima pronuncia ha arricchito ancor di più la tesi per cui la decisione relativa alla cancellazione dei dati personali debba esser guidata da un'attenta «valutazione da compiersi caso per caso»[25] che tenga conto degli elementi contestuali e degli specifici interessi di terzi potenzialmente coinvolti.
Ma la domanda che appare rilevante in questa sede è la seguente: quanto incide la veridicità del fatto sul giudizio di bilanciamento utile all'applicazione del diritto all'oblio? Veridicità che - collocata nelle categorie concettuali del diritto alla *privacy* - si avvicina al concetto di "esattezza" del dato personale quale principio fondativo di tutta la disciplina[26].

[15] L'art. 7 della Carta dei Diritti Fondamentali dell'Unione Europea, rubricato "Rispetto della vita privata e della vita familiare", recita quanto segue: «Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni».

[16] L'art. 8 della medesima Carta, rubricato "Protezione dei dati di carattere personale", recita quanto segue: «Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

[17] I Garanti europei erano già giunti a conclusioni simili nel seguente documento Article 29 Data Protection Woking Party, *Opinion on data protection issues related to search engines*, 00737/EN, WP148, Bruxelles, adottato il 4 aprile 2008.

[18] Paragrafo 97, sentenza *Google Spain*.

[19] *Ibidem*.

[20] Sul piano giuridico italiano, alcuni autorevoli autori hanno commentato l'importanza di questo orientamento, confrontandolo con gli orientamenti maggioritari nazionali. Tra gli altri, si veda: G. Finocchiaro, *Il diritto all'oblio nel quadro dei diritti alla personalità*, in *Il Diritto dell'Informazione e dell'Informatica*, 4-5/2014, 591 ss.; T.E. Frosini, *Diritto all'oblio e internet*, in *Federalismi.it*, 11 giugno 2014.

[21] L'art. 12, comma 1, lett. b), della direttiva 95/46/CE, rubricato "diritto di accesso", stabilisce che «Gli Stati membri garantiscono a qualsiasi persona interessata il diritto di ottenere dal responsabile del trattamento: la notificazione ai terzi, ai quali sono stati comunicati i dati, di qualsiasi rettifica, cancellazione o congelamento, effettuati conformemente alla lettera b), se non si dimostra che è impossibile o implica uno sforzo sproporzionato».

[22] L'art. 14, comma 1, lett. a), della direttiva 95/46/CE, rubricato "diritto di opposizione della persona interessata", stabilisce che «Gli Stati membri riconoscono alla persona interessata il diritto [...] di opporsi in qualsiasi momento, per motivi preminenti e legittimi, derivanti dalla sua situazione particolare, al trattamento di dati che la riguardano [...]».

[23] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati). L'art. 17 affianca al più lineare diritto alla cancellazione gli interessi da bilanciare per decidere in merito all'oblio di un soggetto interessato.

[24] CGUE, C-398/15, *Manni* (2016). La Corte è intervenuta a decidere sul caso di cancellazione dei dati personali contenuti in un pubblico registro delle imprese, legando l'esaurimento della necessità del trattamento del dato personale non allo scioglimento della società, bensì ad un momento successivo. Anche dopo l'avvenuto scioglimento, infatti, questi dati «possono risultare necessari, in particolare, per verificare la legittimità di un atto compiuto a nome di detta società nel periodo in cui essa era attiva o affinché i terzi possano avviare un'azione contro membri degli organi della società o contro i suoi liquidatori. Inoltre, in funzione dei termini di prescrizione applicabili nei diversi Stati membri, anche molti anni dopo che la società ha cessato di esistere possono ancora sorgere questioni per cui è necessario disporre di tali dati«. La conclusione della Corte del Lussemburgo è la necessità di una valutazione caso per caso al fine di poter stabilire con precisione il momento in cui è possibile concludere il trattamento dei dati personali in oggetto o limitarne l'accesso ai soli terzi che dimostrino un «interesse specifico alla loro consultazione».

[25] Paragrafo 64, sentenza *Manni*.

[26] L'art. 6, comma 1, lett. d), della direttiva 95/46/CE, rubricato "diritto di accesso", stabilisce che i dati personali devono essere «esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati o sono successivamente trattati, cancellati o rettificati». Pressoché ugualmente, l'art. 5, comma 1, lett. d), del Regolamento Generale sulla Protezione dei Dati stabilisce che «esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati».

Le evidenze utili per indagare e approfondire questo aspetto sono, ad oggi, molto poche. Il fatto che le decisioni sopra richiamate siano intervenute a giudizio di notizie fattuali e – almeno apparentemente - veritiere ha permesso agli estensori delle sentenze in commento di evitare approfondimenti specifici sulla rilevanza del criterio. I pochissimi elementi che emergono tra le righe della sentenza *Google Spain* e del caso *Manni* portano a desumere come l'intero giudizio di bilanciamento propenda già verso l'oscuramento del dato quando si parli di notizie non veritiere. Elemento coerente con il principio di esattezza del dato personale sopra richiamato e su cui il Gruppo di Lavoro Articolo 29[27] ha contribuito a far chiarezza. Infatti, l'accuratezza è da considerarsi concetto più ampio della mera veridicità del fatto rappresentato e va ricollegata ad effetti e cause anche solo potenzialmente provocabili, tra cui l'inadeguatezza e la generazione di impressioni fuorvianti che potrebbero scaturire dall'acquisizione o dall'interpretazione di tali informazioni[28]. Diversamente, il *Google Advisory Council*[29] - nominato appositamente per definire gli aspetti operativi dell'esercizio del diritto all'oblio - ha concordato che falsità e inaccuratezza della notizia contribuiscono a spostar l'ago della bilancia verso un rafforzamento della *privacy* del soggetto piuttosto che verso l'interesse pubblico diffuso alla conoscenza.

Non è quindi assolutamente chiaro chi abbia la responsabilità di indagare accuratezza e veridicità della notizia o del dato personale di cui si richiede la rimozione. E' però interessante apprendere come i Garanti rimettano in capo al richiedente[30] l'onere di fornire tutte le fonti utili a dimostrazione dell'inaccuratezza delle informazioni di cui si richiede il *de-listing* dai risultati di ricerca, ma solo in caso di richiesta specificamente indirizzata all'Autorità Garante competente[31]. Dunque, al di fuori dai casi patologici portati all'attenzione delle autorità competenti, la responsabilità di indagare la veridicità dell'informazione di cui si chiede la rimozione pare essere riposta in gran parte nelle mani del motore di ricerca[32], il quale non potrà far altro che decidere in base all'informazione parziale e a volte fuorviante che i suoi operatori riusciranno a reperire.

Ma se già valutare veridicità o falsità nonché accuratezza della notizia e del dato personale è un aspetto da sempre particolarmente convulso, come potranno i principali motori di ricerca gestire correttamente il carico immenso di richieste ricevute?

La soluzione è sostenibile solo ragionando in scenari di totale verità o totale falsità dell'informazione di cui si richiede l'eliminazione. Ma la situazione si complica appena – e come quasi sempre succede – il giudizio deve essere operato su fatti particolarmente complessi e mutevoli nel tempo, con sorgenti informative veritiere ed altre mendaci[33]. Si aggiunga poi che l'ingente numero di richieste a cui è necessario dar seguito con rapidità aumenta le probabilità di errori umani ed espone i soggetti interessati e i terzi portatori di interesse a situazioni pregiudizievoli.

Così, la domanda che val la pena porsi in questa sede è la seguente: può la tecnologia intervenire a supporto di questo processo per renderlo più sostenibile e controllabile? Quali rischi potrebbero celarsi dietro ad una soluzione "tecnicista", e quali possibili rimedi potrebbero essere attivati per prevenire queste situazioni rischiose?

4 Diritto all'oblio, verità e design tecnologico

La strada per trovare risposte a quesiti di tale ampiezza non può che essere impervia, e la complessità è dovuta alla numerosità degli strumenti che potrebbero supportare soluzioni realmente scalabili ed efficaci[34]. Sul piano generale, la tensione accresce quando il diritto all'oblio è affiancato

[27] Article 29 Data Protection Woking Party, *Guidelines on the implementation of the Court of Justice of the european union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" c-131/12*, 14/EN, WP225, Bruxelles, adottato il 26 novembre 2014.

[28] In tal senso, la suprema corte italiana ha affermato che «la notizia originariamente complete e vera diviene non aggiornata, risultando quindi parziale e non esatta, e pertanto sostanzialmente non vera». Corte di Cassazione, sent. 5525/2012, cit.

[29] The Advisory Council to Google on the Right to be Forgotten, Final Report, 6 febbraio 2015..

[30] L'iniziativa del soggetto interessato scaturisce dalla richiesta di esercizio del diritto di rettifica previsto dalla Direttiva. Così, L. Bianchi – G. D'Acquisto, *La sentenza Google e la questione delle esternalità dei trattamenti di dati personali*, in F. Pizzetti (a cura di), *Internet e la tutela della persona. Il caso del motore di ricerca*, Firenze, 2015, 67 ss.

[31] Article 29 Data Protection Woking Party, *Guidelines on the implementation of the Court of Justice*, cit., 11.

[32] Sulle complesse e minuziose questioni da cui potrebbero scaturire responsabilità per il motore di ricerca, si veda in particolare: S. Karapapa – M. Borghi, *Search engine liability for autocomplete suggestions: personality, privacy and the power of the algorithm*, in *International Journal of Law and Information Technology*, 23/2015.

[33] Molte situazioni simili sono emerse negli ordinamenti giuridici nazionali. Si pensi, ad esempio, il recente caso relativo al motore di ricerca Yahoo! deciso dal Garante per la Protezione dei Dati Personali italiano. La situazione vedeva una notizia vera e verificabile solo in un preciso momento storico, poi confutata dai fatti emersi in momenti successivi nel tempo. In merito, si veda l'ultimo provvedimento in materia: Garante Privacy, *Rimozione di un URL riconducibile ad una pagina web*, 26 febbraio 2017 (doc. web 6026501).

[34] Da un punto di vista metodologico, l'approccio transdisciplinare pare essere il più adatto al piano di ricerca in esposizione. Sul metodo si veda, in particolare: S.L.T. McGregor, *The nature of transdisciplinary research and practice*, Kappa Omicron Nu Human Sciences Working Paper Series, Boston, 2004.

ai concetti di *Privacy by Design* e *Privacy by Default*[35] quali strumenti di *enforcement* architetturale del fascio dei diritti a tutela dell'identità personale. Certo, tenere in considerazione i requisiti di protezione dei dati personali e dell'identità - nonché gli impatti per i diritti e le libertà delle persone fisiche[36] - fin dalle fasi di progettazione degli ambienti digitali non potrà far altro che portare ad una diminuzione dei costi di gestione dei diritti sia per i titolari che per i soggetti interessati ai trattamenti, riducendone le patologie connesse. Proprio nel contesto degli strumenti a supporto del diritto all'oblio è interessante notare come gli stessi strumenti che scalfiscono la nostra *privacy online* potrebbero essere utili proprio al suo medesimo rafforzamento, permettendo ad ogni utente di personalizzare la protezione della propria identità[37]. In altre parole, la medesima sofisticatezza degli algoritmi di ricerca e aggregazione delle informazioni[38] alla base dei motori di ricerca potrebbe essere utilizzata per prevenire lesioni del diritto alla riservatezza e allo stesso tempo aiutare titolari e responsabili a mantenere aggiornati ed esatti i dati personali dei soggetti interessati[39].

Non finisce qui. Gli strumenti più avanzati di *identity management* già permettono agli utenti di visualizzare e modificare ("accedere", "rettificare" o "cancellare" secondo la nuova tassonomia dei diritti previsti dal Regolamento) i dati personali che il titolare tratta ed alimenta continuamente.

Il passaggio successivo consisterebbe nell'applicazione di questi strumenti alle funzioni di ricerca in rete. Potrà così essere l'utente a selezionare le sorgenti informative che compongono il suo «profilo informazionale»[40]: alcune di queste sono da lui aggiunte, altre sono fornite da testate giornalistiche *online*, siti web o *social network* ed aggregate alternativamente. E se addirittura nascessero nuovi motori di ricerca utente-centrici[41] con modelli remunerativi basati sulla personalizzazione delle *SERP*[42]?

I problemi sono variegati, e muovono dalla soluzione dei casi di omonimia (e dunque ad evitare che notizie attinenti una persona non vengano automaticamente riferite ad un'altra persona solamente per omonimia) alla gestione delle richieste di rimozioni dei link da parte degli utenti nel momento in cui insistano interessi contrapposti di terzi, fino ai criteri di determinazione automatica del grado di esposizione pubblica del soggetto quale criterio basilare del bilanciamento necessario all'esercizio del diritto all'oblio. Varrebbe forse la pena di indagare i parametri dell'ontologia informativa di un soggetto e dei suoi valori etici al fine di "automatizzare" alcune richieste di cancellazione certamente legittime o illegittime, controllandone *ex post* la correttezza, magari anche con meccanismi di *feedback* diffusi, ma agendo immediatamente per rimediare a situazioni che potrebbero avere impatti devastanti sulla reputazione dei singoli soggetti. Governare l'informazione è dunque il primo elemento necessario da cui ri-partire.

Ma è proprio tornando al parametro oggetto dell'indagine del presente contributo – la veridicità della fonte informativa di cui si richiede il *delisting* – che emergono i maggiori profili problematici. Già svariati operatori si sono dotati di algoritmi per automatizzare l'esercizio del diritto all'oblio a fronte delle richieste degli utenti integrando tra loro le tecnologie disponibili[43], ma di fatto richiedendo sempre l'intervento di un operatore a fronte di *alert* inviati dal sistema proprio per verificare l'autenticità della notizia. In altre parole, questi algoritmi permettono di smistare le richieste tra i vari operatori disponibili e di gestire il flusso decisionale a fronte dell'apparente complessità della richiesta rilevata solamente a fronte di parametri quantitativi segnalati dall'utente (come, ad esempio, il numero di fonti a supporto della veridicità o della falsità dell'informazione).

---

[35] Art. 25, Regolamento Generale sulla Protezione dei Dati. Sul tema si veda anche il manifesto fondativo pubblicato da A. Cavoukian (Information and Privacy Commissioner - Ontario - Canada) titolato *Privacy by design - the 7 foundation principles*, 2009 (rev. 2011).

[36] L'analisi degli impatti sui diritti e sulle libertà delle persone fisiche è richiesto dagli articoli 32 (Sicurezza del trattamento) e 35 (Valutazione d'impatto sulla protezione dei dati) del Regolamento Generale sulla Protezione dei Dati al fine di rendere più efficaci le misure tecniche ed organizzative di protezione dei dati personali attivate nelle singole organizzazioni.

[37] Si è anche proposto di prevedere spazi a commento delle notizie in cui l'utente stesso possa "completare" l'informazione parziale, rendendola veritiera. In merito si veda L. Bianchi – G. D'Acquisto, *La sentenza Google e la questione delle esternalità dei trattamenti di dati personali*, cit.

[38] Nel gergo informatico, ci si riferisce agli strumenti di *data mapping*, *data classification* e *data aggregation*. Questi tre termini sono utilizzati per descrivere fasi diverse del processo di *knowledge management* necessario al governo dei sistemi informativi. In particolare, le tecniche di *data mapping* permettono di individuare i dati sparsi nei vari sistemi dell'organizzazione; successivamente, questi dati vengono classificati in base a categorie utili all'ente (*data classification*); infine, dati riferibili alla medesima entità vengono aggregati (*data aggregation*) per poter estrarre ulteriore conoscenza utile al business tramite inferenze logiche. Sul tema, si veda: C. Collison – G. Parcell, *Learning to fly: practical knowledge management from leading and learning organizations*, Canberra, 2005.

[39] A questo fine, Google ha recentemente predisposto una nuova funzionalità che mira a notificare all'utente ogni qual volta il motore indicizzi una notizia sul suo conto, collegandola al suo profilo. Questo potrà certamente permettere un intervento più immediato a rettifica o aggiornamento della notizia appena pubblicata tramite il sistema Alert. Per maggiori informazioni, si veda: https://www.google.com/alerts.

[40] L. Floridi, *The philosophy of information*, Oxford, 2011.

[41] Alcuni "*real-time people search engines*" già esistono, ma ancora non esistono studi approfonditi sulla materia. Tra questi: Waatp (waatp.com), Spokeo (spokeo.com) e QWant (qwant.com).

[42] La *Search Engine Result Page* (*SERP*) si intende la pagina contenente l'elenco ordinato dei risultati restituiti dall'interrogazione di un motore di ricerca.

[43] Tra tutti, si veda: M. Simeonovski - F. Bendun – M.R. Asghar - M. Backes - N. Marnau - P. Druschel, *Oblivion: Mitigating privacy leaks by controlling the discoverability of online information*, International Conference on Applied Cryptography and Network Security, 2015.

La vera rivoluzione consisterà nell'applicazione di strumenti di *deep learning*[44] a decisioni inerenti verità e oblio. Questa tecnica, infatti, riproduce le strutture neurali più complesse della mente umana permettendo all'algoritmo di apprendere dall'analisi di una base esperienziale e di continuare a migliorare le prestazioni in base ad una costante osservazione dell'operato dell'utente, replicando così decisioni complesse in maniera autonoma. Considerando la potenza computazionale oggi disponibile e la vastità informativa con cui potrebbe essere "nutrito" l'algoritmo, è facile immaginare che quel famoso parametro qui in analisi – la veridicità dell'informazione – sia analizzato e "calcolato" automaticamente. A fronte degli immensi benefici in termini di efficienza e tempestività, i rischi sociali da gestire e mitigare sono legati alla possibile perdita di controllo dell'algoritmo. Infatti, anche dopo poco tempo di attività, nemmeno chi ha programmato il sistema sarebbe in grado di ricostruire a ritroso le decisioni prese.
La domanda da porsi, quindi, è la seguente: se decideremo di delegare ad un algoritmo la decisione in merito alla veridicità delle notizie in fase di rimozione, come potremo esser sicuri che le decisioni da esso prese siano ottimali? In altre parole, come sarà possibile aumentare la fiducia che riponiamo in algoritmi a cui è rimessa in maniera pressoché automatica la ricostruzione, l'alimentazione e la gestione della nostra personalità in ambiente digitale, quando di fatto non conosciamo i meccanismi più intimi del loro funzionamento?

5 Trasparenza algoritmica: un possibile punto di partenza

Da dove partire, dunque, per sciogliere questa complessa matassa?
Tra le righe dell'analisi fin qui condotta emerge immediatamente l'importanza del concetto di "fiducia" *online* tra utenti e *service provider*, quale catalizzatore principale dell'economia digitale in costante crescita[45].
E' proprio il nuovo Regolamento Europeo in materia di protezione dei dati personali a ergere la fiducia degli utenti in rete a pilastro portante di tutta l'economia digitale[46]. Questo nuovo e innovativo strumentario giuridico contribuisce a ri-bilanciare i poteri del mercato tecnologico, riponendo nelle mani degli utenti svariati diritti[47] utili a controllare l'operato di chi gestisce le informazioni personali che li riguardano. Tra le maglie di queste nuove previsioni, centrale per questa analisi è il diritto dell'utente di conoscere l'esistenza di un processo decisionale automatico e di «ricevere informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato»[48]. A questo diritto corrisponde un nuovo dovere del titolare del trattamento: governare l'algoritmo e le strutture logiche del suo funzionamento per far fronte tempestivamente alle richieste avanzate dagli utenti[49].
Il concetto di trasparenza algoritmica è dunque un fondamentale punto di partenza, ma non già anche la soluzione. Molti degli strumenti descritti nel precedente paragrafo, oggi alla base dei principali servizi che utilizziamo quotidianamente, già contribuiscono a rendere i provider maggiormente "*accountable*"[50] e trasparenti. Nonostante ciò, il dibattito scientifico è attualmente uno dei più accesi, e dovrà essere analizzato attentamente per capirne gli effetti sulla fiducia dei consumatori e

[44] Il *deep learning* è uno degli strumenti più avanzati di intelligenza artificiale che permette ad un algoritmo di imparare e migliorare le sue reazioni dalla rappresentazione fornita da grandi quantità di dati. Queste tecniche derivano dagli strumenti di riconoscimento facciale e vocale e attualmente sono in corso ricerche per esportarne i benefici in domini quali il riconoscimento di medicinali, droghe e genomi. Sul tema si veda, in particolare: Y. LeCun - Y. Bengio - G. Hinton, *Deep learning*, in *Nature*, 521/2015.
[45] Gran parte dei piani dell'Unione Europea per il Digital Single Market sono proprio rivolti ad aumentare la fiducia degli utenti in rete migliorando i livelli di protezione dei dati personali e la sicurezza. Sul tema si veda, in particolare: Commissione europea, *Digital Single Market, Digital Economy and Society, Digital Privacy*.
[46] Fin dal 2010, Viviane Reding (all'epoca Vice-presidente della Commissione Europea responsabile per il Direttorato Giustizia, Diritti Fondamentali e Cittadinanza) esponeva come «*we need to modernise our data protection rules, which date from 1995. We need to build up a trusted environment for the use of personal data. The internet's full potential will only be realised if it is seen as a trusted and open platform. This is where the European Union can make a difference*». Si veda, in particolare: V. Reding, *Building trust in Europe's Online Single Market*, 2010.
[47] Il Regolamento Generale sulla Protezione dei Dati, oltre ad aver rafforzato il generico diritto ad avere informazioni esaustive ed effettive sulle modalità di raccolta e di trattamento dei dati personali (artt. 13 e 14), ridisegna l'armamentario dei diritti, comprendendo il diritto d'accesso dell'interessato (art. 15), il diritto di rettifica (art. 16), il diritto alla cancellazione (art. 17), il diritto alla limitazione del trattamento (art. 18), il diritto alla portabilità dei dati (art. 20), nonché l'importantissimo diritto di opposizione al processo decisionale automatizzato relativo alle persone fisiche (art. 21).
[48] Questo particolare diritto emerge in varie regioni del Regolamento. *In primis*, il titolare del trattamento è obbligato ad informare il soggetto interessato dell'esistenza di un processo decisionale automatizzato, anche compreso l'eventuale trattamento di profilazione, e fornire informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato, sia nel caso in cui i dati siano raccolti presso l'interessato (art. 13), sia in caso in cui i dati non siano raccolti in sua presenza (art. 14).
[49] Alcuni attenti autori sottolineano le debolezze del Regolamento in questo ambito. Pare, infatti, che questo diritto non sia che un labile tentativo di rendere edotto *ex-ante* il soggetto interessato al fine della decisione in merito al consenso e che non possa invero agire in fase successiva all'avvenuto trattamento. Sulla questione, si veda S. Watcher - B. Mittelstadt - L. Floridi, *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017.
[50] Sul concetto di *accountability* si veda, in particolare, European Data Protection Supervisor, *Meeting the challenges of big data, A call for transparency, user control, data protection by design and accountability*, Opinion, 19 novembre 2015.

sugli impatti che potrebbe avere nel mercato dei diversi motori di ricerca attivi in rete. Nonostante importanti gruppi di lavoro ne sottolineino i benefici[51], le critiche al concetto sono svariate e autorevoli[52], e muovono dalla necessità di mantenere nascoste certe metriche di calcolo per evitare raggiri all'algoritmo[53], alla necessità di rispettare il segreto industriale[54], fino ad indicarne la totale inutilità in varie occasioni[55] e addirittura all'incomprensibilità per gli utenti non dotati di conoscenze tecniche avanzate sulla materia[56]. Anche soluzioni simili quali procedure di *audit*[57] degli algoritmi sarebbero pressoché inefficaci.
L'unica soluzione ad oggi condivisa ritorna sul governo dell'algoritmo e delle sue componenti, in primis sulla correttezza delle basi esperienziali con cui il sistema è "allenato" in fase di avvio. Permettere al software di osservare una serie di decisioni in cui i bilanciamenti di interessi in gioco e la valutazione dell'accuratezza e della veridicità delle notizie sia svolta correttamente potrebbe aiutare ad ottenere decisioni automatizzate ottimali.
Quel che però serve sempre tenere a mente è che l'algoritmo è opera dell'ingegno di un essere umano, con le sue credenze e i suoi pregiudizi. Sempre un uomo lo governa e lo gestisce. Forse, la componente da valorizzare è proprio questa: ogni organizzazione che automatizza importanti decisioni fortemente impattanti sul nostro vivere quotidiano dovrebbe essere obbligata per legge a prevedere momenti di intervento umano in casi di difficile soluzione o non sicuramente prevedibili. Una figura - "*Artificial Intelligence Officer*"[58] - potrebbe essere pensata a supporto di questi controlli, oppure le medesime funzioni potrebbero essere gestite tramite richieste di *feedback* diffusi ad una comunità esperta e formata sulla specifica materia d'interesse[59] al fine di evitare soluzioni improvvisate, non ottimali o addirittura discriminatorie[60]. Ancora: e se questo ruolo fosse ricoperto da un agente software certificato che agisse come controllore dei principi giuridici ed etici durante il funzionamento dell'algoritmo?

6 Conclusioni

In conclusione, ciò che abbiamo di fronte a noi è chiaro: è necessario definire un percorso di ricerca per un'attenta gestione della conoscenza collettiva operata tramite la cura degli indici nei motori di ricerca[61], focalizzando l'attenzione sul governo degli algoritmi intelligenti che ne supportano l'attuazione. Siamo di fronte ad una nuova specie di oblio, che nasce dal bisogno intimo e personale di tutelare la proiezione sociale anche - ma non solo - in ambiente digitale, dove le regole del memorizzare e del cancellare (del conoscere e del dimenticare) sono sempre più imposte dagli algoritmi. Ogni soluzione che si raggiungerà non potrà prescindere dalla crescente importanza sociale del motore di ricerca che, collaborando proattivamente con gli utenti e governando adeguatamente gli algoritmi, avrà l'ardua responsabilità di limitare l'aggregazione delle fonti utili alla costruzione e

[51] Sul tema si veda, in particolare: F. Pasquale, *The Black Box Society - The Secret Algorithms That Control Money and Information*, Cambridge, 2015; R. Pollack-Ichou, *Opening the black box: in search of algorithmic transparency*, in Av.Vv. *GigaNet: Global Internet Governance Academic Network*, Annual Symposium, Chicago, 2016. Più recentemente, la US Association for Computing Machinery dell'US Public Policy Council ha pubblicato un documento che sintetizza i principi cardine della trasparenza algoritmica e di *accountability*. I princìpi sono: *awareness, access and redress, accountability, explanation, data provenance, auditability, validation and testing*. ACM US Public Policy Council, *Statement on algorithmic transparency and accountability*, 12 gennaio 2017.

[52] J. A. Kroll - J. Huey - S. Barocas - E.W. Felten - J.R. Reidenberg - D.G. Robinson - H. Yu, *Accountable algorithms*, in 165(3) *University of Pennsylvania Law Review* (2017), 633 ss.

[53] È stato dimostrato come, conoscendo l'algoritmo sottostante, sia possibile aggirare il sistema di controllo relativo al versamento delle tasse. In merito, si veda J. Reeves, *IRS Red Flags: How to Avoid a Tax Audit*, in www.usatoday.com. 3 maggio 2015.

[54] Basti pensare che gli algoritmi su cui si basano i risultati delle ricerche presentati da Google sono tra i più importanti segreti industriali dell'azienda, e mai potrebbero essere rivelati al grande pubblico contro la perdita di gran parte del potere di mercato.

[55] L'esempio classico riguarda gli algoritmi che presentano componenti di generazione di numeri randomici (si pensi alle lotterie ad estrazione automatica).

[56] Così, proprio J. A. Kroll - J. Huey - S. Barocas - E.W. Felten - J.R. Reidenberg - D.G. Robinson - H. Yu, *op cit.*, 24.

[57] In informatica, per audit si intende la revisione basata su evidenze di ciò che un algoritmo produce in output considerando uno specifico input. Sul tema, si veda D.W. Jones, *Auditing Elections*, ACM Computing Reviews, 2004.

[58] La figura dovrebbe presentare le seguenti caratteristiche: capacita tecniche in materia di intelligenza artificiale e conoscenza delle infrastrutture di gestione dei dati; abilità di lavorare tra le funzioni aziendali; abilita imprenditoriali; attitudine ad attrarre e mantenere altre capacità in materia di intelligenza artificiale. Si veda A. Ng, *Hiring your first chief AI Officer*, in *Harvard Business Review*, 2016. Svariate posizioni contro questa figura muovono dalla necessità di diffondere tra le figure aziendali già presenti le sensibilità necessarie a evidenziare possibilità e problemi in materia di intelligenza artificiale. Si veda, in particolare K.J. Hammond, *Please don't hire a Chief Artificial Intelligence Officer*, in *Harvard Business Review*, 2017. Ad ogni modo, le problematiche intorno questa figura potrebbero essere moltissime: chi è responsabile di controllarne l'operato? In base a quali principi giuridici o etici?

[59] Un ottimo esempio di collaborazione tra giornalisti e grande pubblico, basato su meccanismi di feedback diffusi per il *fact-checking* è la neonata piattaforma *WikiTribune*.

[60] Sulle conseguenze del *training* dell'algoritmo con fonti di origine razziali, si veda: B. Resnick, *How artificial intelligence learns to be racist*, in www.vox.com, 17 aprile 2017.

[61] Di fondamentale importanza per l'implementazione di questo diritto nell'organizzazione dei processi interni dei motori di ricerca è l'opinione dei Garanti europei che ha immediatamente seguito l'emanazione della sentenza Google Spain. Article 29 Data Protection Woking Party, *Guidelines on the implementation of the Court of Justice of the european union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" c-131/12*, 14/EN, WP225, adottato il 26 novembre 2014.

ricostruzione continua nel tempo del profilo dei soggetti interessati, riducendo le sfaccettature e i dettagli della persona che espone nella pubblica piazza digitale.
Certo è che, per continuare a far sì che i trattamenti dei dati personali siano al servizio dell'uomo[62], per continuare a rinforzare la tutela del diritto all'oblio in ambiente digitale nel rispetto di tutti gli altri diritti ed interessi coinvolti, rimarrà comunque necessaria una forte componente umana nel giudizio di bilanciamento, non trasponibile in algoritmo, da operare per imporre ad un sistema informatico di dimenticare. I molti ingranaggi di questo sofisticato meccanismo necessitano di essere quotidianamente oliati - raffinati dall'esperienza - evitando la deriva verso facili censure e abusi[63] che siano operati da umani o da algoritmi. Chissà poi se un cambiamento dirompente causato da strumenti decentralizzati e trasparenti come l'utilizzo della *blockchain*[64] per le liste del motore di ricerca riuscirà a supportare una tutela più efficace ed immediata dei diritti degli utenti, attivando quell'ancora oscuro principio di "responsabilizzazione"[65] del titolare del trattamento previsto dal Regolamento europeo.
Concludiamo ritornando al Sabatini-Colletti, per cui dimenticare è «perdere la memoria di qualcosa». Potremmo tentare un aggiornamento alla voce del noto dizionario. In ambiente digitale, dimenticare corrisponde a de-collegare molecole informative, tornando a frammentare l'informazione in nome della tutela dei nobili diritti fondamentali della persona, perdendo traccia di queste molecole nel profondo mare della conoscenza che è il web.

[62] Il Considerando 4 del Regolamento Generale sulla Protezione dei Dati enuncia che «il trattamento dei dati personali dovrebbe essere al servizio dell'uomo».
[63] Tra le tante critiche, la principale addita l'espansione del diritto alla cancellazione dei dati personali come un rischio alla libertà d'espressione in rete. Si veda, in particolare, D. Keller, *The new, worse 'right to be forgotten'*, in *Politico*, 27 gennaio 2016.
[64] Per le implicazioni della *blockchain* sulle policy europee si veda, in particolare: P. Boucher, *How blockchain technologies could change our lives*, in *European Parliament Research Service*, 2017.
[65] Il concetto di responsabilizzazione del titolare è riassunto dall'art. 5, comma 2, del Regolamento Generale sulla Protezione dei Dati, che attribuisce al titolare il dovere di comprovare il rispetto dei principi applicabili al trattamento dei dati personali elencati nel medesimo articolo, al comma 1.

Note a Sentenza
Sezione Europa
Notes and Comments
Europe

Corte di giustizia dell'Unione Europea
Court of Justice of the European Union

Corte di giustizia dell'Unione europea, 14 giugno 2017, causa C-610/15, *Stichting Brein v Ziggo BV and XS4All Internet BV*

Costituisce "comunicazione al pubblico", ai sensi dell'art. 3, par. 1, della direttiva 2001/29/CE del 22 maggio 2001, (direttiva INFOSOC), la gestione su Internet di una piattaforma di condivisione che, mediante l'indicizzazione di metadati relativi ad opere protette e la fornitura di un motore di ricerca, consente agli utenti di tale piattaforma di localizzare tali opere e di condividerle nell'ambito di una rete tra utenti (*peer-to-peer*). Integra pertanto violazione della predetta esclusiva la messa a disposizione e la gestione di una piattaforma di condivisione online quale è il sito The Pirate Bay se non autorizzata dai titolari del diritto delle singole opere

Il sito BitTorrent più resistente al mondo e la visione "verticale" del diritto di comunicazione al pubblico

The BitTorrent ECJ Case and the "Vertical" Understanding of the Right of Communication to the Public

diritto d'autore
comunicazione al pubblico
peer-to-peer
libertà di espressione
motori di ricerca

Carlo Blengino
Avvocato in Torino, Fellow del Nexa Center for Internet & Society

The Pirate Bay è forse il sito Internet che ha ricevuto maggiori attestazioni di illegalità per violazioni del copyright nella storia del web, rivelando per altro una certa impermeabilità alle statuizioni giudiziarie di buona parte delle Corti europee.
Come noto The Pirate Bay (d'ora innanzi "TPB") è un sito di *file sharing* basato sul protocollo di condivisione BitTorrent. La piattaforma creata nel 2003 riceve ed indicizza i file "*.torrent*" ed oggi i così detti *magnet-link* generati dagli utenti, agevolando la diffusione dei contenuti sulle reti Peer-to-Peer. Sui server della piattaforma non vi sono opere o contenuti tutelati dal diritto d'autore, presenti solo sui computer degli utenti, ma sono archiviati ed organizzati unicamente i file generati dal client BitTorrent all'atto della messa in condivisione: sono piccole stringhe di testo statiche contenenti le informazioni, codificate mediante un algoritmo di *hashing*, che descrivono i file da prelevare e/o da trasferire. Sono gli utenti stessi a caricare sul sito tali file di testo e TPB provvede a indicizzarli affinché siano reperibili per il successivo download dei contenuti direttamente dai vari computer degli utenti della rete.
Nel 2006 vi fu il primo sequestro dei server in Svezia per presunta violazione del copyright e nel 2009 il Tribunale di Stoccolma condannò in primo grado i responsabili del sito ad un anno di carcere ed a un'ingente somma di risarcimento danni a favore dei titolari dei diritti. Nel medesimo anno anche la nostra Corte di Cassazione con la sentenza n. 49437 emessa dalla III sezione penale in data 23 dicembre 2009 decretò, sebbene solo a fini cautelari e con pronuncia per certi versi criticabile, la rilevanza penale dell'attività del sito, astrattamente integrante secondo la Corte il reato di cui all'art.171 *ter*, lett. a-bis), della L.633/1941.
Il processo svedese approdò poi, all'esito dei vari gradi di giudizio, alla Corte Europea dei Diritti dell'Uomo.
La Corte di Strasburgo con la decisione del 19 febbraio 2013 nel procedimento n. 40397/12 *Sunde v. Sweden* riconobbe nella realizzazione della piattaforma di condivisione l'esercizio del diritto fondamentale alla libertà di espressione di cui all'art. 10 CEDU ma ritenne nel caso di specie legittima la compressione di tale diritto, e dunque la condanna, a salvaguardia della proprietà intellettuale, diritto parimenti tutelato dall'art. 1 del Protocollo n°1 della Convenzione.
TPB subì negli anni molteplici blocchi del DNS in quasi tutti i paesi d'Europa; ad ogni inibitoria è seguita la migrazione di dominio ed il sito ha continuato di fatto ad esser *online* senza soluzione di continuità. TPB è, almeno al luglio 2017, raggiungibile dall'Italia all'indirizzo thepiratebay.org.
È proprio in relazione ad una richiesta di inibizione e blocco dei nomi di dominio e degli indirizzi IP della piattaforma TPB che dall'Olanda il caso giunge nel 2015 anche all'attenzione della Corte di Giustizia dell'Unione Europea.
In data 14 giugno 2017 la Corte ha pronunciato, nella causa C-610/15, la sentenza qui in commento.
La Corte suprema dei Paesi Bassi nel decidere circa la legittimità di una inibitoria richiesta da una fondazione a tutela dei diritti d'autore nei confronti di due ISP affinché fosse bloccato l'accesso degli utenti ai nomi a dominio ed agli indirizzi IP corrispondenti al sito TPB, pone alla Corte del Lussemburgo i seguenti quesiti:

> «1. Se si configuri una comunicazione al pubblico, ai sensi dell'articolo 3, paragrafo 1, della direttiva 2001/29 [ndr, d'ora innanzi "INFOSOC"], ad opera del gestore di un sito Internet ove sul sito in parola non si trovano opere protette, ma esiste un sistema [...] con il quale vengono indicizzati e categorizzati per gli utenti metadati relativi ad opere protette disponibili sui loro computer, consentendo loro in tal modo di reperire e caricare e scaricare le opere protette.
> 2. Qualora la prima questione debba essere risolta negativamente: se gli articoli 8, paragrafo 3, della direttiva INFOSOC e 11 della direttiva 2004/48 [ndr, d'ora innanzi "IPRED"] consentano di emettere un'ingiunzione nei confronti di un intermediario ai sensi di tali disposizioni, ove siffatto intermediario faciliti attività illecite di terzi, come indicato nella prima questione».

La Corte affronta dunque nel caso TPB, per l'ennesima volta, un quesito relativo alla concreta portata del diritto di "comunicazione al pubblico" di cui all'art. 3, comma 1, della INFOSOC.
Come noto, la direttiva del 2001, nell'introdurre all'art. 3 un'esclusiva di fondamentale importanza per il mondo *online*, il diritto di comunicazione al pubblico, omise di precisarne la nozione. Fu, crediamo, una scelta cosciente: era opportuno lasciare all'interprete il compito di tracciare i confini di un'esclusiva destinata ad assumere forme e modalità sempre nuove nella rapida evoluzione della comunicazione in Internet.
Nel corso degli ultimi dieci anni la Corte si è così trovata ad affrontare diverse e sempre inedite questioni interpretative sul concetto di "comunicazione al pubblico", e la pronuncia in parola è solo l'ultimo coerente tassello interpretativo.
Il problema è che il cristallino percorso interpretativo della Corte, iniziato nel lontano 2006, si è da

sempre sviluppato in una visione esclusivamente "verticale", o se vogliamo settoriale, del concetto di comunicazione al pubblico.
Sin dalle prime sentenze relative a dispositivi hardware installati nelle camere d'albergo[1] e fino alle più recenti e discusse sentenze relative ai collegamenti *hyperlink* e all'utilizzo del "*framing*[2] la Corte si è sempre mossa nell'interpretare l'art. 3 nella cornice rigida della direttiva INFOSOC evidenziando ed enfatizzando gli scopi perseguiti dalla direttiva stessa[3].
Intento pregevole che ha però generato, nella costante riproposizione del medesimo percorso logico-interpretativo, un progressivo inevitabile ampliamento dell'esclusiva che è andata a coprire ogni attività non solo di diretta comunicazione delle opere, ma anche ogni attività di agevolazione o anche solo di intermediazione nella diffusione delle stesse.
La criticità della sentenza sta proprio in questa visione settoriale "verticale", strettamente legata alla normativa a tutela dei diritti d'autore e connessi: l'interpretazione risulta in sé coerente e nel contesto della direttiva INFOSOC apparentemente ineccepibile, ma omette e travolge ogni considerazione di contesto ed ogni riferimento alla normativa "orizzontale" sui servizi della società dell'informazione, azzerando di fatto le garanzie ed i meccanismi riservati agli intermediari della comunicazione dalla direttiva 2000/31, cosiddetta "e-commerce".
Le premesse sono comuni a tutte le pronunce della Corte in tema di comunicazione al pubblico:

- la direttiva 2001/29 non precisa la nozione di "comunicazione al pubblico" e occorre determinare il senso e la portata di tale disposizione in considerazione degli obiettivi perseguiti dalla direttiva stessa (punto 21);
- quest'ultima persegue quale obiettivo principale la realizzazione di un livello elevato di protezione a favore degli autori (punto 22);
- dunque la nozione di "comunicazione al pubblico" dev'essere intesa in senso ampio, come espressamente enunciato dal considerando 23 di tale direttiva (punto 22);
- gli autori dispongono pertanto di un diritto di natura precauzionale che consente loro di frapporsi tra eventuali utenti della loro opera e la comunicazione al pubblico che detti utenti potrebbero voler effettuare, e ciò al fine di vietare quest'ultima (punto 22).

Su queste basi, nel web, ogni attività volta a facilitare la diffusione dei contenuti, da chiunque compiuta e per qualsivoglia fine, rischia di tradursi in un atto di comunicazione al pubblico, con inevitabile potenziale violazione dell'esclusiva in capo ai titolari. Il diritto esclusivo di comunicazione al pubblico rischia di aver vita dura sul web 2.0., o viceversa.
Coscienti di ciò, i giudici iniziano sin dalla prima sentenza sul tema un faticoso percorso argomentativo per creare artificialmente confini accettabili per gli unici due parametri certi dettati dalla norma: il concetto di "atto di comunicazione" e il significato del termine "pubblico" quale destinatario. Nasce quella «valutazione individualizzata» (punto 23) da condursi caso per caso sulla base di «svariati criteri complementari, di natura non autonoma e interdipendenti fra loro» che si ritrova in tutte le sentenze: criteri non ben definiti, di pura creazione giurisprudenziale, che rischiano di snaturare l'atto di comunicazione «dell'opera» rendendone incerti i confini. I criteri attengono alle modalità tecniche della "comunicazione", che debbono esser «diverse» rispetto ad una eventuale prima lecita comunicazione, sul concetto di "pubblico" che deve esser quantitativamente rilevante e soprattutto «nuovo», e si giunge sino a fumosi criteri soggettivi, quali le finalità lucrative della comunicazione, definite sibillinamente «non prive di rilevanza» (sic!).
Sono tutti criteri che tentano di dare (buon) senso ad un diritto esclusivo che si rivela tanto più indefinito e insidioso per il web, quanto più il concetto di "atto di comunicazione" si amplia e si allontana dall'opera oggetto di tutela e dalla scelta consapevole di chi la detiene più o meno legittimamente, per estendersi alle sempre nuove forme e modalità di condivisione (gli *hyperlink*) giungendo inevitabilmente a coinvolgere potenzialmente le attività di tutti quei servizi della società dell'informazione che si pongono come meri intermediari della comunicazione.
Già sul tema del link, che integra una modalità di comunicazione mediata costituendo il collegamento un semplice rimando ad una comunicazione già in atto, nella sentenza *Svensson* e nelle successive sentenze *GS Media* e *Stichting Brein*[4], emerge evidente lo sforzo (infruttuoso) della Corte di salvaguardare attraverso la "valutazione individualizzata" una delle basi del web, l'*hyperlink* appunto.
Ma nel caso TPB la distanza tra l'atto di comunicazione dei contenuti pacificamente imputabile all'utente e la supposta comunicazione ad opera della piattaforma si amplia ulteriormente, posto

[1] CGUE, C-306/05, *SGAE v. Rafale Hotels* (2006).
[2] Fondamentali sul punto le sentenze CGUE, C-466/12, *Svensson* (2014) e C-160/15, *GS Media BV* (2016).
[3] CGUE, *SGAE v. Rafale Hotel,* cit., punto 34.
[4] CGUE, C-527/15, *Stichting Brein* (2017).

che a caricare i file *.torrent* ed i c.d. *magnet-link* ospitati e indicizzati sul sito sono gli utenti stessi e la piattaforma svolge una funzione non dissimile da quella di molti altri servizi intermediari della comunicazione, ovvero un servizio di hosting, per quanto certamente molto mirato e "attivo".
Ed è su questo passaggio che il ragionamento "verticale" della Corte, basato unicamente sulla direttiva INFOSOC, diviene forzato e pericoloso in una visione sistemica del diritto della rete.
Se TPB offre un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite dai fruitori delle reti peer-to-peer con protocollo BitTorrent, destinatari del loro servizio, (e questo lo si ricava anche dalla sentenza in commento al punto 36), perché non applicare a tale piattaforma la normativa orizzontale sul commercio elettronico, in particolare l'art. 14 della direttiva 2000/31?
Le esigenze di "alta" tutela dei titolari dei diritti perseguite dalla Corte sulla base della direttiva INFOSOC non sarebbero affatto pregiudicate dal regime di *safe harbour* dettato a tutela della libera circolazione dei contenuti: nessuno dubita infatti che gli amministratori di TPB -il cui nome è già un programma- siano effettivamente a conoscenza che le informazioni veicolate tramite il proprio servizio di hosting attivo siano illegali e siano essenziali o quanto meno agevolatrici di attività illecite. Sulla base della normativa orizzontale, in particolare del chiaro disposto dell'art. 14 della direttiva 2000/31, la piattaforma non può beneficiare del regime di irresponsabilità previsto a tutela della libera circolazione dei contenuti e delle informazioni ed infatti TPB ha, come detto, ricevuto molteplici attestazioni di illegalità per violazione del copyright in tutta Europa.
Era davvero necessario costruire una responsabilità diretta per violazione del copyright, quando il ruolo e le responsabilità di colui che oggettivamente appare come mero intermediario, seppur attivo e essenziale, già discendono dall'attento bilanciamento di interessi dettato dalla normativa sul commercio elettronico?
È interessante notare come l'argomentazione spesa dalla Corte ai punti 38 e 45 per tratteggiare una responsabilità diretta di TPB ampliando oltre misura il concetto di "comunicazione al pubblico dell'opera" siano le medesime argomentazioni tratteggiate dalla nota giurisprudenza sull'hosting attivo con riferimento alla "effettiva conoscenza" richiesta, qui sì espressamente, dall'art. 14 della direttiva 2000/31.
La Corte, attraverso quella «valutazione individualizzata» che include «svariati» (e imprecisati) «criteri complementari» di pura creazione giurisprudenziale, introduce elementi legati alla consapevolezza ed alla conoscenza dell'illegalità che poco hanno a che vedere con l'atto di comunicazione al pubblico dell'opera in sé e che appaiono in vero del tutto estranei all'art. 3 della direttiva INFOSOC.
Per quale ragione la Corte nella vicenda TPB pretermetta ogni valutazione in ordine alla natura del servizio ed alla sua funzione di intermediario nella comunicazione, azzerando di fatto il *safe harbour* dettato dalla normativa orizzontale, la cui corretta applicazione avrebbe peraltro consentito nel caso di specie identica tutela dei titolari dei diritti è difficile dirlo.
Vero è che in Europa, anche a livello legislativo, sembrano affacciarsi tempi duri per il regime di (ir) responsabilità degli intermediari della comunicazione che per vent'anni ha comunque garantito un adeguato bilanciamento tra la libera circolazione dei contenuti (e dunque la libertà d'espressione) e la tutela dall'illegalità e degli interessi dei terzi. La Comunicazione della Commissione "*A Digital Single Market Strategy for Europe*" (COM (2015) 192 final) non è confortante.
Proprio sul terreno del copyright, là dove il *safe harbour* è nato, si sta tentando attraverso legislazioni verticali di settore (dalla nuova direttiva dei servizi audiovisivi alla riforma della stessa INFOSOC [5]) di traslare la c.d. *secondary liability* propria dell'intermediario ad una responsabilità diretta, azzerando di fatto principi basilari come l'assenza di obblighi di monitoraggio e il sistema del *notice and take down* con l'introduzione del *notice and stay down*[6]. Sono segnali inquietanti, e la Corte sembra essersi adeguata. E non è cosa buona per Internet.

[5] Si veda Commission, *Proposal for a Council Directive amending Directive 2010/13/EU*, COM(2016) 287 Final e Commission, *Towards a Modern More European Copyright Framework* (Communication) COM (2015) 260 Final

[6] Sul tema segnalo il bell'articolo di G.Frosio, *From Horizontal to Vertical: An Intermediary Liability Earthquake in Europe*, in 12(7) *Journal of Intellectual Property Law & Practice* (2017), 565 ss.

Corte di giustizia dell'Unione europea, 15 marzo 2017, causa C-536/15, *Tele2 (Netherlands) BV, Zigo BV, Vodafone Libertel BV c. Autoriteit Consument en Markt (ACM)*

In un quadro normativo ampliamente armonizzato come quello dell'Unione europea, il consenso di un abbonato telefonico alla pubblicazione dei propri dati ai fini della pubblicazione sugli elenchi abbonati e servizi di consultazione si riferisce anche all'utilizzo dei medesimi in un altro Stato Membro. Infatti, la nozione di «richiesta» ai sensi dell'art. 25, par. 2 della direttiva 2002/22/CE (direttiva servizio universale) include altresì la richiesta da parte di un'impresa con sede in uno Stato membro diverso da quello in cui hanno sede le imprese che attribuiscono numeri di telefono agli abbonati.

Elenchi di abbonati telefonici: il consenso dell'interessato alla pubblicazione dei propri dati si riferisce anche all'utilizzo dei medesimi in un altro Stato Membro?

Publicly Available Directory Enquiry Services and Directories and the Scope of Subscribers' Consent

privacy
dati personali
servizio universale
consenso
elenchi abbonati

Deborah Behar
Cultrice della materia in Diritto Pubblico, Università Commerciale "L. Bocconi"

Il 15 marzo scorso, nella sentenza C-536/15 (*Tele2 (Netherlands) BV, Zigo BV, Vodafone Libertel BV c. Autoriteit Consument en Markt (ACM)*), la Corte di giustizia dell'Unione europea si è pronunciata sull'interpretazione e la portata dell'art. 25, par. 2 della direttiva 2002/22/CE (cosiddetta "direttiva servizio universale") relativa al servizio universale e ai diritti degli utenti in materia di reti e servizi di comunicazione elettronica.

I fatti: Il caso origina dal rifiuto di tre società olandesi (Tele2 BV, Zigo BV, Libertel BV) di comunicare dati relativi ai propri abbonati all'European Directory Assistance ("EDA"), società belga che fornisce elenchi abbonati e servizi di consultazione. In particolare, tali società olandesi ritenevano di non essere autorizzate a trasmettere tali dati a paesi diversi da quelli in cui gli abbonati avevano prestato consenso al loro utilizzo.

Adita dalla controversia, la Corte d'Appello del contenzioso amministrativo in materia economica dei Paesi Bassi (il *College van Beroep voor het bedrijfsleven*) ha sollevato due questioni pregiudiziali dinanzi alla Corte di Giustizia dell'Unione Europea.

Una prima domanda della Corte dei Paesi Bassi verteva sull'interpretazione di un aspetto particolare dell'art. 25 della direttiva servizio universale, ossia se tale direttiva dovesse applicarsi anche a "richieste" provenienti da paesi dell'Unione diversi dal paese in cui hanno sede le imprese che attribuiscono numeri ai loro abbonati.

Sul punto, la Corte di giustizia dichiara che la direttiva servizio universale si applica anche alle richieste provenienti da imprese in paesi diversi rispetto al paese in cui ha sede l'imprese che attribuisce numeri di telefono ai suoi abbonati. Risulta, infatti, dal testo dell'art. 25 della sopra menzionata direttiva, che tale disposizione riguardi «qualsiasi richiesta ragionevole di rendere disponibili le informazioni necessarie, ai fini della fornitura di elenchi e di servizi di consultazione accessibili al pubblico» e ciò «a condizioni non discriminatorie» [1]. Una distinzione nell'applicazione della direttiva servizio universale a seconda che la richiesta di messa a disposizione dei dati degli abbonati provenga da un'impresa che ha sede nello stesso Stato membro in cui ha sede l'impresa a cui è destinata tale richiesta o sia formulata da un'impresa con sede in uno Stato diverso dall'impresa destinataria di tale richiesta non solo violerebbe il principio di non discriminazione derivante dal ricordato art. 25 ma sarebbe altresì contraria allo scopo primario della direttiva servizio universale che, come si evince dalla lettera del suo art. 1, mira a garantire la disponibilità in tutta l'Unione europea di servizi di buona qualità accessibili al pubblico attraverso una concorrenza efficace e una disponibilità di scelta.

A riguardo, nella sentenza *Deutsche Telekom*[2] la Corte di giustizia aveva già fatto riferimento al considerando 35 della direttiva servizio universale[3], che dichiara che la fornitura degli elenchi abbonati e dei servizi di consultazione è già aperta alla concorrenza. Pertanto, in un mercato concorrenziale, l'obbligo a carico delle imprese che attribuiscono numeri di telefono di trasmettere i dati dei loro abbonati a imprese che forniscono elenchi abbonati e servizi di consultazione, conformemente all'art. 25 della direttiva menzionata, dovrebbe consentire non solo all'impresa destinataria dei dati il rispetto dell'obbligo di servizio universale previsto dall'art. 5 della direttiva ma altresì agli operatori telefonici di costituire una banca dati esauriente e di esercitare attività sul mercato dei servizi di fornitura di elenchi abbonati e di consultazione, senza vincoli né discriminazioni di sorta.

Per quanto riguarda la seconda questione pregiudiziale, il giudice di rinvio richiedeva se, in caso di risposta affermativa alla prima domanda, l'operatore telefonico che concede in uso tali numeri telefonici debba e possa operare una distinzione nella richiesta di consenso dell'abbonato per la pubblicazione dei suoi dati negli elenchi.

Ai sensi dell'art. 25, par. 2 della direttiva servizio universale, «gli Stati membri provvedono affinché tutte le imprese che assegnano numeri agli abbonati soddisfino qualsiasi richiesta ragionevole di rendere disponibili le informazioni necessarie, ai fini della fornitura di elenchi e di servizi di consultazione accessibili al pubblico, in una forma concordata e a condizioni eque, oggettive, orientate ai costi e non discriminatorie» e ciò «fatte salve le prescrizioni della legislazione [dell'Unione] in materi di protezione dei dati personali e della vita privata e, in particolare, quelle dell'articolo 12 della

[1] CGUE, C-536/15 (2017), *Tele2 (Netherlands) BV, Zigo BV, Vodafone Libertel BV c. Autoriteit Consument en Markt (ACM)*, punto 29.

[2] CGUE, C-543/09, *Deutsche Telekom* (2011).

[3] Direttiva 2002/22/CE del Parlamento Europeo e del Consiglio del 7 marzo 2002 relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica ("direttiva servizio universale") – Il considerando 35 sancisce che: «La fornitura degli elenchi abbonati e dei servizi di consultazione è già aperta alla concorrenza. Le disposizioni della presente direttiva integrano quelle della direttiva 97/66/CE, conferendo il diritto, per gli abbonati, a veder figurare i propri dati in elenchi su supporto cartaceo od elettronico. Tutti i fornitori di servizi che attribuiscono numeri di telefono ai rispettivi abbonati sono tenuti a mettere a disposizione le informazioni pertinenti con modalità eque, orientate ai costi e non discriminatorie».

[direttiva "vita privata e comunicazioni elettroniche"]» [4]. La direttiva servizio universale sembra pertanto richiamare, da un lato, la disciplina dell'art. 8 della Carta dei diritti fondamentali dell'Unione sul diritto alla protezione dei dati personali e della direttiva 95/46 che mira a garantire la tutela dei dati personali negli Stati membri, ma anche, e più precisamente, l'art. 12 della cosiddetta direttiva "vita privata e comunicazioni elettroniche"[5].

Per quanto riguarda l'interpretazione dell'art. 12 della direttiva "vita privata e comunicazioni elettroniche", la Corte di giustizia richiama la sua giurisprudenza precedente, e in particolare la sentenza *Deutsche Telekom*. In tale sentenza, la Corte aveva sancito che dal tenore letterale dell'art. 12 si desume che, quando un abbonato sia stato informato dall'impresa che gli ha fornito un numero di telefono della possibilità che i suoi dati personali siano trasmessi ad un'impresa terza per essere inseriti in un elenco pubblico e questi abbia acconsentito alla pubblicazione dei propri dati in un simile elenco, egli non è tenuto a prestare nuovamente il suo consenso alla trasmissione dei dati personali a un'impresa terza, purché tali dati non vengano utilizzati per scopi diversi da quello per il quale il primo consenso è stato rilasciato. In altre parole, la Corte ritiene che il consenso dato dall'abbonato alla pubblicazione dei propri dati in elenchi abbonati si estenda a qualunque ulteriore trattamento da parte di imprese terze sul mercato della fornitura di elenchi e servizi di consultazione, purché venga perseguita la medesima finalità. L'art. 12 non concede pertanto un diritto selettivo all'abbonato ossia un diritto di decidere in favore di quale impresa dare il proprio consenso. La Corte considera pertanto che la finalità della prima pubblicazione dei dati personali per il quale l'abbonato abbia assentito sia quella determinante al fine di valutare la portata del consenso. La Corte aggiunge inoltre che la trasmissione dei dati a un'impresa terza rispetto a quella per il quale si è dato il consenso non lede la sostanza del diritto alla tutela dei propri dati personali sancito all'art. 8 della Carta dei diritti fondamentali. Difatti, a prescindere dal loro luogo di stabilimento nell'Unione, le imprese che forniscono elenchi abbonati e servizi di consultazione sono soggette a un sistema di tutela dei dati personali armonizzato. In tali circostanze, non vi sarebbero dunque motivi ragionevoli per praticare una differenza di trattamento né la necessità di ottenere un ulteriore consenso a seconda che l'impresa sia stabilita in un paese membro o no.

[4] Direttiva 2002/22/CE del Parlamento Europeo e del Consiglio del 7 marzo 2002 relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica ("direttiva servizio universale") – art. 25, par. 2: «Gli Stati membri provvedono affinché tutte le imprese che assegnano numeri agli abbonati soddisfino qualsiasi richiesta ragionevole di rendere disponibili le informazioni necessarie, ai fini della fornitura di elenchi e di servizi di consultazione accessibili al pubblico, in una forma concordata e a condizioni eque, oggettive, orientate ai costi e non discriminatorie».

[5] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche ("direttiva vita privata e alle comunicazioni elettroniche").

Corte di giustizia dell'Unione europea, 26 luglio 2017, parere n. 1/15

Su richiesta del Parlamento europeo, lo scorso 26 luglio la Grande sezione della Corte di giustizia dell'Unione europea si è espressa, con proprio parere 1/15, circa la compatibilità del nuovo accordo previsto tra Canada e UE in materia di trasferimento di dati del codice di prenotazione (PNR) dei passeggeri aerei con il diritto dell'Unione europea.
La Corte, chiamata a pronunciarsi sul trasferimento sistematico dei dati di PNR a un'autorità canadese, nonché sulla disciplina del loro trattamento, conservazione ed eventuale trasferimento ulteriore nel quadro della lotta contro il terrorismo e i reati gravi di natura transnazionale, ha concluso per l'incompatibilità dell'attuale formulazione dell'accordo con i diritti fondamentali garantiti dalla normativa dell'Unione.
In particolare, le censure mosse dalla Corte riguardano la violazione dei principi di cui agli articoli 7, 8 e 52 della Carta di Nizza e investono i profili di chiarezza e determinatezza dei dati personali oggetto dell'accordo, i diritti individuali dei soggetti interessati dal trattamento di dati, i meccanismi di controllo del rispetto dell'accordo, i limiti al trattamento e ai trasferimenti ulteriori dei dati PNR.

L'Accordo PNR tra Canada e UE non prende il volo

The PNR EU-Canada Agreement Does not Take the Flight

dati personali
data protection
accordo Canada-UE
Carta di Nizza
privacy

Matteo Leffi
Praticante avvocato in Milano

1 Introduzione

L'affermarsi e il proliferare del terrorismo internazionale, nonché la accresciuta dimensione transnazionale di molti reati, hanno comportato negli ultimi decenni l'esigenza di sviluppare e rafforzare meccanismi di cooperazione internazionale e di coordinamento tra i principali Paesi e potenze regionali del mondo. Coerentemente, l'Unione europea e alcuni tra i principali stati occidentali hanno intensificato i controlli e gli scambi di dati volti a tutelare interessi di ordine generale e sicurezza pubblica. In questo quadro hanno assunto centrale importanza i trasferimenti e i trattamenti dei cd. dati del codice di prenotazione (*Passenger Name Record*, o PNR), una serie di dati personali e di informazioni che i passeggeri forniscono alle compagnie aeree o agli agenti di viaggio al momento della prenotazione dei voli, del *check-in* e dell'imbarco, dai quali le autorità pubbliche possono ricavare importanti informazioni di *intelligence*. Negli ultimi anni, l'Unione europea ha concluso accordi sul trasferimento di dati PNR con gli Stati Uniti, il Canada e l'Australia; ha inoltre adottato, in data 27 aprile 2016, la direttiva 2016/681 "sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti di reati di terrorismo e dei reati gravi", la quale disciplina il trasferimento e il trattamento di siffatti dati internamente al territorio dell'Unione. Oggetto di questa trattazione è il nuovo accordo previsto tra Canada e Unione europea in materia di trasferimento di dati PNR, e in particolare il parere che la Grande sezione della Corte di giustizia dell'Unione europea ha recentemente reso, su richiesta del Parlamento europeo, circa la compatibilità dell'accordo previsto con il diritto dell'Unione (parere 1/15 del 26 luglio 2017).

2 L'accordo tra Unione Europea e Canada sul trasferimento dei dati di PNR.

Nel settembre 2009 è giunto a scadenza l'accordo sottoscritto tra la Comunità europea e il Governo del Canada sul trattamento dei dati PNR, rendendo così necessario l'avvio di negoziati al fine di addivenire a un nuovo accordo. A seguito di un procedimento cominciato nel maggio 2010, Canada e Unione europea hanno quindi firmato, in data 25 giugno 2014, un nuovo accordo sul trasferimento e il trattamento dei dati del codice di prenotazione: l'accordo previsto, che consta di ventotto articoli e un allegato, è volto a consentire il trasferimento sistematico dei dati di PNR dei passeggeri aerei a un'autorità canadese nonché a disciplinare il loro trattamento, la loro conservazione e il loro eventuale trasferimento ulteriore a diverse autorità e paesi terzi nel quadro della lotta contro il terrorismo e i reati gravi di natura transnazionale. Con lettera del 7 luglio 2014, il Consiglio dell'Unione europea ha chiesto al Parlamento europeo di approvare il progetto di decisione avente a oggetto l'accordo sottoscritto con il Canada; il Parlamento ha a propria volta adottato una risoluzione volta alla richiesta di un parere della Corte di giustizia. Più nel dettaglio, il Parlamento ha sottoposto alla Corte due quesiti: *in primis*, ha chiesto alla Corte di sciogliere il nodo della base giuridica adeguata della decisione del Consiglio relativa alla conclusione dell'accordo con il Canada; in secondo luogo, e soprattutto, ha invitato la Corte a pronunciarsi sulla conformità dell'accordo previsto con il diritto dell'Unione.

3 Sulla base giuridica adeguata in relazione al TFUE.

Per quanto concerne l'idoneità della base giuridica, va rilevato come l'art. 1 dell'accordo in esame contenga un duplice riferimento: da un lato, alla definizione delle «condizioni per il trasferimento e l'uso dei dati del codice di prenotazione […] e i mezzi con cui i dati sono protetti»; dall'altro alla finalità di garantire la «sicurezza e l'incolumità delle persone». A partire da questa bipartizione dello scopo dell'accordo, vi è chi ha identificato la base giuridica adeguata nell'articolo 16 TFUE, valorizzando in questo modo una lettura complessiva dell'accordo orientata alla tutela dei dati personali (così le valutazioni formulate dal Parlamento europeo). *Ex adverso*, vi è chi ha ritenuto prevalente l'obiettivo di garantire la sicurezza delle persone, relegando l'obiettivo della protezione dei dati personali a un ruolo strumentale e individuando come base giuridica adeguata gli artt. 82 e 87 TFUE in materia di cooperazione giudiziaria in ambito penale e cooperazione di polizia (così la Commissione e il Consiglio, nonché la Francia, il Regno Unito e i governi estone e bulgaro).
I giudici di Lussemburgo propendono per una soluzione di sintesi tra le due posizioni. Riconoscendo la duplice e inscindibile finalità che ispira e sottende l'intero accordo con il Canada, infatti, la

Corte ha escluso che il trasferimento e il trattamento dei dati di PNR da parte dell'autorità competente canadese – sebbene logicamente precedenti e preordinati all'obiettivo di garantire la sicurezza pubblica – siano prevalenti rispetto alle finalità di protezione dei dati personali che informano larga parte delle norme di dettaglio contenute nell'accordo (il richiamo è soprattutto agli articoli da 7 a 21 dell'accordo, riuniti nel titolo "Salvaguardie applicabili al trattamento dei dati PNR"). Di conseguenza, la Corte identifica la corretta base giuridica parimenti nell'arti. 16, par. 2, e nell'art. 87, par. 2, lett. a), TFUE.

4 Sulla compatibilità dell'accordo previsto con le disposizioni del TFUE e della Carta di Nizza.

Prima di addentrarci nell'analisi dei profili di compatibilità con le disposizioni del TFEU e della Carta esaminati dalla Corte, è d'uopo osservare (come peraltro rimarcato nel comunicato stampa n. 84/17 della Corte di giustizia) che ci troviamo dinnanzi al primo caso in cui la Corte di giustizia dell'Unione europea è stata chiamata a pronunciarsi sulla compatibilità di un progetto d'accordo internazionale, oltre che con le disposizioni dei Trattati, anche con la Carta dei diritti fondamentali dell'UE (la "Carta di Nizza" o la "Carta"). Anche in riferimento a tale giudizio di compatibilità, le osservazioni presentate alla Corte sono state di duplice segno. Da una parte il Parlamento europeo, che ha espresso la propria perplessità circa l'ampiezza e la gravità delle ingerenze nei diritti fondamentali che l'accordo comporterebbe, sulla scorta della recente giurisprudenza *Digital Rights Ireland*[1] e alla luce dei dubbi manifestati dal Garante Europeo della Protezione dei Dati ("GEPD") nel proprio parere del 30 settembre 2013[2]. Dall'altra il Consiglio, la Commissione, e i governi intervenuti, che si sono invece espressi, da ultimo, nel senso del rispetto del principio di proporzionalità e della compatibilità dell'accordo con la Carta e i Trattati. La Corte di giustizia incentra la propria analisi dei trattamenti di dati personali previsti dall'accordo sul doppio binario della valutazione delle ingerenze nei diritti alla vita privata e alla protezione dei dati personali, di cui rispettivamente agli artt. 7 e 8 della Carta dei diritti fondamentali dell'UE (il dettato dell'art. 16 TFUE, infatti, è ritenuto dalla Corte assorbito dalla norma più specifica dell'art. 8). Si noti che l'art. 2 dell'accordo definisce i dati PNR come le «informazioni create da un vettore aereo per ciascun viaggio prenotato da un passeggero o per suo conto, necessarie al trasferimento e al controllo delle prenotazioni». Più nel dettaglio, l'allegato all'accordo contiene un'elencazione in diciannove rubriche delle tipologie di informazioni oggetto di trasferimento, comprendente *inter alia* il nome del passeggero, le date di prenotazione del biglietto e di viaggio, informazioni sul pagamento, sull'itinerario e sui bagagli, sullo status di viaggio del passeggero. A tal proposito la Corte di giustizia rileva, da un lato, come l'accordo previsto consenta il «trasferimento sistematico e continuo» dei dati PNR di tutti i passeggeri dei voli aerei tra Unione europea e Canada; dall'altro, che tali dati, considerati complessivamente, sono in grado di rivelare informazioni precise - e finanche sensibili - sui passeggeri stessi. Appurato quindi che il trasferimento di dati PNR verso il Canada e gli ulteriori trattamenti degli stessi costituiscono un'ingerenza nei diritti fondamentali, e stabilito che tali trattamenti sono tuttavia idonei a perseguire l'obiettivo di garantire la sicurezza pubblica (sancito anch'esso, peraltro, dall'articolo 6 della Carta), la Corte di giustizia ribadisce, in linea con la propria giurisprudenza, che i diritti previsti dagli artt. 7 e 8 della Carta di Nizza non sono tuttavia da considerarsi delle prerogative assolute. In quest'ottica, la Corte ricorda che la clausola generale dell'art. 52 della Carta subordina le limitazioni dei diritti in parola al rispetto del principio di proporzionalità, e passa quindi ad esaminare il carattere di stretta necessità di tali limitazioni, indagando parallelamente il grado di chiarezza e precisione delle disposizioni e delle misure contenute nell'accordo. Nel merito del test di compatibilità con gli artt. 7, 8 e 52, par. 1, della Carta di Nizza, la Corte ha evidenziato nel suo parere una serie di profili di contrasto – la cui analisi è stata qui ritenuta di maggior interesse rispetto ai punti dell'accordo che non hanno sollevato pareri contrari da parte della Corte - stanti i quali l'accordo PNR non può essere concluso nella sua configurazione attuale.

La prima di queste censure investe i profili inerenti ai dati di PNR contemplati dall'allegato all'accordo. A giudizio della Corte, infatti, vi sono almeno tre rubriche (e segnatamente le rubriche 5, 7 e 17) caratterizzate da formulazioni generiche e che non definiscono i dati PNR da trasferire – e dunque la portata delle ingerenze nei diritti fondamentali – con sufficiente chiarezza e precisione. Sullo stesso tema, un aspetto ancor più problematico è poi individuato dalla Corte nella possibi-

[1] CGUE, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland* (2014).
[2] (2014/C 51/06).

lità - lasciata aperta dalla rubrica 17 dell'allegato all'accordo, nonché agli artt. 8 e 16 dello stesso - che oggetto del trasferimento verso il Canada e dei successivi trattamenti siano dei dati qualificati come sensibili. In riferimento a tali dati, la Corte rileva i rischi connessi a trattamenti contrari al principio di non discriminazione sancito all'art. 21, ritenendo necessaria, per la legittimità del trasferimento di dati sensibili verso il Canada, una giustificazione solida e precisa che non può riscontrarsi nella protezione della sicurezza pubblica contro il terrorismo. Ancora, in materia di trattamenti automatizzati di dati, la Corte rileva, da un lato, come i dati trasferiti verso il Canada siano destinati in via principale ad essere analizzati mediante sistemi automatizzati che si basano su criteri prestabiliti e controlli incrociati con diverse banche dati, e, dall'altro, come siffatte analisi presentino un significativo margine d'errore. Nonostante l'accordo contenga - al proprio art. 7 - una clausola di non discriminazione, a parere della Corte i modelli e criteri prestabiliti per i trattamenti automatizzati dovrebbero essere sufficientemente specifici e affidabili da individuare come *target* soltanto i soggetti gravati da un ragionevole sospetto di coinvolgimento in reati di terrorismo o a gravi reati di natura transnazionale. Affinché detti trattamenti possano considerarsi compatibili con i diritti fondamentali, essi dovrebbero essere incrociati esclusivamente con banche dati gestite dal Canada in materia di terrorismo e sicurezza transnazionale, e i risultati positivi di tali analisi automatizzate dovrebbero essere sottoposti a un meccanismo di riesame individuale mediante sistemi non automatizzati, prima che qualunque misura individuale possa essere adottata nei confronti dei passeggeri aerei.

Un terzo profilo di problematicità individuato dalla Corte attiene ai tempi di conservazione dei dati PNR e all'accesso a tali dati da parte delle autorità canadesi. In proposito, la Corte si rifà a principi più volte ribaditi nella propria giurisprudenza (si veda, *ex multis*, il già citato *Digital Rights Ireland*) quali la necessaria previsione normativa tanto di un legame oggettivo tra i dati da conservare e l'obiettivo perseguito, quanto di condizioni sostanziali e procedurali che disciplinino l'uso dei dati stessi. In base al dettato dell'art. 16 dell'accordo previsto, i dati PNR possono essere conservati dal Canada per un periodo massimo di cinque anni successivamente alla loro ricezione; parte di tali dati però dev'essere "mascherata" dopo trenta giorni (segnatamente, i nominativi dei passeggeri) ovvero dopo due anni (eventuali altri nominativi, informazioni di contatto disponibili, altre informazioni che consentano l'identificazione della persona fisica). A questo punto, la Corte distingue due diverse fattispecie. In primo luogo, viene analizzata la legittimità della conservazione e dell'uso dei dati PNR (i.) prima dell'arrivo dei passeggeri aerei, (ii.) durante il loro soggiorno in Canada e (iii.) al momento della loro uscita dal Paese: in riferimento a tale conservazione e a tali trattamenti, i giudici di Lussemburgo ritengono sussistere il necessario rapporto tra dati e obiettivo perseguito dall'accordo, stante la natura intrinsecamente generale e preventiva dei controlli di sicurezza e alle frontiere. Inoltre, i trasferimenti di dati previsti dall'accordo consentono di facilitare e velocizzare i controlli di sicurezza cui sono sottoposti, in linea con l'art. 13 della Convenzione di Chicago, i passeggeri aerei in entrata e uscita dal Canada. L'unico distinguo in questo senso viene operato per l'utilizzo dei dati PNR dei passeggeri durante il loro soggiorno in Canada, che dovrebbe fondarsi su nuove giustificazioni ed essere sottoposto ad un preventivo controllo da parte di un giudice o di un'autorità amministrativa indipendente. Il legame oggettivo tra utilizzo dei dati e obiettivo perseguito viene invece meno, a giudizio della Corte, nella seconda fattispecie analizzata, riferita alla conservazione e all'uso dei dati di PNR dopo la partenza dei passeggeri aerei dal Canada. L'archiviazione dei dati PNR dopo la partenza del passeggero aereo interessato, infatti, è limitata allo stretto necessario soltanto laddove mirata a taluni soggetti che, sulla base di criteri oggettivi, sembrano rappresentare un rischio in termini di lotta al terrorismo anche successivamente alla loro partenza dal Canada. In casi siffatti, la durata fissata in cinque anni per l'archiviazione è conforme al test di stretta necessità, ma ogni uso dei dati PNR archiviati deve fondarsi su criteri e condizioni oggettivi quanto all'accesso delle autorità canadesi ai dati stessi, e dev'essere subordinato a un controllo giurisdizionale o amministrativo indipendente preventivo che autorizzi l'uso a seguito di motivata richiesta.

Le censure della Corte di giustizia investono poi le comunicazioni dei dati PNR da parte dell'autorità canadese competente ad altri soggetti, e in particolare ad autorità pubbliche di paesi terzi e a soggetti privati. Con riguardo alla prima e più importante ipotesi, l'art. 19 dell'accordo previsto garantisce all'autorità canadese competente un potere discrezionale quanto alla valutazione del livello di protezione offerto negli stati terzi. Senonché, tale disposizione non assicura che suddette comunicazioni siano limitate allo stretto necessario: il diritto dell'Unione europea (e segnatamente l'art. 26 della direttiva 95/46/CE, alla luce delle interpretazioni giurisprudenziali) subordina infatti i trasferimenti di dati verso paesi extra UE al requisito della prestazione di un livello di protezione dei dati personali sostanzialmente equivalente a quello garantito nell'Unione, sancito da un accordo

tra l'Unione e il paese terzo interessato, ovvero ad una decisione della Commissione nel senso dell'adeguatezza della tutela garantita nel paese terzo. L'attuale versione dell'accordo è, a giudizio della Corte, incompatibile con i diritti fondamentali previsti dalla Carta di Nizza anche quanto ai diritti individuali riconosciuti ai passeggeri aerei. Gli artt. 12 e 13 dell'accordo prevedono, in linea con il dettato dell'art. 7 della Carta di Nizza, un diritto di accesso e di rettifica dei propri dati PNR in capo ai passeggeri aerei. Tuttavia, nessuna disposizione dell'accordo sancisce un obbligo d'informazione individuale dei passeggeri, con il risultato che la mancanza di tale comunicazione strumentale impedisce e frustra l'esercizio dei due diritti richiamati.
Da ultimo, i giudici di Lussemburgo analizzano l'art. 10, par. 1, dell'accordo previsto, ai sensi del quale a presidio del rispetto delle disposizioni dell'accordo a tutela dei dati personali viene posta «un'autorità pubblica dipendente» o «un'autorità istituita con mezzi amministrativi che eserciti le proprie funzioni in modo imparziale e disponga di una comprovata autonomia». A giudizio della Corte, tale ultima formulazione non garantisce in modo sufficientemente chiaro e preciso l'indipendenza di tale autorità, ed è pertanto incompatibile con i requisiti posti dall'art. 8, par. 3, della Carta.

5 Conclusioni

Le censure mosse in negativo dalla Corte alla attuale formulazione dell'accordo previsto costituiscono dunque il punto di partenza, in positivo, su cui modellare una nuova versione dell'accordo che possa essere compatibile con il diritto dell'Unione. Infatti, pare qui opportuno ricordare che - in ossequio al dettato dell'art. 218, par. 11, TFUE - il parere negativo espresso dalla Corte pregiudica la possibilità che un siffatto accordo entri in vigore in assenza di modifiche allo stesso o di una revisione dei Trattati. Capire in quali forme e con quali tempistiche le istituzioni europee si conformeranno agli indirizzi contenuti nel parere della Corte resta un esercizio speculativo: quel che è certo è che l'accordo sui dati PNR con il Canada, per il momento, non prende il volo.

Corte di giustizia dell'Unione europea, 7 marzo 2013, causa C-275/15, *ITV Broadcasting c. TVCatchup*

L'art. 9 della direttiva 2001/29/CE, nel fare salve le disposizioni concernenti l'accesso ai servizi di diffusione via cavo, non si riferisce alla ritrasmissione via Internet, nella zona di trasmissione iniziale, di opere diffuse su canali televisivi. Pertanto, una normativa nazionale che, in caso di ritrasmissione con tali modalità, preveda un'eccezione al diritto esclusivo dei titolari del diritto d'autore di autorizzare o vietare la comunicazione al pubblico, è estranea all'ambito di applicazione dell'art. 9 della direttiva 2001/29/CE ed è in contrasto con il diritto dell'Unione, stante l'esaustività dell'elenco di eccezioni dell'art. 5 della medesima direttiva.

ITV Broadcasting contro *TVCatchup*, atto secondo: la Corte di giustizia UE torna sulla ritrasmissione *online* di canali televisivi

ITV Broadcasting V. TVCatchup, Chapter II: the Court of Justice of the European Union Takes Another Stance on the Retransmission of Broadcasts of Commercial Television Broadcasters Via the Internet

copyright
comunicazione al pubblico
ritrasmissione
cavo
Internet

Ernesto Apa
Avvocato in Roma

L'effetto dirompente di Internet e più in generale delle nuove tecnologie interessa trasversalmente tutti i settori del diritto, ma trova uno dei suoi terreni d'elezione nella disciplina del copyright. Ciò è dovuto, tra l'altro, alla circostanza che contenuti protetti dal diritto d'autore, ed in particolare opere audiovisive, sono il principale oggetto di fruizione degli utenti della rete (secondo il Rapporto I-Com su reti e servizi di nuova generazione del 2016, la quota di traffico di video su Internet già da anni supera il 50% e salirà all'80% entro il 2019).

In questo contesto, è piuttosto ovvio che la giurisprudenza debba occuparsi di numerosi casi in cui i tradizionali istituti giuridici posti a presidio delle opere dell'ingegno e frutto del lavoro intellettuale devono misurarsi con possibilità di sfruttamento prima sconosciute, originando controversie tra i titolari dei diritti, che vantano la pretesa di conservare il pieno controllo delle proprie opere, e i gestori di servizi innovativi che ritengono inapplicabili i paradigmi tradizionali. Ad esempio, numerosi casi, disseminati in diverse latitudini, hanno riguardato servizi che consistono nella ritrasmissione di contenuti audiovisivi già liberamente accessibili agli utenti, in quanto in origine trasmessi gratuitamente da emittenti televisive in chiaro, o comunque nell'ottimizzazione dell'accesso a tali contenuti[1].

La sentenza della Corte di giustizia dell'Unione europea oggetto di questa nota afferisce al novero di decisioni su tale tipologia di servizi. Nel caso specie, alcune emittenti televisive britanniche, fra cui ITV Broadcasting e Channel Four Television, hanno convenuto in giudizio davanti all'High Court of Justice, Chancery Division dell'Inghilterra e del Galles la società TVCatchup Limited, ritenendo che il servizio da quest'ultima erogato violi i diritti d'autore di dette emittenti.

Il servizio gestito da TVCatchup, ad onta del nome, non è una catch-up TV (ossia la messa a disposizione del pubblico in modalità on demand di programmi già trasmessi nell'ambito di un palinsesto televisivo), bensì un servizio di live streaming gratuito, consistente nella ritrasmissione simultanea (simulcast) su internet di canali televisivi già disponibili in chiaro via satellite o su frequenze terrestri nella medesima zona in cui si trovano gli utenti del servizio. A tali canali TVCatchup associa propri messaggi pubblicitari, che sono la fonte dei suoi proventi, i quali si giustappongono alla pubblicità già presente nei canali, che non viene rimossa.

ITV e le altre emittenti che hanno agito in giudizio ritengono che il servizio di TVCatchup realizzi una comunicazione al pubblico non autorizzata di contenuti sui quali, in base alla legge inglese, insiste il diritto d'autore delle emittenti. Dal suo canto, TVCatchup ritiene invece che la circostanza per cui i canali oggetto di ritrasmissione sono già liberamente accessibili dagli utenti del servizio escluda in radice la necessità di ottenere permessi dalle emittenti, che hanno reso disponibili i propri canali al medesimo pubblico cui si rivolge il servizio; a tal riguardo, giova evidenziare che TVCatchup verifica la provenienza dei propri utenti, per accertarsi che essi si trovino sulla porzione di territorio coperta dalla diffusione di detti canali in modalità free-to-air e che quindi la propria base di utenti coincida con il pubblico originario dei palinsesti ritrasmessi.

La High Court inglese ha sollevato una questione pregiudiziale davanti alla Corte di Giustizia dell'Unione europea e nella sentenza del 7 marzo 2013, la Corte ha stabilito che la ritrasmissione di contenuti televisivi effettuata con le modalità sopra indicate costituisce un'autonoma comunicazione al pubblico ai sensi dell'art. 3, par. 1, della direttiva 2001/29, il quale riconosce al titolare dei diritti di autore il diritto esclusivo di autorizzare o vietare qualsiasi comunicazione al pubblico delle opere oggetto di proprietà intellettuale. Pertanto, in base alla direttiva, come interpretata dalla Corte di giustizia, sia la comunicazione al pubblico in modalità lineare (ossia la diffusione di contenuti trasmessi nel momento predeterminato dall'emittente, nell'ambito di un palinsesto televisivo), sia la messa a disposizione del pubblico in modalità non lineare o a richiesta (laddove la trasmissione dei contenuti avviene al momento scelto dall'utente e su sua richiesta, sulla base di un catalogo predisposto dal fornitore, che esercita il controllo editoriale selezionando e organizzando i programmi), indipendentemente dalla piattaforma trasmissiva, sono nella disponibilità esclusiva dei "*right holder*" (che, nel caso di specie, la legge britannica individua nelle emittenti televisive), restando precluso a terzi qualunque sfruttamento, in assenza di apposita autorizzazione concessa dall'emittente o del ricorrere delle cause di eccezione previste, con elenco tassativo, dall'art. 5 della direttiva 2001/29. La Corte di giustizia ha dato un'interpretazione estensiva del concetto di comunicazione al pubblico, ritenendo che essa ricomprenda anche un servizio consistente in un flusso Internet che ritrasmetta opere dell'ingegno ad una platea di utenti, sebbene tali utenti si trovino nell'area di ricezione della trasmissione iniziale e la possano quindi ricevere, nel pieno rispetto della legge, su un apparecchio televisivo.

[1] Si pensi alla nota vicenda decisa dalla Corte Suprema degli Stati Uniti con la sentenza del 2014 *American Broadcasting Companies v. Aereo*; alla decisione resa nel 2012 dalla Federal Court of Australia nel caso *National Rugby League Investments Pty Limited v Singtel Optus Pty Ltd*; al caso *RecordTV Pte Ltd v. MediaCorp TVSingapore Pte Ltd and others*, deciso nel 2010 dalla Court of Appeal di Singapore; e l'elenco potrebbe continuare.

Sulla scorta della pronuncia resa dai giudici di Lussemburgo, la High Court of Justice ha giudicato illecita l'attività di TVCatchup con riferimento ad alcuni canali, ma non a tutti: ha infatti reputato che in relazione ai canali ITV, Channel 4 e Channel 5, in quanto soggetti a obblighi di servizio pubblico, fosse applicabile un'eccezione, prevista dalla legge inglese, e più precisamente dall'art. 73, par. 2, lett. b) e par. 3 del *Copyright, Designs and Patents Act*, che consente in talune circostanze la ritrasmissione via cavo senza autorizzazione.
Detto articolo, rubricato «Ricezione di una trasmissione senza fili e ritrasmissione della medesima via cavo», dispone che: «[…] ove una trasmissione senza fili effettuata da un luogo del Regno Unito sia ricevuta e immediatamente ritrasmessa via cavo […] 2. [i]l diritto d'autore sulla trasmissione non è violato […] b) se e nella misura in cui la trasmissione è destinata alla ricezione nella zona in cui viene ritrasmessa via cavo e fa parte di un servizio qualificante. […] 3. Il diritto d'autore su qualsiasi opera inclusa nella trasmissione non è violato se e nella misura in cui la trasmissione è destinata alla ricezione nella zona in cui viene ritrasmessa via cavo».
Le emittenti televisive hanno quindi impugnato la sentenza della High Court of Justice davanti alla Court of Appeal (Civil Division) dell'Inghilterra e del Galles, la quale ha a sua volta investito la Corte di Giustizia di una nuova domanda di pronuncia pregiudiziale, che è stata definita con la sentenza oggetto di questa breve nota.
La Court of Appeal (Civil Division) dell'Inghilterra e del Galles ha posto alla Corte di giustizia dell'Unione europea una serie di questioni, che in sostanza si propongono di accertare se l'eccezione al diritto esclusivo dei titolari del diritto d'autore di autorizzare o vietare la comunicazione al pubblico, invocata a favore di TVCatchup, prevista dall'art. 73 del *Copyright, Designs and Patents Act* sopra citato, sia compatibile con il diritto dell'Unione.
La Corte di giustizia dell'Unione europea, Quarta Sezione, con sentenza dell'1 marzo 2017, ha definito la causa in piena consonanza con le conclusioni che erano state rassegnate l'8 settembre 2016 dall'Avvocato Generale Henrik Saugmandsgaard Øe.
Il punto principale deferito alla Corte di Giustizia riguarda la possibilità di ricomprendere l'art. 73 del *Copyright, Designs and Patents Act* nel novero delle norme la cui applicabilità è fatta salva dall'art. 9 della direttiva 2001/29. Infatti, nessuna delle parti, né il giudice *a quo*, nutrono dubbi circa il fatto che la previsione derogatoria dell'art. 73 non rientri tra le eccezioni ammesse dall'art. 5 della direttiva 2001/29. Non essendo invocabile, nel caso del servizio fornito da TVCatchup, alcuna delle eccezioni *ex* art. 5 della direttiva, l'unica base giuridica che, alla stregua del diritto dell'Unione, potrebbe astrattamente giustificare l'art. 73 è stata individuata dalla Court of Appeal nell'art. 9 della direttiva, a mente del quale «La presente direttiva non osta all'applicazione delle disposizioni concernenti segnatamente brevetti, marchi, disegni o modelli, modelli di utilità, topografie di prodotti a semiconduttori, caratteri tipografici, accesso condizionato, accesso ai servizi di diffusione via cavo, la protezione dei beni appartenenti al patrimonio nazionale, gli obblighi di deposito legale, le norme sulle pratiche restrittive e sulla concorrenza sleale, il segreto industriale, la sicurezza, la riservatezza, la tutela dei dati e il rispetto della vita privata, l'accesso ai documenti pubblici, il diritto contrattuale».
La corte inglese ha quindi chiesto alla Corte di giustizia se il riferimento all'«accesso ai servizi di diffusione via cavo» valga a fare salva la disposizione della legge inglese in discorso. La Corte di giustizia, dopo aver premesso che «in mancanza di un rinvio espresso al diritto degli Stati membri, la nozione di «accesso ai servizi di diffusione via cavo» di cui all'art. 9 della direttiva 2001/29, deve ricevere, in tutta l'unione, un'interpretazione autonoma e uniforme», risponde negativamente al quesito: l'art. 73 del *Copyright, Designs and Patents Act* britannico deve ritenersi in contrasto con il diritto dell'Unione in quanto introduce un'eccezione all'esercizio dei diritti dell'autore di un'opera dell'ingegno che non è prevista e quindi va considerata vietata, stante l'esaustività dell'elenco di eccezioni dell'art. 5 della direttiva.
La sentenza, quindi, si pone nel solco dell'orientamento che, con riferimento all'interpretazione della norme in materia di diritto d'autore in relazione all'emergere di nuove modalità di sfruttamento rese possibili dalla tecnologia, valorizza le indicazioni offerte dal preambolo della direttiva 2001/29, ed in particolare il richiamo, contenuto nel considerando 4, agli obiettivi di garantire un elevato livello di protezione della proprietà intellettuale e promuovere gli investimenti in attività creatrici ed innovatrici.
A differenza della sentenza ITV del 2013, che affrontava una questione di grande interesse (inscrivendosi nel filone giurisprudenziale che ha sagomato il concetto di comunicazione al pubblico facendo leva principalmente su due elementi, ossia se l'opera è diretta ad un nuovo pubblico e se

essa è diffusa con una modalità tecnica diversa da quella adottata per la comunicazione originale[2] ed offriva alla Corte la possibilità di chiarire la portata del concetto di comunicazione al pubblico e l'ineludibilità del consenso del titolare dei diritti per quanti vogliano ritrasmettere, su altre piattaforme, canali televisivi in chiaro, la decisione esaminata appare molto concentrata su un tratto peculiare del diritto britannico. L'unica affermazione di portata generale, concernente la tassatività delle eccezioni al diritto di riproduzione e comunicazione al pubblico previste dall'art. 5 della direttiva 2001/29, è tratta dal considerando 32 della direttiva, quindi non riguarda un tema controverso. La Corte si pronuncia recisamente sul caso sottopostole e lo fa con una motivazione molto stringata, che non solo considera – condivisibilmente – assorbite le altre questioni una volta che sia stata data risposta alla terza tra quelle sollevate dalla corte britannica, ma non ritiene neanche necessario, ai fini della definizione della causa, misurarsi con i nodi ermeneutici sui quali invece si era soffermato con dovizia l'Avvocato Generale.

La concisione è un pregio, ma sembra che la Corte ometta qualche passaggio – svolto invece dall'Avvocato Generale – che probabilmente sarebbe stato necessario per offrire un iter argomentativo completo e coerente, certamente sarebbe stato utile per chiarire il contenuto normativo dell'art. 9 della direttiva 2001/29, il quale, come segnalato dall'Avvocato Generale Saugmandsgaard Øe, ricorre ad una nozione, quella di «accesso ai servizi di diffusione via cavo», che, pur apparendo *prima facie* un concetto noto dell'*acquis* dell'Unione, in realtà non lo è affatto.

L'Avvocato Generale non si è sottratto all'onere di interpretare l'art. 9 della direttiva (che poi era il fulcro dei quesiti posti alla Corte), concludendo che (i) nell'articolo in parola, l'espressione "cavo" non designa qualunque rete trasmissiva che usi un conduttore fisico, ma va intesa in senso stretto, come riferita ad una specifica tecnologia, ossia alle «reti cablate classiche», e non comprende quindi Internet (oltre a non comprendere, ovviamente, le trasmissioni via etere o satellite) e (ii) l'art. 9 persegue l'obiettivo di lasciare impregiudicate le disposizioni che regolano l'accesso all'infrastruttura di trasmissione costituita da reti cablate tradizionali. L'aggiunta di questi tasselli consente di cogliere che l'art. 9 della direttiva è inconferente rispetto al tema della ritrasmissione via cavo e, quindi, di avere una migliore comprensione delle ragioni per cui l'art. 73 del *Copyright, Designs and Patents Act* britannico è viziato da illegittimità alla stregua del diritto dell'Unione.

La Corte, invece, si è fermata un passo prima, limitandosi a segnalare che l'art. 9 mira a mantenere l'efficacia di disposizioni che non riguardano la comunicazione al pubblico o comunque il settore armonizzato dalla direttiva. La decisione quindi presenta un esiguo gradiente di novità.

[2] Cfr.l'ordinanza della CGUE nella causa C-314/13, *BestWater*, *BestWater International GmbH v. Michael Mebes e Stefan Potsch* (2014), ma anche la sentenza *Svensson*, C-466/12 (2014).

Corte di giustizia dell'Unione europea, 9 marzo 2017, causa C-398/15, *Camera di Commercio c. Manni*

Non esiste diritto all'oblio per i dati personali contenuti nel registro delle imprese; tuttavia, in via eccezionale, il trascorrere del tempo può consentire la limitazione dell'accesso a tali dati, in presenza di circostanze speciali.
Il mantenimento dei dati relativi alle società anche a distanza di molti anni serve a garantire la certezza del diritto nelle relazioni tra le società e i terzi e a tutelare, in particolare, gli interessi dei terzi rispetto alle società che offrono come unica garanzia il proprio patrimonio sociale, e solo in via eccezionale può essere limitato, con l'effetto di riconoscere comunque, per quanto in via interstiziale, un'autonoma rilevanza del diritto all'oblio anche di dati attinenti alle attività economiche.

Il diritto alla cancellazione dei dati e le attività economiche: una nuova visione del tempo. A margine della sentenza *Camera di commercio c. Manni*

The Right to Be Forgotten and Business Affairs: the Manni Case Before the ECJ

Manni
diritto all'oblio
iniziativa privata
impresa
dati personali

Serena Sileoni
Assegnista di ricerca in Diritto costituzionale presso l'Università degli Studi di Milano – Bicocca

Nei quaderni di Malte Laurids Brigge, Rilke scrive che bisogna dimenticare i ricordi, quando sono troppi, perché solo così emergono quelli che devono tornare.
Ai suoi tempi, non esistevano internet gli archivi digitali. Questi non corrono il problema di dover sgomberare la memoria per lasciar posto all'essenziale: archiviano tutto, dando una priorità algoritmica alle informazioni che non è necessariamente fedele all'importanza e all'attualità dei contenuti.
Si riaccende così, giuridicamente, il diritto all'oblio, in uno spazio temporale che si appiattisce su un infinito oggi: in un mondo che non ha pressoché più una memoria selettiva e breve, gli archivi diventano luoghi del presente, le notizie sono disponibili ora come allora, i database, on line e off line, risultano facilmente consultabili.
Possono quindi meritare tutela dal ricordo fatti e dati risalenti nel tempo, in un bilanciamento caso per caso tra esigenze di riservatezza e/o di immagine da un lato e di informazione e/o espressione dall'altro. Ciò vale per quello strumento oggi fondamentale di informazione che è l'indicizzazione informatica delle notizie, come ha ritenuto la Corte nella sentenza pilota" *Google Spain e Google* (C/131/12, 13 maggio 2014), ma vale anche per il mondo reale delle raccolte, virtuali e non, di dati.
È quanto emerge dalla pronuncia *Camera di commercio c. Manni* della Corte di giustizia europea (causa C-398-15, 9 marzo 2017), che, a tre anni da quella sentenza, ha precisato e chiarito la portata di un diritto non nuovo, ma rinnovato dalle possibilità tecnologiche attuali.
Già a metà degli anni Ottanta, prima che il problema fosse il mantenimento di notizie e dati non più attuali, il diritto all'oblio era infatti stato estrapolato da quello alla riservatezza/immagine come riconoscimento della pretesa a non veder ripubblicate notizie inerenti vicende e fatti passati, che il decorso del tempo non rendeva più di interesse pubblico. Si tratta dunque di un diritto già presente ma silente, che si è fatto più perentorio allorché la modalità di pubblicazione, archiviazione e digitalizzazione delle notizie e dei dati, praticamente sempre disponibili, ha reso concreto il conflitto tra le ragioni di essere dimenticati e quelle di essere informati. Non è più, quindi, l'episodio di un fatto o un dato che può tornare notizia, ma è la costante di un fatto o un dato che restano notizia solo perché è facile conservarne memoria pubblica.
Il caso Manni sembra meno innovativo nei fatti e di conseguenza anche nelle conclusioni di diritto, rispetto al caso Google Spain.
La sentenza risponde a un rinvio pregiudiziale della Corte di Cassazione italiana sull'interpretazione dell'art. 3 della direttiva 68/151/CEE del 9 marzo 1968 e suoi aggiornamenti, che ha uniformato le garanzie richieste negli Stati membri alle imprese in forma societaria, a tutela dei soci e dei terzi. Una direttiva abrogata da successivi interventi legislativi ma in vigore all'epoca dei fatti, che impegna gli Stati, tra le altre cose, a tenere un registro pubblico delle imprese da cui poter rintracciare una serie di informazioni utili a disposizione della collettività.
Il processo da cui muove il rinvio riguarda un ricorso proposto nel 2007 dall'amministratore unico di una società edile a responsabilità limitata, Manni appunto, che citava in giudizio la Camera di commercio di Lecce per la condanna alla cancellazione, anonimizzazione o blocco dei dati che collegano il ricorrente al fallimento di una precedente società. Secondo il ricorrente, infatti, le difficoltà riscontrate dalla sua nuova società nel vendere immobili derivavano dalla notizia del fallimento nel 1992 di una sua precedente attività, notizia ancora ricavabile dal registro delle imprese e utilizzata da una società specializzata nella raccolta e elaborazione di informazioni di mercato e nella valutazione del rischio.
La Corte di Cassazione, a cui la Camera di commercio aveva fatto ricorso contro la condanna da parte dei giudici di prime cure, ha chiesto quindi alla Corte di giustizia se il sistema di pubblicità attuato con il registro delle imprese, laddove esige che chiunque, senza limiti di tempo, possa conoscere i dati relativi alle persone fisiche ivi risultanti, sia coerente con il principio per cui i dati personali vadano conservati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per cui sono rilevati e trattati o se, al contrario, la legislazione europea imponga che i dati siano disponibili solo per un tempo limitato o nei confronti di destinatari determinati, in base a una valutazione casistica affidata al gestore del dato.
In altri termini, il giudice del rinvio chiede se l'art. 3 della direttiva 68/151 - secondo cui i dati di una società devono essere trascritti in ogni Stato in un registro accessibile - e l'art. 6 , par. 1, lett. e) della direttiva 95/46 - secondo cui i dati personali sono conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati - devono essere interpretati, alla luce degli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, nel senso che gli Stati membri possono, o addirittura devono, consentire alle persone fisiche che sono state membri degli organi societari e ai liquidatori di chiedere all'autorità incaricata della tenu-

ta del registro delle imprese, decorso un certo periodo di tempo dopo lo scioglimento della società interessata e in base ad una valutazione da compresi caso per caso, la limitazione all'accesso ai dati personali iscritti in tale registro, non necessariamente elettronico, che le riguardano.
La Corte quindi è investita di un quesito che, seppur attinente al diritto all'oblio già rispolverato nella sua accezione digitale con la sentenza Google Spain, amplia gli orizzonti di tale diritto all'ambito della tenuta dei dati in un registro pubblico, riportandolo dal mondo virtuale anche a quello reale. Da un lato, quindi, si profila il principio di pubblicità dei registri delle imprese, riconosciuto a partire dalla direttiva 68/151, dall'altro, il diritto di chiedere la cancellazione o il congelamento dei dati ai sensi degli artt. 6 e 14 della direttiva 95/46.
Come riconosciuto dalla Corte fin dagli anni '70, la direttiva 68/151 fornisce «una garanzia giuridica per le relazioni tra la società ed i terzi, in previsione di un incremento degli scambi commerciali fra gli Stati membri in seguito all'istituzione del mercato comune» *(Haaga GmbH*, C-32/74, 12 novembre 1974). Il bene tutelato dal registro delle imprese è la certezza dei rapporti giuridici, in particolare a tutela dei creditori, a beneficio della correttezza e agilità delle transazioni commerciali, e quindi del buon funzionamento degli scambi giuridici e economici. Pertanto, «la memorizzazione di dati nel registro delle imprese, in ottemperanza ad un obbligo legale in tal senso, costituisce un'attività svolta nell'interesse generale della certezza del diritto», come di recente ribadito nella sentenza *Compass-Datenbank (*C-138/11, 12 luglio 2012), dal momento che è finalizzato a tracciare il quadro completo della vita di un'impresa, a beneficio di chi abbia bisogno di conoscerne la storia. Ciò vale anche per le imprese cessate, o perché i rapporti pregressi non si sono ancora esauriti, o perché, nell'ambito di rapporti nuovi, si voglia avere informazioni sull'attendibilità delle persone fisiche attraverso una ricognizione della loro attività in precedenti società.
La pretesa di non dare più notizia di dati risalenti nel tempo si scontra quindi con il diritto ancora attuale all'informazione, cui sottosta l'esercizio di quello che è il potere pubblico di raccolta dati relativi a un'impresa.
Sembra qui di poter leggere una ragionevole presunzione della Corte, condivisa con l'Avvocato generale, per cui l'impegno nella vita economica implica la sua esposizione a esigenze di trasparenza: notizie e dati riguardanti l'attività economica di un soggetto sono meritevoli di essere conosciuti anche a distanza di tempo poiché la loro conoscibilità è strumentale a transazioni giuridiche e economiche corrette e stabili.
Tuttavia, la concordanza tra le conclusioni dell'Avvocato generale e la Corte non è piena. Per il primo, infatti, la consapevolezza che lo svolgimento di un'attività economica implichi un'esigenza «permanente» di trasparenza vale a far ritenere che non si possa poi invocare l'oblio, davanti all'esigenza di informazione dei terzi. È proprio per la natura dei dati contenuti nel registro delle imprese, per la finalità del sottostante trattamento e per una sorta di accettazione" implicita dei rischi" connessi alla trasparenza di questi dati che l'Avvocato nega la sussistenza di un autonomo diritto all'oblio.
La Corte accoglie l'interpretazione dell'Avvocato, ma alla fine apre alla possibilità di circostanze eccezionali. A suo giudizio, alla luce della diversità degli scenari possibili e della eterogeneità dei termini di prescrizione nei diversi Stati membri, «risulta impossibile identificare un termine univoco, a far data dallo scioglimento di una società, allo spirare del quale non sarebbe più necessaria l'iscrizione nel registro e la pubblicità dei dati citati. In tali circostanze, gli Stati membri […] non sono tenuti a garantire alle persone fisiche che hanno ricoperto ruoli dirigenziali nelle imprese, decorso un certo periodo di tempo dallo scioglimento di queste, la cancellazione dei dati personali che le riguardano iscritti nel registro o il congelamento nei confronti del pubblico.» Non si può tuttavia escludere, dice la Corte, «che possano sussistere situazioni particolari in cui ragioni preminenti e legittime connesse al caso concreto della persona interessata giustifichino, in via eccezionale, che l'accesso ai dati personali ad essa relativi iscritti nel registro sia limitato, decorso un periodo di tempo sufficientemente lungo dopo lo scioglimento della società di cui trattasi, ai terzi che dimostrino un interesse specifico alla loro consultazione.»
È un uso litotico del ragionare, quello della Corte, che finisce comunque per ampliare la portata di un autonomo diritto all'oblio opponibile al trattamento lecito di dati. Negando in via di principio la sussistenza di tale diritto nel caso di trattamento dei dati contenuti nel registro delle imprese, essa affida alle autorità nazionali la possibilità di ribaltare eccezionalmente la regola. Rimette infatti alle autorità nazionali che tengono i registri delle imprese la scelta di determinare il prevalere dell'interesse alla conoscenza dei dati, o di taluni dati, o piuttosto della pretesa a che essi siano dimenticati" (cancellati, congelati o limitati ad alcune categorie di interessati), valutando, caso per caso, l'eccezionalità della situazione che possa giustificare l' oblio", «per ragioni preminenti e legittime connesse alla loro situazione particolare, decorso un periodo di tempo sufficientemente

lungo dopo lo scioglimento della società interessata».
La sentenza può quindi quindi solo a una prima lettura poco rilevante, almeno rispetto alla precedente Google Spain. Stavolta, infatti, non è in discussione un autonomo *digital right to privacy* (che là, per giunta, viene riconosciuto come regola generale), ma più tradizionalmente è in discussione il bilanciamento tra l'attuale interesse alla conoscenza di un dato lecitamente trattato e il pregiudizio all'immagine e/o riservatezza derivante dal trattamento di quel dato.
Ciò non toglie che le conclusioni della sentenza si aprano a conseguenze importanti.
Nel dichiarare, infatti, che non esiste diritto all'oblio per i dati personali contenuti nel registro delle imprese, si riconosce comunque la possibilità che, in via eccezionale, il trascorrere del tempo possa consentire la limitazione dell'accesso a tali dati, in presenza di circostanze eccezionali.
Ponendo un tassello in più nella costruzione del diritto all'oblio, sembra importante quale considerazione dia la Corte del tempo nelle vicende economiche.
Il decorso del tempo determina essenziali differenze tra le ragioni giuridiche e quelle economiche (si pensi all'usucapione o alla prescrizione), motivate dalla necessità di garantire certezza ai titoli giuridici e agli scambi economici. Questa volta, invece, è proprio quest'ultima a sembrare di poter essere sacrificata, per quanto in via eccezionale, dal trascorrere del tempo. La trasparenza a tempo indefinito dei dati societari serve a garantire la certezza del diritto nelle relazioni tra le società e i terzi e a tutelare, in particolare, gli interessi dei terzi rispetto alle società che offrono come unica garanzia il proprio patrimonio sociale. Tali esigenze di certezza e di conoscenza possono esistere anche molti anni dopo che la società ha smesso di esistere, a beneficio sia di chi ha avuto con essa rapporti che possono ancora essere vantati, sia di chi, *ex novo*, voglia conoscerne le vicende, ad esempio perché voglia documentarsi sulle attività svolte dalle persone fisiche che ne hanno ricoperto ruoli dirigenziali. È quella certezza che, stavolta, seppur in via eccezionale, la Corte ritiene che possa essere sacrificata, con l'effetto di riconoscere comunque, per quanto in via interstiziale, un'autonoma rilevanza del diritto all'oblio di dati attinenti alle attività economiche.
Sarà, ancora una volta, il tempo e l'esperienza dei casi concreti a definire quali possano essere queste circostanze particolari. Il trattamento dei dati per la tenuta dei registri delle imprese sembra infatti rientrare, considerando la giurisprudenza sopra richiamata, tra gli adempimenti «di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento», oltre che «a fini di archiviazione nel pubblico interesse». Condizioni, queste, che ai sensi del nuovo regolamento sul trattamento dei dati personali non consentono di chiedere il diritto alla cancellazione (regolamento (UE) 2016/679, art. 17, comma 3).
Resta significativa, intanto, l'attività della Corte di scoperta e attualizzazione di diritti, o di loro manifestazioni, che erano rimasti, come nel caso dell'oblio, negli angoli dell'ordinamento, e che riaffiorano tramite l'esegesi dei giudici, nella costante opera di adeguamento del diritto alla realtà.

Note a Sentenza
Sezione Europa
Notes and Comments
Europe

Corte europea
dei diritti dell'uomo
European Court
of Human Rights

Corte europea dei diritti dell'uomo, 17 gennaio 2017, *Jankovskis v. Lituania*, ric. 21575/08

L'accesso a Internet non può essere considerato un diritto garantito dalla CEDU. Tuttavia, nell'ambito dell'art. 10 della Convenzione, l'uso del web può venire in rilievo come mezzo attraverso cui ottenere informazioni non altrimenti procacciabili, risultando in tale senso meritevole di protezione giuridica. Ciò è a maggior ragione sostenibile alla luce del fine perseguito dal cittadino: nel caso di specie, un detenuto chiedeva di potersi iscrivere ad un corso di laurea in giurisprudenza – per il quale l'uso del web si rivelava necessario – stimolando così il proprio percorso di riabilitazione e reintegrazione nella società.

«Understood as a right»: il diritto ad Internet tra mezzi, fini e rieducazione della pena

«Understood as a Right»: Access to the Internet and Rehabilitation of Prisoners

CEDU
accesso a internet
detenuti
riabilitazione
libertà di espressione

Fabio Ferrari
Assegnista di ricerca in Istituzioni di diritto pubblico, Università degli Studi di Verona

Sono ben noti i dilemmi che accompagnano il presunto diritto ad Internet: per taluni riguardano la specie (si ragiona sulla possibile natura di diritto fondamentale), per altri investono direttamente il genere (si dubita cioè, a monte, che esso sia addirittura qualificabile come diritto).
Sotto questi profili la pronuncia in esame appare assai interessante: sia perché emessa dalla Corte EDU, ossia dal giudice tenuto a garantire lo standard minimo convenzionale in tema di diritti fondamentali; sia perché la "fonte" della controversia è il carcere; luogo, quest'ultimo, ove la privazione della libertà personale non può pregiudicare irragionevolmente la garanzia di diritti strettamente connessi alla dignità dell'uomo.
I fatti.
Nel 2006 un detenuto lituano, già laureato in medicina prima della condanna, chiedeva al proprio Ministero (*Ministry of Education and Science*) informazioni sulla possibilità di ottenere una seconda laurea, questa volta in giurisprudenza e perlopiù con specializzazione in "diritti umani".
Il Ministero, nella propria replica, indicava un sito Internet pubblico, da esso gestito, denominato "*AIKOS*": ivi era possibile reperire ogni genere di informazione necessaria, tra cui quelle relative a corsi, insegnamenti, programmi e regole di ammissione; i contenuti venivano aggiornati quotidianamente, garantendone così l'attualità; inoltre, era consentito fruire di un canale diretto nel quale porre quesiti specifici, ricevendo consulenza *ad hoc*.
Il detenuto si rivolgeva dunque alle autorità competenti del carcere, chiedendo di poter accedere al servizio.
La risposta era tuttavia negativa, sulla base delle seguenti argomentazioni: 1) nella sua missiva, il Ministero non aveva preso in considerazione la particolare condizione – soggetto sottoposto a detenzione – del richiedente; 2) nessuna norma allora vigente nell'ordinamento lituano consentiva ai detenuti di accedere ad Internet o di avere un *account* di posta elettronica.
Replicava il detenuto che l'accesso al web per soggetti nella sua condizione non era né esplicitamente consentito, né esplicitamente precluso dal diritto in essere. Forte dunque della comunicazione del Ministero, ribadiva le proprie doglianze, decidendo però ora di adire il giudice amministrativo (*Kaunas Regional Administrative Court*).
Innanzi alla Corte, con memoria scritta, l'autorità del carcere argomentava ulteriormente la propria posizione, precisando quanto segue: 1] secondo la normativa vigente, i detenuti avevano il diritto di entrare in comunicazione con i vari soggetti della pubblica amministrazione, ma solo per tramite dell'ordinaria posta cartacea (art. 100 del *Code of the Execution of Sentences*); 2] l'uso di Internet avrebbe facilitato la progettazione e il coordinamento di attività illecite dall'interno del carcere: in esso, con la medesima finalità di prevenzione, era già precluso l'utilizzo della telefonia mobile e della radio; 3] ai detenuti era altresì impedito di comunicare tra loro mediante posta ordinaria: consentire l'utilizzo di Internet avrebbe di fatto eluso tale divieto; 4] le norme vigenti, infine, permettevano l'utilizzo del computer in carcere, precludendo però *in toto* l'accesso al web (art. 96 del *Code of the Execution of Sentences*) .
La Corte accoglieva pedissequamente tali argomenti.
Il detenuto, dal canto suo, ricorreva in appello, lamentando che la Corte di primo grado aveva ignorato il nucleo fondante della sua istanza, ossia il diritto all'educazione e all'accesso alle informazioni: come parametri, egli indicava l'art. 25 della Costituzione lituana, nonché gli artt. 10 e 14 della CEDU.
La controparte si limitava invece ad aggiungere che all'interno del carcere vi era una scuola di secondo grado pienamente operativa: per tramite di essa, il detenuto poteva avere accesso a copioso materiale educativo e culturale, senza alcun bisogno di Internet. Inoltre, il carcere offriva altresì corsi di "alfabetizzazione informatica", e il fatto che nel loro espletamento non fosse previsto l'accesso ad Internet non aveva mai dato luogo a dissidi o controversie di alcun genere.
Il giudice di secondo grado rigettava il ricorso, ribadendo in sintesi quanto già espresso nella pronuncia impugnata: non vi era una norma che esplicitamente consentiva l'uso di Internet; l'accesso al web, nonostante i propositi educativi del ricorrente, poteva degenerare in uso improprio e potenzialmente incline a scopi criminosi; al contempo, il diritto ad utilizzare il pc era *in*idoneo ad essere così estensivamente inteso da includervi, *de jure*, l'utilizzo di Internet.
A questo punto, il detenuto decideva di ricorrere innanzi alla Corte di Strasburgo.
Egli, lamentando la lesione dell'art. 10 CEDU, affermava che nessuna norma lituana, esplicitamente, proibiva l'accesso ad Internet; a tale preclusione, per stessa ammissione delle autorità lituane, si era arrivati conferendo un significato ampio alle fonti in vigore, le quali però se così interpretate si caratterizzavano per un'ambiguità prescrittiva non consona agli *standard* imposti dalla Corte EDU; inoltre, l'uso illecito del web (oltreché i pericoli correlati ad un suo capillare utilizzo in carcere) era del tutto estraneo alle intenzioni che animavano, fin da principio, la richiesta, avendo essa carattere

meramente educativo e culturale. Da ultimo, la proibizione era senz'altro sproporzionata, posto che, come indicato dallo stesso Ministero, il complesso delle informazioni richieste sul corso di laurea erano esaustivamente reperibili solo sul sito, il quale veniva continuamente aggiornato proprio al fine di garantirne la sistematica attualità di contenuti tipica del web.
L'autorità lituana sosteneva, al contrario, che con qualunque altro mezzo – stampa specializzata, pubblicazioni varie etc. – il detenuto poteva reperire le informazioni del caso, le quali erano comunque abbondantemente fornite dalle stesse strutture detentive; non vi era dunque alcuna sproporzione nel divieto imposto, essendo quest'ultimo, peraltro, necessario per perseguire efficacemente delicate finalità di sicurezza pubblica. Inoltre, la norma poteva a ragione considerarsi fondata – seppur solo implicitamente – sul diritto in vigore, come riconosciuto dalle Corti nazionali adite. In ogni caso, per fugare almeno *pro futuro* ogni dubbio sul punto, nel 2010 era intervenuta una modifica legislativa, la quale aveva definitivamente esplicitato tale precetto. Ancora, sottolineava come la giurisprudenza della Corte EDU sull'art. 10 non aveva mai imposto agli Stati forme particolari di accesso alle informazioni per i detenuti, evidenziando inoltre come in moltissimi Paesi contraenti era esplicitamente previsto un limite di accesso ad Internet in situazioni analoghe.
Questi i fatti. La parola, ora, alla Corte EDU.
I giudici di Strasburgo, anzitutto, rigettano un'eccezione di inammissibilità del resistente, della quale pare opportuno dare conto fugacemente poiché fondata, perlopiù, su mero tuziorismo: il Governo lituano sostiene difatti che il ricorrente non avrebbe esaurito i ricorsi nazionali interni, omettendo di agire innanzi al Ministero e chiamando in causa, direttamente, l'istituto di detenzione. La Corte, agevolmente, ribadisce un orientamento più volte espresso: ove vi siano *rimedi* giurisdizionali "paralleli", tali da perseguire il medesimo obiettivo e livello di protezione, spetta al ricorrente scegliere quale intraprendere, dovendo essi – ai fini dell'accesso alla Corte EDU – considerarsi alternativi, non certo complementari (cfr., *ex pluribus*, *Leja v. Latvia,* ric. 71072/01 (2011), § 46).
Nel merito, i giudici riconoscono (e ribadiscono: cfr. *Kalda v. Estonia*, ric. 17429/10 (2016), § 52) l'importanza sempre crescente assunta oggigiorno da Internet nella vita dei consociati, a maggior ragione nel convogliare informazioni di ogni genere: tuttavia, se tale ruolo consente di percepirlo come un diritto («*understood as a right*», § 62), non si può certo affermare che ai sensi dell'art. 10 CEDU esso debba essere considerato come tale. Ciò che viene in rilievo, al contrario, è il diritto dei cittadini – sancito nel medesimo articolo – di ricevere informazioni, il quale può essere limitato dagli Stati solo mediante apposita riserva di legge, per fini legittimi e necessari in una società democratica.
Il trittico di requisiti coglie in radice i termini del conflitto tra le parti: quanto al primo – la riserva di legge – la Corte afferma che il divieto di accesso ad Internet, pur non esplicitato dalla disciplina vigente al momento del sorgere della controversia, è da considerarsi sufficientemente chiaro. Se, argomentano i giudici, vi era una preclusione letterale per telefonia mobile e radio, se ne poteva tranquillamente dedurre il divieto anche per uno strumento ben più invasivo come Internet (§ 57).
Del pari da accogliere è la tesi del Governo in merito al secondo argomento, circa la legittimità dei fini che hanno motivato il divieto: la sicurezza all'interno e all'esterno del carcere, e più in generale la necessità di impedire i generalissimi «*disorder and crime*», giustificano la preclusione ai detenuti di un mezzo potenzialmente così pervasivo come Internet; questo, a maggior ragione in un Paese, la Lituania, nel quale le autorità hanno già dovuto affrontare numerose truffe telefoniche provenienti proprio dal carcere, come allegato dallo stesso Esecutivo (§§ 58, 14).
È, pero, in merito al terzo punto che la Corte esprime le considerazioni di maggior interesse: si tratta di una limitazione necessaria in una società democratica?
I giudici di Strasburgo sottolineano che il dettaglio di informazioni rinvenibile sul sito indicato dal Ministero al ricorrente non è, nemmeno lontanamente, paragonabile a quello ottenibile mediante altri mezzi più tradizionali: sia per la quantità di contenuti che il web – il programma *AIKOS* in questo caso particolare – mette a disposizione, sia per il fondamentale, continuo aggiornamento a cui il mezzo informatico è sottoposto. Internet, dunque, non entra in gioco frontalmente, come diritto protetto dall'art. 10 CEDU, bensì mediatamente, ossia come mezzo attraverso cui ottenere informazioni non altrimenti procacciabili, anche semplicemente avendo riguardo alla rapidità del contenuto informativo; basti pensare, si legge tra le righe, ai requisiti di accesso per il corso di laurea: ove questi variassero repentinamente, sarebbe senz'altro necessario – per il detenuto – averne notizia immediata, onde evitare confusione su quanto richiesto al momento dell'iscrizione. In gioco, evidenzia la Corte, non vi è soltanto un generico diritto all'informazione, bensì la riabilitazione del detenuto e la sua reintegrazione nella società («*It is not unreasonable to hold that such information was directly relevant to the applicant's interest in obtaining education, which is in turn of relevance for his rehabilitation and subsequent reintegration into society*»), (§§ 59, 60).

Alla controparte pubblica, pertanto, risulta imputabile un doppio profilo di responsabilità: da un lato, essa ha totalmente omesso ogni considerazione sulla natura del sito in questione; difatti, si tratta di una piattaforma pubblica, interamente gestita dal Ministero; ciò avrebbe dovuto rappresentare un punto fermo idoneo quantomeno a stemperare i rischi, in teoria perfettamente comprensibili, legati alla sicurezza e al proliferare di attività criminose. In secondo luogo, si rimprovera all'autorità nazionale di aver preso in considerazione il "diritto" ad Internet in quanto tale, *ex se*, senza comprendere come in realtà esso sia "solo" uno strumento finalizzato ad un fine particolare, quello educativo, vero obiettivo del ricorrente.
Per tutti questi motivi, dunque, la Corte ritiene che il pregiudizio patito dal ricorrente a cagione del mancato accesso ad Internet per fini educativi non sia rispettoso della prescrizione *ex* art. 10 CEDU.
La violazione è dunque accertata, anche se la particolarità delle circostanze induce la Corte a non irrogare alla Lituania la sanzione economica richiesta dal detenuto.
Tuttavia, la pronuncia appare importante: secondo la CEDU Internet non è ancora un diritto in senso stretto, ma può essere uno strumento attraverso cui esercitare diritti fondamentali. Un mezzo dunque, non un fine.
Per i sostenitori di questo nuovo diritto può sembrare un risultato di poco conto: senza voler dare alcun giudizio sul tema, andrebbe però tenuto presente che a certe condizioni e a lungo andare il mutamento di mezzi in fini è assai probabile, secondo una riflessione cristallizzata nel pensiero occidentale da Hegel ma risalente, a quanto pare, già al mitico Eubulide.
E sono proprio piccole brecce come queste a dare il là, in potenza, a tali mutamenti.

Corte europea dei diritti dell'uomo, 9 marzo 2017, ric. 74742/14, *Rolf Anders Daniel Pihl c. Svezia*

Secondo la Corte europea dei diritti dell'uomo (CEDU), costituisce una violazione dell'art. 10 la condanna per diffamazione del gestore di un sito Internet quando sia originata dalla pubblicazione di un commento di un terzo rimasto anonimo, e il gestore del sito abbia provveduto tempestivamente alla sua rimozione, a seguito della segnalazione della persona offesa.

La Corte di Strasburgo torna sulla responsabilità del gestore del sito: il caso *Rolf Anders Daniel Pihl c. Svezia*

The Court of Strasbourg Back on Website Owners' Liability: the Rolf Anders Daniel Pihl V. Sweden Case

responsabilità degli ISP
diffamazione
libertà di espressione
CEDU
anonimato

Silvia Vimercati
Dottoranda di ricerca in Diritto pubblico, Università degli Studi di Milano - "Bicocca"

La ricerca di un punto di equilibrio tra tutela dei diritti della personalità e libertà di espressione sul web e, più in particolare, l'individuazione dei confini della responsabilità dei fornitori di servizi in rete per gli scritti pubblicati da soggetti terzi sono temi che da tempo occupano giudici e legislatori, nazionali ed europei. In particolare, è ancora aperto l'interrogativo se e a quali condizioni al gestore di un sito internet possa essere attribuita una qualche forma di responsabilità per i contenuti offensivi immessi in rete dagli utenti.

La Corte europea dei diritti dell'uomo, con la sentenza *Rolf Anders Daniel Pihl c. Svezia* del 9 marzo 2017 (ric. 74742/2014), torna ad affrontare la questione, stabilendo che il gestore di un blog non può essere ritenuto responsabile per la pubblicazione di un commento diffamatorio immesso da un utente rimasto anonimo, sempre che non contenga espressioni che trasmodino nell'incitamento all'odio e alla violenza e abbia provveduto tempestivamente alla sua rimozione, a seguito della segnalazione della persona offesa.

Dato conto del principio di diritto espresso dalla Corte, questa in breve la vicenda che ha originato la decisione in commento: nel settembre 2011, in un blog gestito da una piccola associazione senza scopo di lucro, veniva pubblicato un post in cui si riferiva che un cittadino svedese, Rolf Anders Daniel Pihl, era membro di un partito nazista. Il giorno successivo, un utente utilizzando uno pseudonimo, inseriva un commento a tale scritto, accusando la medesima persona di essere anche un abituale consumatore di sostanze stupefacenti. Pochi giorni più tardi, la persona offesa pubblicava a sua volta un commento chiedendo la rimozione di entrambi gli scritti in quanto veicolavano informazioni offensive e non corrispondenti al vero. A quel punto, l'associazione prontamente provvedeva a rimuovere i contenuti asseritamente diffamatori, pubblicando altresì un post di scuse. Ciononostante, anche in ragione del fatto che attraverso i motori di ricerca i due contenuti fossero ancora rinvenibili, il soggetto leso citava in giudizio il gestore del sito, chiedendo il risarcimento per la pubblicazione del post e per l'omesso controllo preventivo in relazione al commento immesso dall'utente anonimo. I giudici interni, in primo grado e in appello, respingevano sia la domanda di risarcimento relativa allo scritto redatto dallo stesso gestore sia quella relativa al commento pubblicato dal soggetto rimasto anonimo: la prima per una ragione di tipo processuale, la seconda perché nell'ordinamento svedese non vi era alcuna norma che potesse fondare una responsabilità del blogger per la mancata rimozione di un contenuto diffamatorio immesso da terzi prima della segnalazione dell'interessato. Successivamente, il soggetto leso si rivolgeva al *Chancellor of Justice*, organo di garanzia dell'ordinamento svedese che vigila sulla corretta applicazione della legge, il quale tuttavia statuiva che nel caso di specie non vi fosse stata alcuna violazione dell'art. 8 della Convenzione europea dei diritti dell'uomo, ossia del diritto alla riservatezza e alla reputazione.

Una volta esauriti tutti i rimedi interni, il soggetto leso presentava ricorso alla Corte di Strasburgo, affermando di aver subito una lesione dei diritti della personalità tutelati dall'art. 8 della Convenzione, a causa della assenza nell'ordinamento svedese di una disposizione che consentisse di ascrivere una qualche forma di responsabilità in capo al gestore del sito.

La Corte dei diritti muove innanzitutto dalla nozione di "vita privata" contenuta nell'art. 8 della CEDU, rammentando come nell'alveo di tale disposizione debbano essere ricondotti una serie di diritti della persona che vanno dalla identità personale, al nome, all'immagine, all'integrità fisica e psichica fino ad arrivare ai diritti dell'onore e della reputazione.

Tuttavia, perché possa ravvisarsi una violazione di tale norma occorre che l'attacco alla reputazione raggiunga un certo livello di gravità e l'offesa arrecata sia idonea a pregiudicare in concreto il diritto al rispetto della vita privata. Da qui, la Corte di Strasburgo, pur riconoscendo che il contributo in esame presentasse dei profili offensivi, rileva che non conteneva espressioni che costituivano incitamento all'odio e alla violenza; circostanza che, secondo la giurisprudenza della Corte, dovrebbe indurre a riconoscere maggior ampiezza alla libertà tutelata dall'art. 10 della Convenzione.

Fatte tali premesse, la Corte riprende un passaggio della sua prima decisione in materia [*Delfi c. Estonia* del 2013 (ric. 64569/09)[1], confermata dalla Grande Camera con sentenza del 16 giugno 2015], con la quale, come noto, era giunta ad un esito almeno *prima facie* opposto al caso che ci occupa, statuendo che lo Stato membro non era incorso in una violazione dell'art. 10 per aver condannato un portale web al risarcimento dei danni derivanti dalla pubblicazione di commenti anonimi ritenuti offensivi e incitanti all'odio e alla violenza nei confronti di soggetti terzi. In particolare, anche nella decisione in commento, viene ribadito il principio di diritto secondo cui, laddove lo Stato abbia individuato un punto di equilibrio tra diritto al rispetto della vita privata e libera manifestazione del pensiero in linea con i criteri stabiliti dalla giurisprudenza della Corte, quest'ultima potrebbe far prevalere la sua visione rispetto a quella dei giudici interni solo in caso di[2] ragioni

[1] Su cui cfr. la nota di G.E. Vigevani, *La responsabilità civile dei siti per gli scritti anonimi: il caso Delfi c. Estonia*, *in Quaderni costituzionali*, 2014, 457 ss.

[2] Su cui si rinvia a S. Vimercati, *Magyar c. Ungheria: la Corte europea ritorna sulla responsabilità dei portali web*, *in Quaderni costituzionali*, 2016, 393 ss.

particolarmente forti.

Delineati così i confini del proprio intervento, i giudici di Strasburgo utilizzano i criteri fissati dalla giurisprudenza - da ultimo nella sentenza *Magyar Tartalomszolgáltatók Egyesülete e Index.hu Zrt c. Ungheria* del 2016 (ric. 22947/13), per operare tale valutazione, ossia: il contesto e il contenuto dei contributi incriminati, le misure adottate per prevenire o rimuovere i commenti lesivi dei diritti altrui, la responsabilità degli effettivi autori degli scritti in alternativa a quella del provider e, infine, la condotta tenuta dall'intermediario.

Partendo da tale ultimo elemento, la Corte rileva innanzitutto che il gestore del sito, a seguito della richiesta del ricorrente, aveva provveduto tempestivamente alla rimozione del contributo ritenuto offensivo, pubblicando altresì uno scritto di scuse. In più, il sito, benché non avesse un sistema di filtro preventivo, aveva un *disclaimer* mediante il quale declinava ogni responsabilità per quanto inserito da soggetti terzi e aveva predisposto un sistema per poter segnalare e chiedere la rimozione dei commenti offensivi, strumento ritenuto dalla giurisprudenza in materia adeguato per tutelare i diritti della personalità dei soggetti eventualmente lesi.

Quanto all'identificazione dell'autore effettivo dello scritto, i giudici valorizzano la circostanza che in concreto non vi era nel caso di specie un anonimato assoluto, in quanto la persona offesa conosceva l'indirizzo IP del computer utilizzato per inserire gli scritti nel sito e, ciononostante, non si era in alcun modo attivato per individuare il soggetto che aveva redatto e diffuso i commenti diffamatori. In sostanza, una certa rilevanza ai fini della decisione sembra averla avuta il fatto che il ricorrente, pur avendo le informazioni che gli avrebbero consentito di risalire al vero autore della condotta asseritamente diffamatoria, abbia scelto di rivolgersi all'autorità giudiziaria per ottenere tutela tramite l'attribuzione di una responsabilità in capo ad un soggetto diverso da colui che aveva concretamente pubblicato le affermazioni offensive.

Da ultimo, e pare essere proprio questo il dato su cui pone maggiormente l'accento la Corte in armonia con quanto statuito nel suo ultimo precedente, far ricadere la responsabilità in modo automatico sui gestori dei siti può avere conseguenze assai negative sulla loro attività, fino a indurli a chiudere lo spazio dedicato ai commenti degli utenti, determinando così un *chilling effect* sulla libertà di espressione in rete. Di qui, dunque, l'affermazione del corretto bilanciamento degli interessi in gioco operato dai giudici nazionali e la dichiarazione di inammissibilità del ricorso.

La decisione in commento offre un nuovo contributo all'individuazione di un corretto bilanciamento tra libertà di manifestazione del pensiero in rete e tutela dei diritti della personalità degli individui, ma soprattutto sembra confermare quell'indirizzo teso a porre un argine ai tentativi di responsabilizzazione degli intermediari.

Non si incorra in equivoco: come dal primo precedente in materia, il già citato caso *Delfi c. Estonia*, non poteva essere ricavata una automatica responsabilità del provider per gli scritti immessi dagli utenti, in modo analogo appare peregrino ritenere che sia la successiva pronuncia del 2016, *Magyar c. Ungheria*, sia quella presa in esame con il presente scritto consentano di desumere una regola generale di totale irresponsabilità. Si cadrebbe infatti in errore se si dimenticasse lo specifico ruolo che la Corte di Strasburgo è chiamata a ricoprire e si rileggesse la sentenza prescindendo dalle peculiarità del caso concreto e traendone un principio valido universalmente.

A prescindere dagli esiti diversi, nella ricerca di un punto di equilibrio tra gli interessi in gioco, pare possa rinvenirsi un filo rosso che lega tutte le pronunce della Corte europea in tema di responsabilità dei fornitori di servizi in rete: va esclusa l'attribuzione automatica di responsabilità in capo a tali soggetti per gli scritti immessi dagli utenti, ma è possibile che siano chiamati a risponderne qualora contengano affermazioni che incitino all'odio e alla violenza e l'intermediario, dopo aver ricevuto notizia della loro pubblicazione, non provveda tempestivamente a eliminarli.

Note a Sentenza
Sezione Italia
Notes and Comments
Italy

Corte costituzionale, 24 gennaio 2017, n. 20

Con la sentenza 20/2017, la Corte costituzionale dichiara non fondate le questioni di legittimità costituzionale dell'art. 266 c.p.p. e degli artt. 18 (nel testo anteriore alle modifiche introdotte dalla l. 95/2004) e 18-*ter* della l. 354/1975, sollevate dalla Corte di assise di appello di Reggio Calabria, in riferimento agli artt. 3 e 112 Cost. giacché – a differenza di quanto accade per conversazioni, comunicazioni telefoniche e telecomunicazioni – non consentono di captare in maniera occulta la corrispondenza epistolare dei detenuti. Secondo la Consulta, è invece possibile prevedere forme diverse di controllo della corrispondenza dei detenuti, differenziandole sulla base del mezzo comunicativo utilizzato. Infatti, poiché i varî mezzi di comunicazione possiedono un "diverso grado di materializzazione", il legislatore può prevedere differenti mezzi di ricerca della prova, tecnicamente confacenti alla diversa natura del mezzo utilizzato per la comunicazione, anche al fine di garantire i residui margini di libertà dei soggetti sottoposti a detenzione in carcere. Tali scelte, rientrando nella discrezionalità del legislatore, potranno essere riviste ma solo nel rispetto delle riserve di legge e di giurisdizione previste dall'art. 15 Cost. e in osservanza dei canoni di ragionevolezza e di proporzionalità.

La Corte costituzionale non dà il suo avallo alle "intercettazioni" della corrispondenza epistolare dei detenuti ma non esclude futuri sviluppi

The Italian Constitutional Court Against the Interception of Prisoners' Correspondence

corrispondenza
comunicazione
intercettazioni
detenuti
Corte costituzionale

Daniele Coduti
Ricercatore confermato di Diritto costituzionale, Università degli Studi di Foggia

1. Le "intercettazioni" della corrispondenza epistolare dei detenuti. – 2. La decisione della Corte costituzionale: l'art. 15 Cost. – 3. Segue: i diritti dei detenuti. – 4. I possibili sviluppi dopo la decisione della Consulta.

1 Le "intercettazioni" della corrispondenza epistolare dei detenuti

La possibilità di controllare la corrispondenza epistolare dei detenuti è una questione foriera di contrasti, anche giurisprudenziali. La disciplina vigente consente di intercettare conversazioni, comunicazioni telefoniche e altre forme di telecomunicazioni per taluni reati, ma senza far riferimento alla corrispondenza epistolare (art. 266 c.p.p.); per quest'ultima, gli artt. 254 e 353 c.p.p. prevedono il sequestro ma non l'intercettazione all'insaputa del mittente e del destinatario. Con specifico riferimento ai detenuti, la l. 354/1975 consente di controllarne la corrispondenza ma con l'apposizione di un segno idoneo a comprovare l'avvenuto controllo (cd. visto di controllo), il che rende l'attività di investigazione conoscibile ai soggetti coinvolti nella comunicazione.

Pur alla luce di tale quadro normativo, è accaduto che la corrispondenza spedita o ricevuta da un imputato detenuto in carcere non sia stata sequestrata ai sensi dell'art. 254 c.p.p. bensì copiata dalla polizia giudiziaria – previa autorizzazione del giudice per le indagini preliminari – e recapitata ai destinatari senza che questi ultimi potessero venire a conoscenza dell'attività investigativa compiuta, con lo scopo di utilizzare in giudizio il materiale probatorio così acquisito. Questa attività, che parrebbe configurare una sorta di intercettazione "atipica", non è però contemplata dalle norme sopra richiamate, dunque non sarebbe consentita e le prove eventualmente acquisite dovrebbero essere inutilizzabili in giudizio[1]. L'interpretazione di tale disciplina, tuttavia, ha dato luogo a un contrasto giurisprudenziale[2] che è giunto sino alla Corte costituzionale, investita della questione dalla Corte d'assise d'appello di Reggio Calabria[3].

Secondo il giudice *a quo*, il complesso normativo in materia, anche alla luce della giurisprudenza di legittimità, sarebbe irragionevole e, dunque, in contrasto con l'art. 3 Cost., poiché, sottoponendo a una disciplina diversa le intercettazioni telefoniche e quelle epistolari, produrrebbe un'ingiustificata disparità di trattamento; tale disparità riguarderebbe anche il trattamento dell'indagato detenuto rispetto a quello non detenuto, perché «attribuirebbe una sorta di status privilegiato» al primo[4]. Secondo l'Autorità giudiziaria rimettente, infatti, lo stato detentivo, da ritenersi irrilevante ai fini investigativi, si porrebbe così quale fattore ulteriormente limitativo delle indagini, in quanto imporrebbe all'autorità procedente, per la corrispondenza, oneri comunicativi incompatibili con la necessità di assicurare la segretezza delle indagini, che non sono richiesti per i soggetti non privati della libertà personale. L'irragionevolezza di tale disciplina risulterebbe ancor più evidente a fronte del fatto che la legislazione in vigore consentirebbe le intercettazioni ambientali di colloqui con persone in visita al detenuto, video-riprese che permettano di cogliere segni occulti o altri gesti comunicativi, non meno invasivi della privatezza e della segretezza delle comunicazioni.

Il giudice *a quo*, poi, ritiene che la disciplina impugnata contrasti anche con l'art. 112 Cost., poiché l'impossibilità di intercettare le comunicazioni epistolari dei detenuti renderebbe «ineffettivo» il principio di obbligatorietà dell'azione penale in relazione alle ipotesi considerate, producendo una «irragionevole menomazione dell'attività investigativa costituzionalmente attribuita agli uffici di Procura»; ciò anche perché la completa individuazione degli elementi e delle fonti di prova – che sarebbe compromessa dall'esclusione dell'intercettazione epistolare – costituirebbe il «precipitato naturale» del principio codificato dall'art. 112 Cost., che ne risulterebbe quindi parimenti compromesso.

[1] Cfr. Cass., sez. un.,19 aprile 2012, n. 28997.

[2] Sulla giurisprudenza della Corte di Cassazione si v. A. Chelo Manchìa, *Acquisizione di corrispondenza o "intercettazione epistolare"?*, in *Diritto penale e processo*, 8/2007, 1049 ss., C. Fanuele, *Sequestro di corrispondenza proveniente da persona detenuta: una forma d'intercettazione "mascherata"*, *ibidem*, 4/2010, 465 ss., e O. Murro, *Il rapporto tra controllo e garanzie della corrispondenza*, *ivi*, 6/2010, 706 ss.

[3] Ord. 8 febbraio 2016, n. 67, dalla quale sono estratte le frasi tra caporali.

[4] L'espressione è ripresa dall'ordinanza del giudice *a quo*, che richiama Cass. pen., sez. II, 3 aprile 2014, n. 15197.

2 La decisione della Corte costituzionale: l'art. 15 Cost.

Con la sentenza 20/2017 la Consulta ha rigettato la questione di legittimità costituzionale, con una pronuncia che appare interessante con riferimento sia alla libertà prevista dall'art. 15 Cost. sia ai diritti dei detenuti.

Quanto al primo aspetto, la formulazione della citata disposizione costituzionale fa riferimento all'inviolabilità della libertà e della segretezza della «corrispondenza e di ogni altra forma di comunicazione», consentendo di tutelare le comunicazioni effettuate con qualunque mezzo sia messo a disposizione dall'evoluzione tecnologica, dunque anche con mezzi diversi da quelli noti nel momento in cui si redigeva la Costituzione. L'ampiezza di tale garanzia, tuttavia, non comporta che la scelta del mezzo con cui comunicare sia irrilevante, poiché le eterogenee caratteristiche degli strumenti di comunicazione possono giustificare un trattamento giuridico diversificato. Secondo la Corte costituzionale, infatti, tali mezzi sono caratterizzati da un «diverso grado di materializzazione»[5], che può giustificare un diverso trattamento giuridico delle comunicazioni con essi veicolate. Con specifico riferimento all'interesse – costituzionalmente protetto – della collettività alla repressione degli illeciti penali, allora, non è irragionevole che il legislatore preveda modalità di ricerca della prova differenziate sulla base del diverso mezzo comunicativo utilizzato, ovvero, il sequestro per la comunicazione realizzata attraverso un mezzo cartaceo e l'intercettazione per la comunicazione realizzata attraverso mezzi visivi, acustici o elettronici; ciò che conta, infatti, è che le limitazioni della libertà contemplata dall'art. 15 Cost. «siano rispettose della riserva assoluta di legge e di giurisdizione e siano volte alla tutela di un altro diritto o al perseguimento di un altro interesse costituzionalmente rilevante, in ossequio ai principi di idoneità, necessità e proporzionalità»[6].

La decisione della Consulta deve far riflettere sulla libertà enunciata dall'art. 15 Cost. perché, sebbene la disposizione costituzionale consenta di tutelare le comunicazioni indipendentemente dal mezzo utilizzato, la sua attuazione può essere differenziata sulla scorta del grado di materializzazione di tale mezzo, sicché la distinzione tra i mezzi "tradizionali" (come la corrispondenza epistolare) e quelli tecnologicamente più avanzati (come quelli telematici) è tutt'altro che irrilevante perché può far ricadere le comunicazioni sotto una diversa disciplina giuridica e diverse forme di controllo, influendo, così, anche sulla scelta dello strumento da utilizzare per comunicare.

Sempre in merito all'art. 15 Cost., la sentenza 20/2017 rileva anche con riferimento alla distinzione tra la libertà e la segretezza della corrispondenza, sulla quale la dottrina ha assunto posizioni contrastanti, soprattutto in merito alla possibilità di prevedere interventi limitativi solo di uno dei due aspetti della comunicazione[7]. Libertà e segretezza sono indubbiamente connesse nell'art. 15 Cost., tuttavia, la decisione della Consulta sembra avvalorare l'ipotesi secondo cui i limiti alla corrispondenza possono riguardare anche uno solo dei due aspetti considerati, poiché possono esservi misure limitative della libertà di corrispondenza che non ne violano la segretezza (come il sequestro della corrispondenza epistolare) e misure che ne violano la segretezza ma non la libertà (come le intercettazioni delle comunicazioni telematiche). Anche in queste ipotesi, lo strumento utilizzato per comunicare non appare irrilevante: in primo luogo, perché le sue caratteristiche potrebbero non consentire di intervenire su uno solo dei profili della comunicazione tutelati dall'art. 15 Cost.; in secondo luogo, perché la comunicazione può esporsi a misure limitative di natura diversa, derivanti anche dall'evoluzione tecnologica dei mezzi di comunicazione e degli strumenti di intercettazione; infine, perché le peculiarità di ciascun mezzo di comunicazione possono comportare una differenziazione della loro disciplina giuridica. La scelta del legislatore in merito alle modalità di limitazione delle comunicazioni, inoltre, può essere influenzata dall'esigenza di preservare un margine residuo di riservatezza per quei soggetti che hanno uno *status* particolare, come i detenuti.

La sentenza induce a meditare anche sulla connessione tra l'art. 15 Cost. e gli altri diritti costituzionali. La scelta dell'Assemblea costituente di disciplinare nell'art. 15 Cost. la libertà di comunicazione e nell'art. 21 Cost. quella di manifestazione del pensiero è stata oggetto di un intenso dibattito in dottrina, volto a individuare gli elementi idonei a differenziare i due fenomeni[8]. L'evoluzione della tecnologia, però, attenua sempre più la differenza tra le due libertà, poiché l'utilizzo del medesimo strumento può essere ricondotto all'una o all'altra sulla scorta delle modalità di

[5] Così Corte cost., sent. 20/2017, pt. 3.5 cons. dir.
[6] Così, ancora, Corte cost., sent. 20/2017, pt. 3.3 cons. dir.
[7] Sul punto si v. quantomeno P. Caretti, *Corrispondenza (libertà di)*, in *Digesto delle discipline pubblicistiche*, IV, Torino, 1989, 201 ss., A. Pace, *Art. 15*, in G. Branca (a cura di), *Commentario della Costituzione*, Bologna-Roma, 1977, 85 ss., e M. Olivetti, *Brevi note in materia di libertà di comunicazione*, in *Giurisprudenza costituzionale*, 1996, 3863 ss..
[8] Basti ricordare che C. Esposito, *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Milano, 1958, 23, nt. 45, riteneva la libertà di comunicazione una sottospecie di quella di manifestazione del pensiero.

impiego scelte di volta in volta (è il caso, ad es., dei *social network*); inoltre, alcuni strumenti messi a disposizione dal progresso tecnologico consentono di incidere contemporaneamente su più libertà (si pensi ai cd. *trojan horses*, capaci di effettuare simultaneamente intercettazioni ambientali e telematiche, riprese video, geolocalizzazioni, etc.)[9]. Questa evoluzione rischia di porre in crisi i paradigmi congegnati dai costituenti a tutela di alcuni diritti costituzionali, poiché essi possono diventare inadatti a fornire una protezione adeguata contro le pervasive capacità di limitazione di tali diritti offerte dai nuovi strumenti tecnologici, rafforzando, di conseguenza, le tesi di quanti ritengono opportuno novellare la Costituzione su tali profili[10]. Per di più, lo sviluppo delle comunicazioni via internet e la gestione dei relativi dati da parte di aziende a carattere internazionale pongono sempre più in dubbio l'efficacia di una regolamentazione esclusivamente nazionale di tali fenomeni, facendo emergere l'esigenza di una disciplina transnazionale[11].

3 Segue: i diritti dei detenuti

Passando alla parte della pronuncia che si sofferma sui diritti dei detenuti, la Corte costituzionale fa due considerazioni preliminari. Innanzitutto, afferma che la disciplina vigente dell'art. 18-*ter* della l. 354/1975 (novellata dalla l. 95/2004) «rappresenta un delicato punto di equilibrio raggiunto dal legislatore, anche a seguito di numerose decisioni della Corte europea dei diritti dell'uomo in cui l'Italia veniva ripetutamente condannata per violazione degli artt. 8 e 13 CEDU»[12]. In secondo luogo, la Consulta ricorda che «la tutela costituzionale dei diritti fondamentali opera anche nei confronti di chi è stato sottoposto a legittime restrizioni della libertà personale, sia pure con le limitazioni imposte dalla particolare condizione in cui versa: "Chi si trova in stato di detenzione, pur privato della maggior parte della sua libertà, ne conserva sempre un residuo, che è tanto più prezioso in quanto costituisce l'ultimo ambito nel quale può espandersi la sua personalità individuale"»[13].

Quello detentivo, dunque, non è uno "*status* privilegiato", bensì una legittima limitazione dei diritti di un soggetto che deve comunque rispettare l'art. 27 Cost., secondo il quale le pene non possono consistere in trattamenti contrari al senso di umanità e devono tendere alla rieducazione del condannato. Il perseguimento di tale fine richiede – tra l'altro – che il detenuto possa intrattenere delle relazioni sociali con i familiari e con altri soggetti esterni all'istituto penitenziario, relazioni che – stante la situazione di reclusione – possono essere favorite proprio dalla corrispondenza epistolare, la quale, di conseguenza, deve essere tutelata anche per i detenuti, pur con i limiti connessi alla loro condizione[14].

Occorrer considerare, inoltre, che uno dei diritti maggiormente sacrificati in carcere è quello alla *privacy*, di cui l'art. 15 Cost. costituisce uno dei fondamenti costituzionali; sicché, preservare un margine di segretezza della corrispondenza epistolare significa anche tutelare i residui margini di riservatezza del detenuto. Nella società contemporanea tale osservazione potrebbe apparire paradossale, poiché (soprattutto utilizzando i *social network*) si tende a diminuire volontariamente gli aspetti della propria vita coperti da riserbo[15]; tuttavia, proprio le ridotte capacità di disporre della propria sfera di riservatezza da parte dei detenuti possono giustificare una particolare tutela delle modalità attraverso le quali garantire la (pur minima) *privacy*.

Dunque, la Corte costituzionale riconosce che anche per il detenuto residuino dei margini di tutela della libertà di corrispondenza, sebbene essi siano limitati sia dalla condizione di reclusione sia dalle legittime esigenze investigative volte alla repressione dei reati, che devono comunque

[9] Al riguardo si v. C. Pinelli, *Sull'ammissibilità di restrizioni alla libertà di domicilio e alla libertà di comunicazione tramite "virus di Stato"*, in *Diritto penale contemporaneo*, 2017, spec. 4, e S. Romano - C. Sorio, *L'utilizzo dei c.d.* trojan horses *nelle indagini penali e la tutela "progressiva" della libertà e segretezza delle comunicazioni*, in *Law and Media WorkingPapers Series,* 14/2016.

[10] Cfr. M.Orofino, *La libertà di espressione tra Costituzione e Carte europee dei diritti. Il dinamismo dei diritti in una società in trasformazione*, Torino, 2014, spec. 141.

[11] In questo senso già L. Scaffardi, *La comunicazione in rete e i diritti della persona: tra rischi e opportunità*, in A. D'Aloia (a cura di), *Diritti e Costituzione*, Milano, 2003, 67 ss.

[12] Così Corte cost., sent. 20/2017, pt. 4 cons. dir., che richiama CEDU, *Calogero Diana c. Italia*; ric. 15211/89 (1996); *Domenichini c. Italia*, ric.15943/90 (1996); *Labita c. Italia*, ric. 26772/95 (2000); *Di Giovine c. Italia,* ric. 8229/02 (2005); *Ospina Vargas c. Italia,* ric. 40750/98 (2004); si v. anche CEDU, *Di Giacomo c. Italia*, ric. 25522/03 (2008), nella quale la Corte di Strasburgo prende atto della riforma del 2004 ma osserva che essa non rimedia alle violazioni verificatesi prima della sua entrata in vigore, riscontrando, dunque, una violazione dell'art. 8 CEDU. La riforma non pare comunque aver dissipato tutte le perplessità sulla disciplina in questione: si v. L. Filippi, *Il controllo sulla corrispondenza dei detenuti*, in *Diritto penale e processo*, 10/2004, 1200 ss., E.Gianfrancesco, *Profili ricostruttivi della libertà e segretezza di corrispondenza e comunicazione*, in *Diritto e Società*, 2/2008, 231, e C. Mainardis, *Art. 15*, in S. Bartole - R. Bin (a cura di), *Commentario breve alla Costituzione Paladin-Crisafulli*, II ed., Padova, 2008, 125, e A. Martufi, *Diritti dei detenuti e spazio penitenziario europeo*, Napoli, 2015, 120-121. Per la disciplina anteriore alla riforma, si v. le critiche di M. Ruotolo, *Diritti dei detenuti e Costituzione*, Torino, 2002, 88 ss.

[13] Così C. cost., sent. 20/2017, pt. 4.1 cons. dir.

[14] Invero, la condizione di detenuto del mittente o del destinatario della comunicazione rientra tra i casi comunemente individuati dalla dottrina come quelli dai quali deriva una limitazione della relativa libertà: cfr., ad es., P. Barile - E. Cheli, *Corrispondenza (Libertà di)*, in *Enciclopedia del diritto*, X, Milano, 1961, 751-752, e C. Troisio, *Corrispondenza (libertà e segretezza della)*, in *Enciclopedia giuridica*, IX, Roma, 1988, 8.

[15] In proposito, si v. le osservazioni di Z. Bauman, *Danni collaterali*, Bari, 2011, 98-99.

tener conto dei principî espressi dall'art. 27 Cost. Trovare un equilibrio tra le diverse esigenze in questione è un compito rimesso al legislatore, il quale ha individuato la soluzione nella disciplina del cd. visto di controllo, che alla Consulta non appare né manifestamente irragionevole né arbitraria. Secondo la Corte, peraltro, il legislatore può cercare una soluzione differente, prevedendo, ad esempio, mezzi di captazione occulta dei contenuti della comunicazione dei detenuti che non interrompano il flusso comunicativo, come già accaduto per le comunicazioni telematiche e informatiche; si tratta, però, di «delicate scelte discrezionali, non costituzionalmente necessitate, che, come tali, rientrano a pieno titolo nelle competenze e nelle responsabilità del legislatore», che devono comunque essere compiute nel rispetto «delle riserve di legge e di giurisdizione previste dall'art. 15 Cost. e in osservanza dei canoni di ragionevolezza e di proporzionalità»[16].

4 I possibili sviluppi dopo la decisione della Consulta

La sentenza 20/2017 appare sostanzialmente da condividere almeno per due ragioni: perché ricorda la necessità di rispettare i diritti dei detenuti e perché cerca di porre termine a un conflitto giurisprudenziale che si protrae da tempo. Invero, non sarà semplice valutare appieno gli effetti di tale pronuncia, giacché se, per un verso, è probabile che i giudici penali vi si adegueranno, rinunciando all'utilizzo processuale del materiale probatorio ottenuto attraverso modalità di intercettazione "atipiche", per altro verso sarà particolarmente arduo appurare se essa riuscirà ad avere un impatto sulle prassi interne all'amministrazione penitenziaria, che non sono agevolmente verificabili.

La pronuncia della Corte costituzionale, peraltro, non esclude sviluppi futuri, che potrebbero dipendere dall'evoluzione tecnologica e dalle esigenze di tutela di diritti costituzionalmente protetti.

In merito al primo aspetto, non si può escludere che l'evoluzione della tecnologia consenta di "leggere" il contenuto di una lettera senza la necessità di aprire nemmeno la busta che la contiene17; un'evoluzione del genere potrebbe consentire di svolgere delle vere e proprie "intercettazioni epistolari" e, di conseguenza, indurre il legislatore a rivedere la disciplina del sequestro della corrispondenza e del cd. visto di controllo.

Quanto all'esigenza di tutela dei diritti costituzionali, la Consulta ribadisce la necessità di «un continuo e vicendevole bilanciamento tra principi e diritti fondamentali, senza pretese di assolutezza per nessuno di essi»18. Non si può sottovalutare, allora, la necessità di contrastare la criminalità e, in questo particolare momento storico, il terrorismo di matrice islamica; infatti, poiché quest'ultimo è legato non di rado alla cd. radicalizzazione in carcere, le attività investigative volte alla prevenzione e alla repressione di tale fenomeno potrebbero suggerire di ripensare le modalità di controllo della corrispondenza dei detenuti19.

È comprensibile, dunque, che la Corte costituzionale non escluda modifiche della disciplina impugnata dal giudice *a quo*, rimettendo al legislatore il compito e la responsabilità di approvare eventuali riforme; i giudici della Consulta, però, ricordano che la discrezionalità del legislatore trova un limite nelle riserve di legge e di giurisdizione previste dall'art. 15 Cost. e nell'osservanza dei canoni di ragionevolezza e di proporzionalità, il cui rispetto potrà essere sempre verificato dalla stessa Corte costituzionale.

---

[16] Così C. cost., sent. 20/2017, pt. 5 cons. dir. La Consulta non si sofferma sui dubbi di legittimità costituzionale avanzati dal giudice *a quo* con riferimento all'art. 112 Cost.; per qualche considerazione in merito sia consentito rinviare a D. Coduti, *Libertà e segretezza della corrispondenza dei detenuti nella sentenza n. 20 del 2017 della Corte costituzionale*, in *Federalismi.it*, *Focus Human Rights*, 2/2017, spec. 14 ss.

[17] Già lo stato attuale della tecnologia ha consentito di "leggere" alcuni papiri di Ercolano senza bisogno di svolgerli; lo studio è pubblicato in I. Burkreeva et. al., *Virtual unrolling and deciphering of Herculaneum papyri X-ray phase-contrast tomography*, in *Scientific Reports*, 6/2016, 27227.

[18] Così C. cost., sent. 20/2017, pt. 3.1 cons. dir.

[19] Infatti, A. Sperti, *La libertà e segretezza della corrispondenza e delle comunicazioni tra vecchie e nuove prospettive di tutela dei diritti fondamentali*, in Aa.Vv., *Il rispetto delle regole. Scritti degli allievi in onore di Alessandro Pizzorusso*, Torino, 2005, 95-96, osserva che le misure antiterrorismo causano spesso un indebolimento della garanzia della libertà e della segretezza della corrispondenza.

Tar Lazio, sez. I, 30 marzo 2017, n. 4101

Sussiste il potere regolamentare dell'Agcom in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica, nonché la potestà di vigilanza, nei confronti dei prestatori di servizi, da esercitarsi anche con l'imposizione di misure volte a porre termine alle violazioni della disciplina sul diritto d'autore, attraverso rimedi che si pongono in concorrenza, e non in sostituzione, di quelli già attribuiti all'Autorità giudiziaria.

L'arbitro delle controversie sul diritto d'autore *online* supera il vaglio del giudice amministrativo

AGCOM Online Copyright Enforcement Powers Unchallenged by the Rome Administrative Tribunal

diritto d'autore
AGCOM
principio di legalità
reti di comunicazione elettronica
enforcement

Pasquale Pantalone
Assegnista di ricerca in Diritto amministrativo, Università Commerciale "L. Bocconi"

Con sentenza n. 4101 del 30 marzo 2017, il Tar Lazio ha confermato la legittimità della delibera dell'Autorità per le garanzie nelle comunicazioni n. 680/13/CONS del 12 dicembre 2013, avente a oggetto il regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica.
Come noto, la titolarità del potere regolamentare dell'Agcom nella predetta materia ha suscitato un ampio dibattito in dottrina, specie con riferimento all'annosa questione della sua copertura legislativa, risultata, sin dalla prima procedura di consultazione pubblica avviata dall'Autorità nel 2010, una delle maggiori criticità del regolamento.
L'importanza della questione era, peraltro, resa ancor più manifesta dalla circostanza che la mancanza di una chiara predeterminazione legislativa non investiva esclusivamente la potestà regolamentare dell'Autorità in materia di tutela del diritto di autore *online*, ma anche le misure interdittive (quali, ad esempio, gli ordini rivolti ai prestatori di servizi di *hosting* di rimozione selettiva delle opere digitali rese illecitamente disponibili o, addirittura, di disabilitazione dell'accesso all'intero sito) che la stessa Agcom avrebbe potuto adottare sulla base delle proprie previsioni regolamentari.
Ebbene, la questione è giunta dinanzi al giudice amministrativo, il quale, pur senza celare un tortuoso percorso argomentativo, ha aderito alla tesi prospettata dall'Autorità, volta al riconoscimento in capo ad essa del potere regolamentare in esame e, di conseguenza, delle potestà interdittive ivi stabilite.
Prima di addentrarsi più specificamente nelle argomentazioni fornite dal Tar Lazio a suffragio delle proprie conclusioni, non si può non rammentare che sul punto è, altresì, incidentalmente intervenuta la Corte costituzionale con la sentenza n. 247/2015.
La decisione della Consulta è stata, in particolare, sollecitata dalle ordinanze nn. 10016 e 10020 del 26 settembre 2014, con cui il Tar Lazio aveva sollevato questione di legittimità costituzionale di talune disposizioni legislative che il giudice rimettente aveva posto a fondamento del potere regolamentare dell'Agcom e che – ad avviso del medesimo giudice - avrebbero violato, tra gli altri, i principi di legalità e di riserva di legge per l'assenza di parametri che garantissero una adeguata ponderazione, da parte dell'Agcom, dei diversi diritti costituzionali coinvolti nell'esercizio delle proprie attribuzioni regolamentari.
La Corte ha dichiarato inammissibili le questioni di legittimità costituzionale sollevate dal Tar Lazio, «in quanto entrambe [le ordinanze] presenta[va]no molteplici profili di contraddittorietà, ambiguità e oscurità nella formulazione della motivazione e del petitum».
Per quanto più rileva ai nostri fini, e con specifico riguardo alla titolarità in capo all'Agcom del potere regolamentare in esame, la decisione della Corte assume particolare rilievo nella misura in cui essa non ha mancato di rilevare che «[a] prescindere da ogni considerazione sulla accuratezza della ricostruzione del quadro normativo e della interpretazione datane dal rimettente, è evidente che nessuna delle disposizioni impugnate, in sé considerata, dispone specificamente l'attribuzione all'autorità di vigilanza di un potere regolamentare qual è quello esercitato con l'approvazione del regolamento impugnato nei due giudizi davanti al Tar. Esso è desunto dal giudice a quo, in forza di una lettura congiunta delle previsioni sopra esaminate, che non risulta coerentemente o comunque adeguatamente argomentata».
Ed invero, è proprio sul tentativo di una più coerente, e logicamente intelligibile, interpretazione sistematica dell'ambigua trama legislativa che si è appuntata la decisione in commento.
Occorre, tuttavia, sin da ora evidenziare che il rinnovato sforzo argomentativo messo in atto dal Tar Lazio per rinvenire nell'ordinamento un fondamento legislativo del potere regolamentare dell'Agcom in materia di tutela del diritto d'autore *online* non pare sufficiente – almeno sul piano del diritto positivo e della stretta compatibilità col principio di legalità amministrativa – a rendere immuni da critiche le conclusioni cui è giunto il giudice amministrativo.
Lasciando in disparte – anche per ragioni di economia della presente nota – l'analisi delle ulteriori censure avanzate dai ricorrenti, quella relativa alla carenza di potere dell'Autorità appare, in effetti, la più problematica e, dunque, meritevole in questa sede di un più attento e specifico esame.
Ciò posto, la norma che, secondo il Tar, riveste "un'importanza centrale" ai fini dell'individuazione del fondamento legislativo del potere regolamentare di Agcom è l'art. 182-*bis* della l. 633/1941, da "leggere" in combinato disposto con gli artt. 14, 15, 16 e 17 del d.lgs. 70/2003 (che ha recepito la direttiva 2000/31CE sul commercio elettronico).
Più precisamente, l'art. 182-*bis* cit. attribuisce all'Agcom, in coordinamento con la SIAE «nell'ambito delle rispettive competenze previste dalla legge», compiti di vigilanza per la prevenzione e l'accertamento delle violazioni concernenti la normativa sul diritto d'autore. Gli artt. 14-16 del d.lgs. 70/2003 (riferiti, rispettivamente, all'esercizio, da parte dei prestatori dei servizi della società dell'informazione, dell'attività "di semplice trasporto – *mere conduit*", "di memorizzazione temporanea

– *catching*" e "di memorizzazione di informazioni – *hosting*") dispongono, invece, che l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza possano esigere che il prestatore, nell'esercizio delle predette attività, impedisca o ponga fine alle violazioni commesse. Infine, l'art. 17 del d.lgs. n. 70/2003 introduce una clausola generale di esenzione della responsabilità del prestatore di servizi per la commissione di altrui illeciti.

La conclusione che il Tar trae dalla «visione sistematica delle norme richiamate» è presto detta: «[…] la sussistenza in capo ad Agcom di compiti di regolamentazione e di vigilanza nel settore del diritto d'autore che possono anche consentirle di impedire l'accesso a determinati contenuti resi disponibili sulla rete internet per il tramite di un prestatore di servizi].

Come anticipato, l'apparato argomentativo che supporta il verdetto del giudice amministrativo presta il fianco a una serie di critiche.

In primo luogo, il riferimento del Tar all'art. 182-*bis,* l. 633/1941 e al potere di vigilanza ivi previsto non pare idoneo a radicare in capo all'Agcom un ulteriore e inespresso potere di tipo regolamentare.

Pur se non espressamente evocato, è di tutta evidenza, infatti, il ricorso del giudice alla cd. teoria dei poteri impliciti, secondo cui il potere amministrativo privo di base legislativa sarebbe da ricavare "implicitamente" dall'ambito "abilitativo" della norma attributiva del potere tipico al quale il primo è legato da un nesso di strumentalità.

A tacere della sussistenza di una riserva di legge nella materia interessata dal regolamento, non pare comunque ammissibile l'auto-attribuzione da parte dell'Agcom di un potere implicito regolamentare, stante l'impossibilità, se non a scapito di stigmatizzabili forzature interpretative (peraltro prive di una adeguata base motivazionale), di estendere l'ambito "abilitativo" del potere di vigilanza sino a includere il succitato potere regolamentare.

In altri termini, sebbene non possa negarsi l'eterogeneità delle molteplici manifestazioni della funzione di vigilanza espressamente attribuita all'Agcom, non sembra che essa possa financo estrinsecarsi in un'attività normativa vincolante nei confronti dei soggetti vigilati.

Inoltre, più specificamente, non può sottacersi che la vigilanza di cui è titolare l'Agcom in base all'art. 182-*bis*, l. 633/1941, si traduce essenzialmente in una serie di poteri ispettivi demandati ai funzionari dell'Autorità ai sensi dell'art. 182-*bis*, comma 3, cit., che sono strumentali all'accertamento di alcune fattispecie penalistiche (v., a tal proposito, l'art. 182-*ter*, l. 633/1941, secondo cui «Gli ispettori, in caso di accertamento di violazione delle norme di legge, compilano processo verbale, da trasmettere immediatamente agli organi di polizia giudiziaria per il compimento degli atti previsti dagli articoli 347 e seguenti del codice di procedura penale»).

In secondo luogo, non appare, altresì, convincente a fondare la potestà regolamentare e i conseguenti poteri interdittivi in capo all'Agcom la "lettura" dell'art. 182-*bis*, cit., "congiuntamente" agli artt. 14-17 del d.lgs. 70/2003. Difatti, oltre a non fare alcun riferimento esplicito alla potestà regolamentare, tali disposizioni, siccome interpretate alla luce della direttiva 2000/31/CE sul commercio elettronico, non si appalesano direttamente attributive di un generale potere interdittivo in capo all'Agcom, ma mirano, piuttosto, a proteggere la posizione giuridica del prestatore di servizi a fronte del rischio di essere sempre ritenuto corresponsabile di altrui illeciti.

In ragione di quanto sopra, non sono, pertanto, condivisibili le argomentazioni offerte dal Tar Lazio per giustificare la legittimità del regolamento impugnato, specie in considerazione della riflessa e significativa "tensione" venutasi a creare col principio di legalità, nella sua veste sia formale sia sostanziale.

Ad ogni modo, pur ammettendo la potestà regolamentare dell'Agcom, un altro profilo su cui occorre riflettere (che non è emerso dalla vertenza da cui è scaturita la sentenza in commento) concerne la definizione dei limiti del potere para-giurisdizionale che l'Autorità esercita in base al regolamento. Più precisamente, in dottrina e in giurisprudenza non si sottovaluta il rischio – non sconosciuto all'attività dell'Agcom e di altre autorità indipendenti (si pensi ad. es. alle decisioni dell'Aeegsi sui reclami presentati ai sensi dell'art. 44 del d.lgs. 93/2011) – che l'esercizio di poteri para-giurisdizionali possa travalicare lo stretto recinto della singola controversia e "debordare" in atti impliciti di regolazione del mercato di volta in volta considerato, i quali sarebbero incompatibili con l'ordinamento generale.

Con ciò, si badi bene, non s'intende negare che il diritto d'autore sulle reti di comunicazione elettronica esiga strumenti di tutela rapidi ed efficaci, ma si vuole osservare che essi potrebbero risultare, da un lato, sufficientemente "coperti" da una norma di rango primario e, dall'altro, che il loro utilizzo sia circoscritto alla risoluzione della singola controversia.

In merito alla non stretta osservanza del principio di legalità e delle esigenze garantistiche e democratiche a esso sottese, non parrebbe, infine, ardito il tentativo di trovarne una possibile spiega-

zione nella natura – più evidente rispetto ad altre *authorities* – essenzialmente neutrale e apolitica dell'Agcom nella protezione del diritto d'autore *online*.
Il ruolo di "arbitro" che l'Autorità assumerebbe nell'esercizio di tale funzione potrebbe, infatti, giustificare un'accezione debole del principio di legalità, che ammetta poteri innominati (anche di carattere inibitorio) in vista della tutela del soggetto debole del rapporto (il quale, in genere, corrisponde al titolare del diritto d'autore), senza che il contratto venga intaccato in via amministrativa.
Dunque, il ricorso da parte dell'Autorità a poteri impliciti potrebbe forse trovare una giustificazione nello scopo "compensativo" che essi perseguirebbero per riequilibrare posizioni in partenza sbilanciate a favore di una delle parti del rapporto (si pensi a una multinazionale come Google rispetto a una persona fisica titolare di un diritto d'autore su un'opera digitale). D'altra parte, la sola tutela giurisdizionale si rivelerebbe inadeguata a offrire una tutela rapida ed effettiva al diritto d'autore su internet.

Cassazione penale, sez. V, 14 luglio 2016, n. 54946

Il legale rappresentante di una società che gestisce un sito Internet concorre nel reato di diffamazione con l'utente autore di un commento offensivo dell'altrui reputazione se ha consapevolmente mantenuto il commento sul sito dopo averne appreso l'esistenza, consentendo che lo stesso eserciti una efficacia diffamatoria.

Una pronuncia problematica in tema di responsabilità del gestore del sito per i commenti dei lettori

A Critical Judgment on the Criminal Liability of Website Owners for Third Parties' Defamatory Comments

diffamazione
Internet
responsabilità degli ISP
libertà di espressione
Cassazione

Carlo Melzi d'Eril
Avvocato in Milano

1. Il principio. – 2. La vicenda. – 3. Qualche timida perplessità.

1 Il principio.

La Corte di Cassazione è tornata ad occuparsi di un tema di non semplice soluzione e che costituisce un buon esempio delle nuove questioni aperte con l'avvento e la massiccia diffusione di Internet, anche come veicolo della libertà di manifestazione del pensiero. Stiamo parlando della possibilità di attribuire al gestore del sito web o della piattaforma una qualche forma di responsabilità per i contenuti prodotti da terzi ed ospitati nella pagina web.
La sentenza che qui segnaliamo, emessa dalla V sezione della Cassazione, sembrerebbe ritenere che il gestore di un sito web risponda per i contributi diffamatori pubblicati da altri, anche se firmati dall'autore, qualora sia a conoscenza dalla pubblicazione. Per di più, parrebbe sufficiente ad emettere una condanna in concorso con l'autore materiale del fatto, una presunzione di conoscenza derivante dal fatto che il gestore dello spazio sia stato avvisato con una e-mail da un privato – in questo caso lo stesso autore – della diffusione.

2 La vicenda.

Non è semplice dalla motivazione della sentenza capire tutte le sfaccettature del fatto utili ad apprezzare le ragioni della decisione. Proviamo qui a sintetizzarle. Nell'agosto del 2009 un lettore pubblicava su un sito specializzato in notizie relative al gioco del calcio un commento offensivo nei confronti di un soggetto che stava per ricoprire una carica importante a livello nazionale. Più precisamente, tra l'altro, lo apostrofava come «emerito farabutto» e «pregiudicato doc», allegando il certificato penale della persona in questione. A quanto si è inteso, i commenti sul sito in questione erano liberi, cioè i lettori potevano introdurli senza alcun preventivo filtro da parte della redazione. Non molti giorni dopo, l'autore delle frasi "incriminate" inviava questa volta per e-mail al "direttore" del sito il certificato penale già accluso al commento.
Mentre in primo grado veniva esclusa la responsabilità del titolare del blog, la Corte d'Appello, riformando la sentenza, lo condannava per concorso nel delitto di diffamazione a mezzo internet (art. 595 comma 3 c.p.), riconoscendo altresì alla parte civile un risarcimento non irrilevante. La condotta rimproverata sembra unicamente quella di non avere provveduto alla cancellazione del contenuto oggetto di querela, nonostante la conoscenza del suo tenore, o almeno di non averlo fatto fino a quando l'autorità giudiziaria non ne disponeva il sequestro preventivo.
La tesi del ricorrente che chiedeva l'annullamento della sentenza si basava su due argomenti. Da un lato egli affermava di non avere affatto contribuito alla pubblicazione poiché, come accennato, quello in esame sembrerebbe essere un blog non monitorato. In secondo luogo, l'imputato sottolineava di aver preso coscienza del messaggio pubblicato soltanto al momento della notifica della misura cautelare reale.
La Cassazione, come anticipato, conferma la condanna del responsabile del sito per concorso nella diffamazione commessa dall'autore del messaggio. La rimproverabilità in capo al primo deriverebbe dal fatto che egli ha «mantenuto consapevolmente l'articolo sul sito, consentendo che lo stesso esercitasse l'efficacia diffamatoria» fino al momento in cui non è stato oscurato in virtù del provvedimento di sequestro. È interessante notare come lo sforzo della motivazione sia tutto incentrato sulla dimostrazione della consapevolezza circa la presenza del contenuto diffamatorio sulla piattaforma. A questo proposito la Corte sembra porre l'attenzione e sottolineare soprattutto, quando non esclusivamente, due dati: il Collegio ricorda come l'imputato abbia da un lato ricevuto una e-mail dall'autore del commento "incriminato" con allegato il certificato penale che quest'ultimo aveva diffuso, dall'altro pubblicato un articolo, questa volta a propria firma, in cui faceva espresso riferimento al "post" del lettore.
Dal tenore della motivazione pare che la conferma della condanna del gestore sia derivata dalla sua mera coscienza del fatto che il testo fosse *online*.
La circostanza che la Corte si concentri sull'aspetto appena descritto potrebbe far intendere che, secondo i Supremi giudici, sia ormai consolidato – e non abbia quindi bisogno di una spiegazione ad hoc – il principio in base al quale il titolare di un sito web, se non cancella un contributo diffamatorio inserito da altri, risponde del reato di cui all'art. 595 c.p.

3 Qualche timida perplessità.

Quella appena sintetizzata non pare una conclusione convincente e per più di una ragione.
In primo luogo, perché un simile "precedente" non sembra essere coerente con le regole in materia di concorso di persone nel reato che, pur ampie, non pare riescano ad abbracciare anche una condotta come quella dell'amministratore della pagina web in relazione a quella dell'autore del post. Cercando di declinare tali regole nel caso concreto, certamente al titolare di un blog può essere contestato il delitto di diffamazione per un testo di terzi, se ne viene appurato un contributo morale o materiale alla esecuzione del fatto, cioè la lesione della reputazione del querelante, prima o al momento della diffusione del messaggio offensivo.
Volendo entrare ancora più nel dettaglio, ciò può accadere quando il "dominus" della pagina abbia ispirato o istigato o rafforzato il proposito criminoso dell'agente materiale, come nel caso in cui abbia commissionato un articolo con l'esplicito scopo di screditare la persona offesa, oppure abbia convinto l'autore titubante o l'abbia rassicurato circa la correttezza del suo agire, in modo tale da incidere sulla sua decisione e sul tenore del messaggio. Una responsabilità può essere attribuita anche quando il sito sia monitorato e le parole dei lettori siano pubblicate soltanto dopo il vaglio e l'autorizzazione dell'amministratore. In quest'ultimo caso, non sembrano esservi molti dubbi sul fatto che il moderatore dello spazio di discussione abbia concorso nell'eventuale reato: senza la sua condotta attiva, infatti, il massaggio non sarebbe mai stato divulgato e, di conseguenza, l'offesa recata.
La Cassazione, lo si ribadisce, non si dilunga, né per la verità nemmeno accenna, a circostanze che possano far giungere a ritenere davvero sussistenti i presupposti per un concorso, del primo o del secondo tipo. La Corte appunta la propria decisione sul fatto che il titolare del sito non si sia attivato per cancellare il messaggio offensivo, pur essendo a conoscenza della sua presenza *online* e ciò in quanto con tale comportamento egli avrebbe consentito la ulteriore diffusione del contenuto lesivo.
Va detto, tuttavia, che il comportamento omissivo, posto in essere dopo l'esecuzione di un'attività illecita già integralmente realizzata, non sembra consentire di contestare il concorso nel delitto consumato.
Nel caso specifico, poi, tenuto conto della natura istantanea della diffamazione, che si realizza con la lettura da parte di due persone, il mero consentire che gli effetti lesivi si procrastinino, a causa della persistenza in rete del commento, non si ritiene possa essere qualificato come una partecipazione penalmente rilevante. Per la verità, poi, nel caso di propalazione a un pubblico indefinito, il momento consumativo del reato è stato ritenuto, per convenzione, quello della diffusione, senza che sia necessaria la dimostrazione concreta della percezione da parte di una pluralità di soggetti, sicché la condotta del gestore sembra "contare" ancora meno.
Vi è un'altra ragione per cui la decisione in commento non ci pare condivisibile. La condotta contestata al gestore è di natura omissiva e si sostanzia nel non essere intervenuto, in presenza di un contenuto illecito, a eliminarlo dalla piattaforma. Più precisamente i Giudici paiono avere ascritto all'imputato il delitto di diffamazione combinando l'art. 595 c.p. con l'art. 40, comma 2, c.p. in base al quale, come noto, non impedire un evento illecito che si ha l'obbligo giuridico di impedire equivale a cagionarlo. Ci troviamo quindi di fronte a un reato omissivo improprio, contestabile però soltanto se esiste, come accennato, una posizione di garanzia (l'obbligo giuridico di impedire l'evento). Le posizioni di garanzia nel nostro ordinamento possono avere soltanto tre fonti: la legge, un contratto o il pregresso esercizio di un'attività pericolosa.
Il titolare di uno spazio web non risulta essere destinatario di alcuna posizione di garanzia rispetto ai contenuti della "sua" pagina derivante dalla legge: al semplice blogger non è certo applicabile, per giurisprudenza ormai costante, l'art. 57 c.p., che prevede una responsabilità per omesso controllo del direttore di un periodico cartaceo per i reati commessi sul periodico da lui diretto. Egli, infatti, da una parte non ha alcun dovere, in vista della pubblicazione, di controllare i contenuti al fine di impedirne la diffusione di illeciti. Né, in seguito alla pubblicazione, sempre il titolare ha alcun dovere di cancellare quelli diffamatori o, meglio, con una precisazione che spiegheremo di qui a un momento, quelli di cui la persona offesa lamenta la diffamatorietà.
La maggior parte delle pagine web, poi, chiarisce bene, tra le regole generali di utilizzo dello spazio, che i titolari del dominio non rispondono dei contenuti prodotti da terzi. E, infine, pare obiettivamente arduo affermare che la diffusione di fatti e opinioni, tutelata dall'art. 21 della Costituzione, sia catalogabile fra le attività pericolose.
La mancanza di una posizione di garanzia ha come ovvia conseguenza l'impossibilità di contestare una diffamazione in forma omissiva impropria per la mera mancata cancellazione di testi,

quand'anche fossero ritenuti penalmente rilevanti, in assenza di una richiesta in tal senso della pubblica autorità.
Quest'ultimo accenno alla pubblica autorità va chiarito, come va chiarito il riferimento al fatto che il gestore non ha l'obbligo di cancellare testi a richiesta del privato. L'unica disposizione all'interno dell'ordinamento che ha disciplinato la responsabilità dell'host provider – figura assimilabile all'amministratore di una pagina web, per quanto qui interessa – per i contenuti prodotti da terzi è l'art. 17, d.lgs. 70/2003 che, quindi, in assenza di altre, è divenuta quella di riferimento. La disposizione prevede che, appunto, il soggetto fornitore dello spazio in rete non risponde di quanto ivi introdotto da altri purché non ne conosca la illiceità e non rifiuti di eliminare i contenuti quando ciò viene chiesto dalla pubblica autorità.
Nel caso in esame non era accaduto nulla di simile: non sembra che dalla motivazione emergano elementi che inducano a ritenere con certezza che l'imputato fosse a conoscenza della pubblicazione e, in ogni caso, non pare che il gestore avesse coscienza del carattere illecito del testo. E ciò se non altro perché qui, come accade spesso nelle diffamazioni, in astratto l'espressione poteva risultare offensiva, ma la concreta illiceità del messaggio "si giocava" soprattutto sulla verità del fatto narrato o posto alla base della critica. Questo tipo di analisi, di solito, non è né semplice né immediata.
Per concludere, la soluzione della Corte risponde a una comprensibile richiesta di giustizia. In assenza di un legislatore, ormai per antonomasia latitante, la Cassazione è indotta a supplire alle carenze normative, introducendo regole finalizzate a disciplinare un fenomeno con spiccati tratti di novità, come è la manifestazione del pensiero in rete.
Il risultato però non soddisfa. La responsabilità posta in capo al gestore del sito somiglia molto a una responsabilità oggettiva "per posizione", inammissibile in un sistema penale costituzionalmente ben orientato. Inoltre, se un indirizzo di questo tenore prendesse piede, i titolari dei siti sarebbero indotti a operare una drastica censura per evitare di incorrere in guai giudiziari, circostanza che rischia di impoverire la rete delle opinioni controcorrente, col risultato di rendere il web peggiore di come potrebbe essere e diverso da come abbiamo imparato a conoscerlo.
Astraendosi dal caso concreto, poi, l'odierna tendenza della giurisprudenza av generare regole, come si diceva comprensibile nel contesto odierno, diventa rischiosa se supera i confini posti dal sistema. Continuiamo a pensare che un vuoto legislativo possa anche essere riempito dall'opera del potere giudiziario, se ciò accade stando nei limiti tracciati per l'esercizio di tale potere.

Tribunale di Torino, sez. I civile, 7 aprile 2017 n. 1928

Un *hosting provider* può qualificarsi come attivo solo se manipola, altera o comunque incide sui contenuti che esso ospita. Le attività attinenti alla migliore utilizzazione, visualizzazione e sfruttamento anche commerciale dei contenuti ospitati non sono idonee a mutare la qualificazione di un *hosting provider* da passivo ad attivo.

L'*hosting provider* è tenuto ad attivarsi per rimuovere l'accesso a un contenuto illecito, ai sensi dell'art. 16 del d. lgs. n. 70 del 2003, se riceve una lettera di diffida specifica, contenente gli URL dei singoli contenuti, da parte del titolare dei diritti di sfruttamento economico sui contenuti stessi.

Il fornitore di servizi deve rimuovere completamente il contenuto illecito dai propri sistemi e attivarsi per rimuoverlo anche dai sistemi dei fornitori con cui ha accordi di memorizzazione e conservazione dei dati, non essendo sufficiente limitarsi a oscurare il contenuto dall'Italia.

Il Tribunale di Torino interviene sulla responsabilità degli Internet Service Provider

The Court of Turin Takes the Floor in the Debate on ISP Liability in Italy

direttiva e-commerce
Internet Service Provider
hosting provider
responsabilità degli ISP
diritto d'autore

Filippo Frigerio
Cultore della materia in Diritto pubblico, Università Commerciale "L. Bocconi"

1. Premessa. – 2. Le parti in causa. – 3. Fatti processuali pregressi. – 4. Sul *framework* normativo e sulla natura di YouTube LLC. – 5. La decisione del tribunale. – 6. Conclusione.

1 Premessa.

Con la sentenza n. 1928 pubblicata il 7 aprile scorso, il Tribunale di Torino ha messo il punto nel giudizio di primo grado alla controversia che dal 2013 vede impegnate, da un lato, la società Delta TV Programs S.r.l. e, dall'altro, le società Google, Inc., YouTube LLC e Google Ireland Holdings. La decisione dei Giudici si inserisce in un vivace dibattito giurisprudenziale che impegna le Corti italiane, con alterne vicende, da quando è entrato in vigore il decreto legislativo n. 70 del 2003 (il c.d. "decreto e-commerce"), che segue di pochi anni l'approvazione della direttiva 2000/31/EC sul commercio elettronico.

2 Le parti in causa.

You Tube LLC e le società del gruppo Google sono state convenute in giudizio dalla società torinese Delta TV Programs S.r.l., la quale lamentava la violazione dei propri diritti di proprietà intellettuale e, in particolare, dei diritti di sfruttamento economico di alcune telenovelas sudamericane, che Delta TV deteneva in esclusiva per il territorio italiano.
Nello specifico, la violazione si era concretizzata poiché Delta TV aveva ravvisato la presenza non autorizzata dei contenuti a essa licenziati in via esclusiva sulla piattaforma di *video-sharing* YouTube. La presenza di questi video *online* e il fatto che gli utenti di YouTube non pagassero alcunché a Delta TV per visionare suddetti contenuti avrebbero cagionato ingenti danni all'attrice. Questa, infatti, lamentava che nessun operatore economico sarebbe mai disposto a pagare un prezzo per rendersi licenziatario laddove gli stessi contenuti licenziati fossero accessibili sulla rete liberamente e gratuitamente.

3 Fatti processuali pregressi.

Nella fase pre-contenziosa, Delta TV ha affidato a una lettera di diffida le proprie doglianze nei confronti delle società poi convenute, chiedendo loro di interrompere le trasmissioni delle telenovelas e rimuovere tutto il materiale caricato in violazione dei propri diritti d'esclusiva. Ha chiesto, inoltre, di astenersi dal perpetrare nuove violazioni impedendo il caricamento sulla piattaforma di ulteriore materiale in violazione dei diritti di proprietà intellettuale di Delta e risarcire i danni già prodottisi.
Non avendo dato seguito alle richieste dell'attrice, le società del gruppo Google sono state convenute in giudizio. Con un ricorso cautelare depositato in corso di causa, l'attrice-ricorrente ha chiesto in via d'urgenza la cancellazione del materiale di cui è causa dai sistemi di YouTube. La richiesta è stata negata in prima sede cautelare. Invero, il Giudice ha ravvisato come, dopo la notifica dell'atto di citazione, e l'avvenuta conoscenza da parte di YouTube dell'effettiva lista di materiali in violazione dei diritti di Delta TV, gli stessi materiali non risultassero più disponibili sulla piattaforma YouTube e quindi fosse cessata la materia del contendere.
Di diverso avviso il Collegio in sede di reclamo, il quale ha parzialmente riformato la decisione del Giudice dell'urgenza, ordinando alle convenute-resistenti di rimuovere dalla piattaforma gli audiovisivi e di impedire l'ulteriore caricamento degli stessi mediante l'utilizzo del *software* "Content ID", utilizzando come riferimenti i file corrispondenti agli URL indicati da Delta.

4 Sul *framework* normativo e sulla natura di YouTube LLC.

Nella lunga decisione, i Giudici ritengono opportuno spendere vari paragrafi per individuare la legge applicabile alla piattaforma YouTube. In particolare, il Tribunale ritiene che YouTube offra un servizio di *videosharing* (attraverso siti Internet come www.youtube.it e www.youtube.com). Ciò significa che sono i singoli utenti a caricare i video sulla piattaforma. Gli stessi utenti possono accedere, visionare, condividere e commentare i video stessi.

Ai sensi della legislazione italiana ed europea applicabile, YouTube rientra pertanto nella categoria dei fornitori di servizi della società dell'informazione e, in particolare, nella categoria del *hosting provider*, *ex* art. 16 del d. lgs. 70/2003 e art. 14 della direttiva 2000/31/CE.
Il Tribunale si interroga, poi, sulla tipologia di fornitore di servizi di cui YouTube assume la natura. Negli anni, sia la giurisprudenza italiana che quella europea hanno rimarcato la differenza tra le categorie del c.d. *hosting provider passivo*, ovverosia di mero *host*, per identificare i casi in cui il prestatore si limiti a fornire un servizio in maniera neutrale, e di *hosting provider attivo*, nella misura in cui esso operi con modalità tali da fargli perdere il proprio carattere neutrale.
Questa distinzione, accolta con favore dal Tribunale di Roma, ha trovato l'opposizione della Corte d'Appello di Milano. Essa, infatti, ha preferito porre l'accento sul carattere "innovativo" del fornitore di servizi di *hosting* per allontanare il servizio stesso dagli scarni e ampiamente superati modelli legislativi. Il carattere "evoluto", tuttavia, non vale ad allontanare l'*hosting provider* dal perimetro normativo di riferimento, quantomeno per quel che riguarda la responsabilità. In assenza di modifiche legislative, non v'è ragione per ritenere in via interpretativa l'*hosting provider* non soggetto alle disposizioni di favore del decreto e della direttiva e-commerce.

5 La decisione del Tribunale.

La sentenza si caratterizza per una serie di profili innovativi che meritano di essere qui brevemente elencati. Il primo punto verte sulla qualificazione dell'*hosting provider*, il secondo sulla tipologia di *notice* che il titolare dei diritti che rivendica deve inviare al *provider* per attivare il suo obbligo di intervento *a posteriori* e il terzo riguarda i potenziali effetti extra-territoriali dell'ordine del Giudice.
In primo luogo, il Tribunale di Torino fornisce un'interpretazione a tratti innovativa per quanto concerne l'annosa disputa *l'hosting provider attivo/passivo* e il c.d. *hosting provider evoluto*. I Giudici, infatti, ritengono che l'attività svolta in generale e il modello di business adottati dal prestatore di servizi non siano idonei a mutare la qualifica dell'ISP. Lo è, per l'inverso, l'attività svolta in concreto dal prestatore nei riguardi del contenuto che esso ospita.
Un *hosting provider* può qualificarsi come attivo solo se pone in essere attività funzionali a manipolare, alterare o comunque incidere sui contenuti ospitati. Le attività attinenti alla migliore utilizzazione, visualizzazione e sfruttamento commerciale dei contenuti non sono idonee a mutare la qualificazione di un *hosting provider* da passivo ad attivo. Siffatto *hosting provider* che pone in essere tali comportamenti non può veder mutare il proprio regime di responsabilità limitata di derivazione comunitaria.
Passando al secondo aspetto, come conseguenza del primo, al fine di attivare l'obbligo di controllo *a posteriori* di cui all'art. 16 del decreto e-commerce del 2003, il titolare dei diritti di sfruttamento economico deve inviare all'*hosting provider* una diffida specifica e contenente l'URL dei singoli contenuti di cui si assume la violazione.
Una volta a conoscenza dell'illiceità di alcuni contenuti che ospita, l'*hosting provider* è investito dell'obbligo di attivarsi e di cooperare con il titolare dei diritti, al fine di interrompere effettivamente l'illecito denunciato ed evitarne la prosecuzione. Se non lo fa, diviene soggetto – assieme all'autore della violazione, alla responsabilità che da quest'ultima scaturisce.
Mette conto notare che, in virtù delle difese svolte da YouTube nel caso in esame, e alla luce delle peculiarità di quel servizio, il Tribunale riconosce che quest'ultima utilizza già un *software*, Content ID, per la miglior tutela dei contenuti protetti. Partendo proprio da questa difesa di parte, il Tribunale (già sul punto anticipato dal Collegio in sede di reclamo, come visto sopra) ritiene che YouTube sia tenuta a utilizzare il suddetto *software* al fine di evitare che altri soggetti carichino nuovamente i medesimi contenuti, già oggetto di rimozione, sulla piattaforma.
Saggiamente, il Tribunale riconosce i limiti di suddetto sistema, con ciò facendo quindi salvi quei casi in cui l'utilizzo del *software* Content ID è soggetto a «un minimo margine di probabilità di insuccesso».
Infine, con l'obiettivo di evitare il protrarsi della violazione dei diritti di sfruttamento economico, l'*hosting provider* deve rimuovere completamente dai propri sistemi (e da quelli dei fornitori con cui intrattenga accordi per la memorizzazione e la conservazione di contenuti) il contenuto illecito, non potendosi limitare a oscurarlo dall'Italia, poiché è agevolmente possibile – utilizzando meccanismi di mascheramento dell'IP – simulare una connessione dall'estero, aggirando così il blocco.
Questo punto della decisione apre a domande e questioni che, per la brevità della presente esposizione, appare opportuno riservare a ben altre sedi. Basti per ora ricordare che il tema dell'estensione extra-giurisdizione dell'ordine di un Giudice nazionale è molto controverso ed è stato affrontato,

in tempi assai recenti, dalla Corte Suprema del Canada nel caso *Equustek Solutions, Inc. e altri v. Google, Inc.*
Per la suddetta violazione, le società convenute sono state condannate alle spese legali, nonché alla corresponsione di Euro 250.000 a titolo di risarcimento danni.

6 Conclusione.

Come accennato, la sentenza annotata si caratterizza per essere particolarmente innovativa e per offrire soluzioni, fino ad oggi esplorate con scarsa attenzione dalla giurisprudenza italiana, a problemi che affliggono da anni il dibattito – anche dottrinale – in materia di responsabilità dei fornitori di servizi della società dell'informazione.
In attesa di un auspicabile mutamento normativo che chiarisca, ma non scardini i caratteri essenziali della disciplina sul commercio elettronico, il Tribunale di Torino non ritiene di discostarsi dalle disposizioni in tema di responsabilità limitata degli ISP. Con ciò, si pone in aperto contrasto con altri fori che, con soluzioni più o meno giustificate e/o giustificabili, hanno dato una risposta diametralmente opposta alle stesse domande.

Cronache
New Legislation

Un primo commento alla legge sul cyberbullismo

Some Prima Facie Observations on the Italian Law to Fight Cyber Bullying

cyberbullismo
minori
Internet
diritto penale
social network

Monica Alessia Senor
Avvocato in Torino, Fellow del Nexa Center for Internet & Sociery

1 Lo scorso 3 giugno è stata pubblicata in Gazzetta Ufficiale la l. 29 maggio 2017, n. 71, recante "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo". Una mirabile sintesi del provvedimento è stata formulata dal Garante privacy nel suo discorso in occasione della presentazione alla Camera della Relazione 2016 sull'attività dell'Autorità: «Particolarmente positiva è la scelta di coniugare un approccio preventivo e riparatorio, grazie alla promozione dell'educazione digitale e alla specifica procedura di rimozione dei contenuti lesivi presenti in rete».
In effetti, il più grande pregio della nuova normativa in tema di cyberbullismo è sicuramente quello di aver mantenuto l'originaria *ratio*, fortemente voluta dalla prima firmataria del ddl, la senatrice Elena Ferrara, che escludeva qualsiasi forma di repressione di carattere penale.
Il risultato ottenuto non era affatto scontato atteso che alcune delle proposte di legge (C.1986, C.2435, C.2670), che erano state riunite al ddl Ferrara alla Camera dopo la sua approvazione al Senato, introducevano un reato *ad hoc* ed il testo approvato dalla Camera in seconda lettura (C.3139) prevedeva una nuova circostanza aggravante ad effetto speciale per il reato di *stalking,* nel cui precetto possono essere fatti rientrare i più classici atti di bullismo e di cyberbullismo.
Fortunatamente, l'invisa prassi del legislatore italiano di ricorrere alla sanzione penale per regolamentare qualsiasi fenomeno sociale nuovo - o vecchio, ma modernamente declinato - ha ceduto il passo, nel caso di specie, ad una logica normativa basata sull'individuazione di strumenti preventivi di carattere educativo, affiancata da procedure amministrative di *notice & takedown*.

2 A fronte di questo indubbio elemento positivo, permangono alcune perplessità in merito ad altri snodi della legge, a partire dalla definizione stessa di cyberbullismo, a cui si interseca la contestuale eliminazione (alla Camera, in quarta lettura) della connessa definizione di bullismo.
L'art. 1, comma 2, della legge definisce il cyberbullismo come «qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti *online* aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo».
Si tratta di una definizione disorganica in quanto sovrappone condotte di fatto (pressioni, aggressioni, ricatto, furto d'identità) a condotte normative (molestia, diffamazione, trattamento illecito di dati personali) ed illogica nella parte in cui oppone alla generica diffusione *online* di qualsiasi tipo di contenuto la specificità dello scopo perseguito, incomprensibilmente circoscritto alla sola emarginazione sociale di un minore o di un gruppo di minori.
È, soprattutto, una definizione che non tiene conto dei molti studi condotti, specie all'estero, in materia: dai lavori preparatori emerge, infatti, come l'iter legislativo sia stato ispirato e motivato non tanto da ricerche accademiche quanto piuttosto da dati statistici, desunti da alcune indagini condotte da associazioni private a tutela dei minori le quali, esatte o meno che siano, si sono occupate di quantificare il fenomeno, non certo di analizzarlo.
La confusa definizione *de qua* non ha preso in considerazione neppure i fondamentali studi dello psicologo scandinavo Dan Olweus, luminare della teorizzazione del bullismo, secondo il quale per la sussistenza del fenomeno sono necessari tre requisiti minimi: un'aggressione intenzionale, fisica o verbale; la ripetizione nel tempo; uno squilibrio di potere o di forza.
Secondo Olweus, infatti, non possono essere catalogati come atti di bullismo né le aggressioni occasionali o reciproche, né i comportamenti in cui una parte non si pone in una posizione di predominanza fisica, psicologica, sociale o razziale rispetto ad un'altra, che si ritrova, per contro, a subire passivamente gli attacchi senza alcuna possibilità di difendersi.
L'importanza di una definizione precisa non è un elemento meramente formale in quanto solo una attenta descrizione del fenomeno (bullismo o cyberbullismo che sia) può consentire la predisposizione di contromisure efficaci e l'indirizzamento delle risorse disponibili verso (e solo verso) quei comportamenti che denotano un effettivo disvalore sociale. Basta por mente all'assoluta carenza, nella definizione in esame, di qualsiasi riferimento al fattore reiterazione, per comprendere come la legge in commento sia mal calibrata e, paradossalmente, possa comportare, nel prossimo futuro, interventi assai invasivi nei confronti dei minori per episodi isolati o puramente occasionali.
La difficoltà mostrata dal legislatore nel descrivere puntualmente cosa si debba intendere per cyberbullismo, peraltro, è sintomatica dell'insipienza del nostro legislatore nel ricercare le cause dei fenomeni che generano allarme sociale e, più in generale, nell'affrontare le sfide della moderna *ICT*

society, insipienza da cui discende la tendenza a legiferare in maniera emozionale, con la tecnica della c.d. "pecetta normativa", ovverosia mediante l'apposizione di un cerotto senza diagnosi della malattia.

3 Il secondo punto critico della legge riguarda la procedura di *notice & takedown*.
A tal proposito, la nuova normativa prevede che i minori ultraquattordicenni e i soggetti esercenti la responsabilità del minore (che abbia subito un atto di cyberbullismo, come sopra definito, sigh!) possano chiedere al titolare del trattamento o al gestore del sito internet o del social media l'oscuramento, la rimozione o il blocco di «qualsiasi altro dato personale». Qualora il destinatario del *notice* non provveda entro 48 ore o qualora non sia possibile identificare il titolare del trattamento o il gestore del sito internet o del social media, l'interessato può rivolgere analoga richiesta, mediante segnalazione o reclamo, al Garante per la protezione dei dati personali, il quale provvede entro 48 ore ai sensi degli artt. 143 e 144 del Codice privacy.
L'art. 1, comma 3, specifica che per gestore di un sito internet si intende un prestatore di servizi della società dell'informazione, diverso da quelli di cui agli artt. 14, 15 e 16 del d.lgs. 70/2003, per i quali la direttiva e-commerce prevede un'esenzione di responsabilità.
L'esclusione di *access, caching* ed *hosting provider* dal concetto di gestore di un sito internet e dunque dall'obbligo di osservare le procedure di *takedown* previste dalla legge risponde alla corretta esigenza di salvaguardare i principi essenziali della direttiva e-commerce, in particolare le libertà di iniziativa economica e di espressione ivi tutelate.
L'esclusione di tali provider pare ineludibile anche alla luce del fatto che i contenuti *online* di cui può essere chiesta la rimozione non necessariamente debbono essere illeciti, come si evince dalla formula «qualsiasi altro dato personale» utilizzata dal legislatore.
La soluzione adottata genera però alcuni dubbi interpretativi.
La legge in esame, infatti, distingue i gestori di siti internet dai gestori di *social network*, nonostante questi ultimi rientrino pacificamente nella categoria degli *hosting provider*.
Quid juris?
Si tratta di un'*impasse* di non poco conto: se si applica testualmente la legge e si ritiene che una richiesta di rimozione possa essere comunque indirizzata ad un SNS (*hosting*) *provider* in quanto gestore di un social media si viola il d.lgs. 70/2003; se, al contrario, si opta per una interpretazione sistematica e dunque si ritiene che i gestori di social media rimangano esclusi dalla procedura di *notice & takedown* in quanto *hosting provider*, la reale portata innovatrice della l. 71/2017 risulta davvero risicata.
Verosimilmente, nella prassi, la rigidità di tali tecnicismi verrà smorzata da un lato dall'elaborazione giurisprudenziale della figura del c.d. *hosting provider* attivo, dall'altro dalle iniziative che i principali ISP stanno negli ultimi tempi intraprendendo per la prevenzione e la rimozione spontanea di contenuti *online* lesivi, tra cui anche quelli riconducibili ad atti di cyberbullismo, di cui la piattaforma per la prevenzione contro il bullismo, sviluppata da Facebook in collaborazione con Telefono Azzurro e Save The Children, rappresenta un valido esempio.
A prescindere da quale sarà la concreta applicazione della procedura di *notice & takedown*, resta invece fermo e saldo il ruolo centrale attribuito dalla legge al Garante privacy il quale, per la prima volta, viene chiamato ad intervenire, in tempi rapidissimi, non sulla base della tutela amministrativa di cui agli artt. 145 e ss. del Codice privacy, bensì, direttamente in prima battuta, mediante gli strumenti del reclamo e della segnalazione.
In questi casi, essendo il Garante un'autorità competente *ex* art.17 d.lgs. 70/2003, la rimozione di eventuali contenuti lesivi potrà sempre essere ordinata a qualunque *provider*, di qualunque natura esso sia, trascendendo l'infelice disciplina prevista per titolari e gestori.

4 La terza criticità riguarda la procedura di ammonimento prevista all'art.7, in base al quale fino a quando non sia proposta querela o presentata denuncia per taluno dei reati di cui agli artt. 594 (ingiuria), 595 (diffamazione) e 612 (minaccia) c.p. e all'art. 167 Codice privacy (trattamento illecito di dati personali) commessi, mediante la rete internet, da minorenni di età superiore agli anni quattordici nei confronti di altro minorenne, è applicabile la procedura di ammonimento già prevista per il reato di *stalking*.
Due le osservazioni da fare al riguardo: da un lato il legislatore pare essersi dimenticato, nonostante il servizio studi della Camera avesse riscontrato il problema, che il delitto di ingiuria è stato depenalizzato dal d. lgs. 7/2016, dall'altro non ha rilevato che l'ammonimento è compatibile solo

con reati procedibili a querela in quanto nel momento stesso in cui l'interessato espone al Questore ai fini dell'ammonimento fatti che integrano reati procedibili di ufficio (nella fattispecie, minaccia grave e trattamento illecito di dati personali) quest'ultimo, nella sua veste di pubblico ufficiale, è tenuto *ex* art. 331 c.p.p. a farne immediatamente denuncia per iscritto.

5 Da ultimo, lascia attoniti la circostanza che per tutte le attività di formazione scolastica e territoriale finalizzate alla prevenzione e al contrasto del cyberbullismo sia stata dalla legge stanziata l'esigua somma di 203.000,00 Euro per ciascuno degli anni 2017, 2018 e 2019.
Al netto di tutte le critiche, dunque, la nuova legge in tema di cyberbullismo rimane una normativa molto più ambiziosa nel titolo e nelle dichiarazioni di intenti che nel suo contenuto.

Data retention a sei anni. La Corte di giustizia dell'UE la boccerebbe come ha fatto con l'accordo Europa Canada sui PNR

Data Retention Extended to a Six-Year Term in Italy: Some Critical Remarks in Light of the Court of Justice Opinion on the EU-Canada PNR Agreement

privacy
dati personali
data retention
accordo Canada-UE
Carta di Nizza

Lucio Scudiero
Avvocato, Direttore esecutivo Lex Digital

Sta facendo finalmente discutere l'emendamento approvato la scorsa settimana dalla Camera dei Deputati che allunga a sei anni la conservazione di dati di traffico telefonico e telematico per finalità di contrasto al crimine e al terrorismo.
La *data retention* in Italia era fissata dal Codice della privacy in due anni per il traffico telefonico, un anno per quello telematico, trenta giorni per le chiamate senza risposta. Una durata estesa con il decreto legge antiterrorismo del 2015 che aveva imposto la conservazione di tutti i dati fino al 30 giugno 2017, in deroga al Codice, che di fatto aveva ammesso una conservazione fino a quattro anni.
L'emendamento in questione, presentato dai deputati Verini, Berretta e Mucci, assesta il regime di conservazione ordinario di tali dati a sei anni. E recita come segue:

> «Dopo l'articolo 12-bis, aggiungere il seguente:
> *Art. 12-ter. – (Termini di conservazione dei dati di traffico telefonico e telematico). – 1. In attuazione dell'articolo 20 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio del 15 marzo 2017 sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio, al fine di garantire strumenti di indagine efficaci tenuto conto delle straordinarie esigenze di contrasto al fenomeno del terrorismo, anche internazionale, per le finalità di accertamento e repressione dei reati di cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera a), del codice di procedura penale il termine di conservazione dei dati di traffico telefonico e telematico, nonché dei dati relativi alle chiamate senza risposta, di cui all'articolo 4-bis, commi 1 e 2, del decreto-legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, è stabilito, in deroga a quanto previsto dall'articolo 132, commi 1 e 1-bis, del decreto legislativo 30 giugno 2003, n. 196, in settantadue mesi.*
> *12-bis. 020.(Testo modificato nel corso della seduta) Verini, Berretta, Mucci. (Approvato)*»

Nel merito, hanno ragione quanti, in testa il Garante per la protezione dei dati personali, paventano una incompatibilità del nuovo regime interno con il diritto europeo.
Infatti, con la sentenza *Digital Rights Ireland* del 2014 (cause riunite C-293/12 e C-594/12), la Corte di Giustizia dell'Unione Europea aveva annullato la direttiva 2006/24/CE (cd. "*Data Retention*"), su cui si basano le norme interne oggetto di modifica tramite l'emendamento sopra citato, giudicando sproporzionata l'interferenza che essa esercitava sul diritto alla riservatezza dei cittadini europei per ragioni di sicurezza.
La direttiva infatti aveva un'applicazione generalizzata nei confronti di chiunque (non dei soli sospettati di reati), non distingueva tra reati (gravi e meno gravi), non gradava i tempi di conservazione in maniera coerente, e non prevedeva garanzie relative all'accesso a tali dati personali da parte delle forze di polizia.
Il risultato di quella pronuncia era ed è ancora che la nostra normativa interna (emanata sulla base della direttiva annullata), seppure formalmente ancora in vigore, è sostanzialmente illegittima, e cadrebbe certamente al primo rinvio pregiudiziale alla Corte di giustizia dell'Unione europea effettuato da un giudice italiano. A maggior ragione se venisse modificata nei termini approvati dalla Camera.
E se qualcuno pensa che dal 2014 ad oggi sul punto sia sostanzialmente mutata la sensibilità dei giudici di Lussemburgo, in ragione dei cruenti sviluppi del terrorismo in Europa, si sbaglia.
Non più tardi di tre giorni fa, esprimendosi su richiesta del Parlamento Europeo su una bozza di accordo per il trasferimento dei dati PNR (*Passenger Name Records*) dall'Europa al Canada, la stessa Corte ha reiterato alcuni dei concetti giuridici a suo tempo elaborati nella sentenza *Digital Rights Ireland*, concludendo per l'incompatibilità col diritto europeo della bozza di accordo.
Ciò perché – secondo i giudici lussemburghesi – lo schema di accordo col Canada prevede una serie di ingerenze non proporzionate e non necessarie su una vasta platea di interessati, cioè tutti i viaggiatori dall'Europa al Canada. Sebbene la Corte riconosca che – in principio – il trasferimento dei dati dei passeggeri sia necessario e funzionale ad esigenze preventive di gravi crimini in Canada, esso tuttavia viola i parametri di proporzionalità del diritto europeo allorché l'accordo consente alle autorità canadesi di accedere a tali dati anche una volta che l'ingresso dei passeggeri sia stato autorizzato, dunque durante il soggiorno di questi ultimi in Canada. Sostiene infatti la Corte che le autorità canadesi non possono semplicemente "aprire il cassetto" dei PNR raccolti in costanza di viaggio una volta che i passeggeri a cui si riferiscano siano stati autorizzati ad entrare; servono esigenze nuove e circostanziate, nonché garanzie procedurali ulteriori, quali il placet di un giudice terzo. Inoltre, la conservazione indiscriminata di tutti i PNR per 5 anni, e l'accesso agli stessi da parte della autorità canadesi una volta che i passeggeri siano usciti dal territorio canadese, sono altresì eccessivi: soltanto i PNR relativi a soggetti per i quali sussistano elementi obiettivi che consentano di ritenere che essi potrebbero, anche dopo la loro partenza dal Canada, presentare

un rischio in termini di lotta al terrorismo e ai reati gravi di natura transnazionale, possono essere oggetto di trattamento, e sempre previa autorizzazione di un giudice.
È evidente come la Corte di giustizia dell'Unione europea non ritenga affatto superato l'indirizzo interpretativo inaugurato nel 2014, ma anzi provi a inserirlo in un'ottica di cosiddetta *privacy by design* anche per i legislatori, a cui affida il delicato compito di bilanciare le esigenze di interesse pubblico perseguite con le garanzie di dettaglio sostanziale e procedurale per le libertà fondamentali dei cittadini europei.
Un esercizio, quest'ultimo, nemmeno abbozzato dal legislatore italiano.

How the Hungarian government nationalized criticism

For the past seven years, the Fidesz regime in Hungary has built, bit by bit, an effective media-control system. That allows them to attack anybody. Central European University was first.

freedom of speech
freedom of art and science
academic freedom
populism
freedom of criticism

Marius Dragomir
Director of the Center for Media, Data and Society (CMDS) at the CEU School of Public Policy (SPP)

1

«I know that the power, size and weight of Hungary is much smaller than that of the financial speculator, George Soros, who is now attacking Hungary», Viktor Orban, the Hungarian premier told the European Parliament on 26 April 2017.
The intervention was yet another part of the Soros-the-evil narrative that dominated the government's discourse during the CEU saga, a concerted attack that the Hungarian government launched in late March 2017 against Budapest-based Central European University (CEU). Back then, the Hungarian parliament adopted in a matter of days a law that is likely to force CEU to fold its operation in Hungary. Mr Soros is CEU's founder.
Critics of the law, mostly the Hungarian, liberal-minded intelligentsia and legions of foreign universities, NGOs, liberal politicians and thinkers, slammed the move as a political maneuver hatched by Mr Orban and his conservative Hungarian Civic Alliance (Fidesz) party, now in power. Thousands of Hungarians took the streets in protest.
But nothing has persuaded the Hungarian government to cede any ground in its battle with CEU. On the contrary, authorities seem poised to go for broke. According to the law, CEU will not be able to issue diplomas for newly enrolled students as of October 2017.
For many local observers, the attack on CEU is a political issue. The incumbent government is already in electoral mode: the values and people CEU is associated with are the perfect "enemy" that the government needs in its campaign for the next national elections primed for April 2018.
Yet, unleashing an attack of that scope and, unprecedentedly, against a university, can only happen in a dissent-controlled environment conducive to impunity. Building that environment was the project the Hungarian government has been steadily working on since it came to power seven or so years ago.
That is democratic Hungary's biggest problem.

2 A Party State

The first thing that Fidesz did following the electoral victory in 2010 was to adopt new media legislation. At the time, Mr Orban said that the measures were intended as a corrective for the leftist bias in the country's media.
The changes in law were clearly aimed at bullyragging vocal journalists. For example, the new law required media content to be "balanced" and not to incite hatred "against any majority," vague legal provisions that can open the gates to government's interference. For violations of these provisions, steep fines were introduced. A new authority, Media Council, composed of people appointed by parliament where Fidesz had a two-third majority, was created to enforce the new rules.
The 2010 law set a new regulatory framework for the media, laying the basis for a sheaf of measures aimed at shackling criticism that were yet to come.
First came public media. The Hungarian public broadcaster, whose history harks back to the communist times, has never been a paragon of independent journalism and quality programming. But after 2010, it became a mere government agency. All public media, including the country's news agency, were brought under the roof of a newly established organization, MTVA, led by the head of the Media Council, according to provisions in the same 2010 law.
Criticism abounded. European Parliament and the Organization for Security and Cooperation in Europe (OSCE), an intergovernmental institution, cried foul. Under pressure, the Hungarian parliament subsequently amended parts of the legislation. But its grip on the media regulator and the public media remained firm.
The reforms of the state media were accompanied by a massive staff purge: senior executives in MTVA, mostly those critical of Fidesz, were thrown out. "There were always pockets of professionalism, islands of freedom," said Attila Mong, then an anchor with the Hungarian state radio who was also given the ax. "There is no island. One party controls the system now."
Back then he didn't know that that was just the beginning.

3 Market Lego

The following six years saw a cavalcade of attacks, direct or indirect, aimed at private media, some of whom were still brave enough to report independently. Knowing that commercial media were financially vulnerable after the economic crisis hit their revenues, the government embarked on a

plan to "reshape" the market to their benefits, explained Attila Batorfy, a Hungarian journalist who's a fellow with the Center for Media, Data and Society (CMDS), CEU's flagship media research hub.
A big showdown was the clash with RTL Klub, a TV channel run by the German media conglomerate Bertelsmann. In 2014, the government introduced the advertising tax act, a law overtly targeted at the station. According to the law, RTL Group alone fell into the largest tax bracket. A 40% cut on their advertising revenues was imposed, clouting the company's bottom line. The net profit of the RTL group tumbled from €535m in the first three quarters of 2013 to €306m in the same period the following year, according to Financial Times.
Private media were given a strong signal: the government was serious about its critics. RTL Klub tempered, if not reined in, its criticism.
Attacks continued unabated. A law in 2014 raised barriers to journalists' access to public interest information. The media authority played a significant role in the "market reshaping" operation. Arbitrary licensing decisions favored government-allied radio channels. For five years, the merger of Swiss owned Ringier and Germany's Axel Springer, two major publishing houses, was blocked by the same authority. Some of their assets ended up in the hands of Mediaworks, a company with murky ownership linked with a dubious Austrian businessman.
Personal attacks against critical journalists became rife. Zoltan Speder, owner of Index, the biggest independent news portal by audience, was constantly traduced in articles published by government-supportive media. The stories were allegedly placed by the premier's cabinet office under the management of Antal Rogan.
An investigation by the largest opposition newspaper, *Nepszabadsag*, into the lavish lifestyle of Mr Rogan didn't eventually get published as the newspaper folded unexpectedly on 8 October 2016. Its owners, Mediaworks, argued that poor economic results prompted them to scrap the title. But less than three weeks later, the brand was purchased by Opimus, a company under the influence of businessman Lorinc Meszaros, a close ally of Mr Orban, according to reports from Reuters.
On top of all that, government funding in the media has grown massively in recent years. In 2016, the government spent 80% more on advertising, becoming the single largest advertiser in the country. With the subsidy from the state budget earmarked for the public media (close to €280m), the government now dwarfs all advertisers and media outlets in Hungary. Atlatszo, an investigative journalism outlet funded by private donors and citizen donations, operated last year with a frugal budget of €300,000.
Today, a few independent media outlets are still standing. They include Atlatszo, the news server 444 and the investigative non-profit organization Direkt36. At the other end of the spectrum, an opposition media empire is growing in parallel with the government media. It is led by Lajos Simicska, a wealthy businessman who was in cahoots with Mr Orban until 2014 when the two had a bitter argument over a new advertising tax that Mr Simicska feared it would hurt his own media.
A former roommate of Mr Orban during the university years, Mr Simicska is invested in construction, energy and media. He used to be Fidesz's financial mastermind. His companies received year after year fat public orders and state ad contracts. But as of 2014, his largest construction company, Kozgep, was barred from participating in public tenders. Between 2010 and 2014, nearly two-thirds of state ad spend was channeled to Mr Simicska's media companies. After 2014, some 70% of that went to the government-allied media.
The latest media acquisition by forces close to Mr Simicska was the news portal Index, now in the hands of a foundation managed by people close to him, including family. The investment by Mr Simicska in media is also election-related. He apparently doesn't have political ambitions, but being hell-bent on sweeping Mr Orban from power in 2018, he is shopping around for political allies who could carry out that task.

4 Politics First

It might seem far-fetched to say that Fidesz's media strategy over the course of the past seven years has been implemented according to a detailed plan agreed on at the onset of the party's rule. It is implausible to imagine Mr Orban and his party planning four years in advance to attack a TV station with a law purposely designed to clobber the station's finances. Most of the government's actions were reactive. An unflattering story here, a spurt of criticism there: the government responded.
However, taken together, all the moves of the government in the media are pieces of a strategy, relentlessly and systematically implemented, to secure control of criticism in the media. Mr Orban

and his Fidesz chums repeatedly said a decade ago that their previous loss in elections was much to blame on "liberal" media.

Only in such an environment can a government get away with almost everything it does, including the attack on CEU. Hungarian authorities could have attacked the university many years ago, but they waited until most of the major dissent channels were taken over or, worse, garroted. The timing for the attack on CEU is also strategic for political reasons. A fight was needed to boost Fidesz's electoral capital. Unfortunately, they chose a university to provide just that.

And it doesn't stop there. On 13 June 2017, the Hungarian government adopted a law imposing drastic restrictions on NGOs funded by foreign entities, another move aimed at hobbling dissent.

To sacrifice academic freedom for political gains is a supreme act of cynicism, but Mr Orban is determined to go to great lengths to win the next elections because the stakes are huge. A raft of investigations over the past year by local media outlets unveiled illegal deals, involving public money, between the government and some of Mr Orban's allies: both family and friends.

If Fidesz loses power, the party's fat cats will be out on a limb. Some of them might face slammer time. That is business (or politics, for that matter) as usual, especially in this part of the world.

But on a longer term, what really matters for a healthy Hungarian society is media freedom. Without it, anybody can be CEU next.

Legge per migliorare la tutela dei diritti sui social network (*Netzwerkdurchsetzungsgesetz – NetzDG*)

Law to Enhance Legal Enforcement on Social Network (Netzwerkdurchsetzungsgesetz – netzDG)

Germania
hate speech
social network
responsabilità degli ISP
libertà di espressione

Traduzione a cura di Giorgio Giannone Codiglione
Assegnista di ricerca presso l'Università degli Studi di Salerno

Articolo 1
Legge per migliorare la tutela dei diritti sui social network

§ 1
Ambito di applicazione

(1) La legge si applica ai fornitori di servizi di telecomunicazione che per scopo di profitto gestiscono piattaforme Internet progettate per permettere agli utenti di condividere qualunque tipo di contenuto o di renderlo accessibile al pubblico (social network). Le piattaforme che offrono contenuti di tipo giornalistico o editoriale, rispetto ai quali la responsabilità è dello stesso fornitore di servizi, non sono considerate come social network ai sensi della presente legge. Lo stesso vale per le piattaforme che sono destinate alla comunicazione individuale o alla diffusione di contenuti specifici.

(2) Il gestore di un social network è esonerato dagli obblighi di cui ai §§ 2 e 3 se il social network ha meno di due milioni di utenti registrati in Germania.

(3) Per contenuto illecito si intende il contenuto definito nel comma (1), che soddisfa quanto previsto dai §§ 86, 86a, 89a, 91, 100a, 111, 126, 129-129b, 130, 131, 140, 166, 184b in combinato disposto con 184d, 185-187, 241 o 269 del codice penale e che non è legittimo.

§ 2
Obbligo di resocontare

(1) Il gestore di un social network che ha ricevuto più di 100 segnalazioni di contenuti illeciti in un anno solare è obbligato a redigere semestralmente un rapporto in lingua tedesca sulla gestione delle segnalazioni di contenuti illeciti sulle proprie piattaforme, completo delle informazioni di cui al comma (2) ed è obbligato a pubblicarlo sulla Gazzetta Federale e sulla propria home-page entro un mese dalla fine di ogni semestre di riferimento. Il rapporto pubblicato sulla propria home-page deve essere facilmente individuabile, direttamente accessibile e costantemente disponibile.

(2) Il rapporto deve contenere:

1. Osservazioni generali sulle azioni intraprese dal gestore del social network al fine di eliminare dalla piattaforma ogni attività penalmente rilevante,

2. Descrizione dei meccanismi di invio delle segnalazioni riguardanti contenuti illeciti e dei criteri utilizzati per decidere sulla cancellazione o sul blocco dei contenuti illeciti,

3. Indicazione del numero delle segnalazioni di contenuti illeciti ricevute durante il periodo di riferimento, distinguendo tra segnalazioni ricevute da associazioni o da utenti e ancora evidenziando i motivi del reclamo,

4. Informazioni su organizzazione, risorse, competenze tecniche e linguistiche delle unità responsabili della gestione delle segnalazioni, nonché sulle attività di formazione e supporto dei soggetti responsabili della gestione delle segnalazioni,

5. Informazioni sulla partecipazione delle associazioni di categoria con l'indicazione dell'eventuale specifica via di accesso per le loro segnalazioni,

6. Indicazione del numero di segnalazioni in cui è stato consultato un soggetto terzo prima di adottare la decisione,

7. Indicazione del numero di segnalazioni che durante il periodo di riferimento hanno condotto all'eliminazione o al blocco di un contenuto offensivo, distinguendo tra quelle presentate da associazioni o dagli utenti e ancora indicando i motivi del reclamo o se sussiste un'ipotesi di cui al § 3, comma (2), punto 3, lettera a) e, in tal caso, se proviene da un reclamo di un utente o da un'organo di autoregolamentazione riconosciuto ai sensi del § 3, comma (2), punto 3, lettera b),

8. Indicazione del tempo intercorso tra la ricezione della segnalazione e la cancellazione o il blocco dei contenuti illeciti, distinguendo tra segnalazioni formulate da associazioni o dagli utenti, precisando le motivazioni e i periodi temporali "entro 24 ore"/"entro 48 ore"/"entro una settimana"/"in una data successiva",

9. Misure intraprese per informare della decisione adottata i soggetti che hanno inoltrato la segnalazione e gli utenti che hanno pubblicato il contenuto oggetto di contestazione.

§ 3
Gestione dei reclami riguardanti contenuti illeciti

(1) Il gestore di un social network deve garantire una procedura efficace e trasparente per la gestione delle segnalazioni di contenuti illeciti ai sensi dei commi (2) e (3). Il prestatore deve fornire agli utenti una procedura per la trasmissione delle segnalazioni riguardanti contenuti illeciti facilmente individuabile, direttamente accessibile e costantemente disponibile.

(2) La procedura deve garantire che il gestore del social network:

1. Accolga immediatamente la segnalazione, verifichi se il contenuto segnalato è illecito e va rimosso o se l'accesso a detto contenuto deve essere bloccato,

2. Rimuova o blocchi l'accesso a un contenuto manifestamente illecito entro 24 ore dalla ricezione della segnalazione, salvo che il social network abbia concordato con l'autorità giudiziaria competente un periodo più lungo per la cancellazione o il blocco dei contenuti manifestamente illeciti,

3. Rimuova o blocchi senza indugio tutti i contenuti illeciti, entro sette giorni dalla ricezione della segnalazione; il termine di sette giorni può essere superato se:

a) la decisione sull'illiceità del contenuto dipende dalla falsità di una dichiarazione o dipende chiaramente dalle circostanze di fatto; in tali casi, il gestore del social network può dare all'utente l'opportunità di replicare alla segnalazione prima che venga adottata una decisione;

b) il social network rimette la decisione sull'illiceità a un organo di autoregolamentazione riconosciuto ai sensi dei commi (6) e (8) entro sette giorni dalla ricezione della segnalazione, accettando di conformarsi alla decisione di tale organo.

4. Nel caso di rimozione, mantenga il contenuto come prova e lo conservi per questo scopo per un periodo di dieci settimane nel rispetto delle direttive 2000/31/CE e 2010/13/UE.

5. Informi senza indugio chi ha inoltrato la segnalazione e l'utente di qualsiasi decisione adottata e ne fornisca le motivazioni.

(3) La procedura deve garantire che ogni segnalazione e ogni misura adottata vengano documentati nel rispetto delle direttive 2000/31/CE e 2010/13/EU.

(4) La gestione delle segnalazioni deve essere monitorata dal managementdel social network con controlli mensili. Ogni carenza organizzativa nella gestione delle segnalazioni ricevuti deve essere immediatamente corretta. Il management del social network deve garantire ai soggetti preposti alla gestione delle segnalazioni corsi di formazione e programmi di supporto in lingua tedesca; questo deve accadere non meno di una volta ogni sei mesi.

(5) Le procedure di cui al comma (1) possono essere supervisionate da un soggetto designato dall'autorità amministrativa indipendente di cui al § 4.

(6) Un organismo viene riconosciuto come organo di autoregolamentazione ai sensi della presente legge se:

1. Assicuri l'indipendenza e le capacità tecniche delle proprie risorse,

2. Offra mezzi adeguati per garantire una valutazione rapida entro sette giorni,

3. Abbia adottato norme di procedura che regolino lo scopo e la durata della valutazione, stabiliscano i requisiti di ammissione dei social network affiliati e prevedano la possibilità di riesaminare le decisioni,

4. Abbia attivato un servizio di ricezione delle segnalazioni e,

5. Sia finanziato da diversi gestori di social network o istituzioni garantendo la disponibilità di mezzi adeguati. L"organismo deve rimanere aperto all'adesione di altri prestatori di servizi e in particolare di social network.

(7) La decisione di accreditamento di un organo di autoregolamentazione è presa dall'autorità amministrativa di cui all'articolo 4.

(8) L'accreditamento può essere revocato in tutto o in parte o collegato al soddisfacimento di ulteriori requisiti se qualcuna tra le condizioni iniziali non viene più soddisfatta.

(9) L'autorità amministrativa di cui al § 4 può anche inibire temporaneamente l'esercizio della-facoltà del social network di rimettere le decisioni ad un organo di autoregolamentazione di cui al comma (2), n. 3), lettera b) ove ci sia un ragionevole motivo per pensare che il prestatore sia venuto meno agli obblighi di cui al comma (2), numero 3, non affiliandosi al sistema di autoregolamentazione.

§ 4
Sanzioni

(1) È illecito ogni atto commesso da chi, con dolo o colpa,

1. Contrariamente al § 2, comma (1), primo periodo, non provvede al rapporto, o non vi provvede in maniera corretta e completa entro i termini, oppure non lo pubblica, o non lo pubblica correttamente, o maniera completa, secondo le modalità previste o entro i termini,

2. Contrariamente al § 3, comma (1), primo periodo, non predispone, o non predispone correttamente o in maniera completa una procedura per la gestione delle segnalazioni delle associazioni o degli utenti residenti o domiciliati nella Repubblica Federale tedesca,

3. Contrariamente al § 3, comma (1), secondo periodo, non prevede una procedura di cui sopra o non la mette a disposizione correttamente,

4. Contrariamente al § 3, comma (4), primo periodo, non attua il monitoraggio della gestione delle segnalazioni o non lo attua correttamente,

5. Contrariamente al § 3, comma (4), secondo periodo, non corregge una carenza organizzativa o non la elimina tempestivamente,

6. Contrariamente al § 3, comma (4), terzo periodo, non offre o non fornisce tempestivamente formazione o supporto,

7. Contrariamente al § 5, non nomina una persona autorizzata a ricevere notifiche nella Repubblica Federale tedesca o non nomina una persona autorizzata a ricevere richieste di informazioni nella Repubblica Federale tedesca o,

8. contrariamente al § 5, comma (2), secondo periodo, non risponde alla richieste di informazioni agendo come soggetto autorizzato a ricevere notifiche.

(2) Nel caso di violazione dell'art. 5, può essere inflitta un'ammenda fino a cinquecentomila euro; nel caso di violazione dell'art. 2, comma (1) e 3 commi (1) e (4), un'ammenda fino a cinque milioni di euro. Si applica in ogni caso il § 30, comma secondo, terzo periodo, della legge sugli illeciti amministrativi.

(3) La sanzione può essere applicata anche se il fatto non viene compiuto all'interno della Repubblica Federale tedesca.

(4) L'autorità amministrativa competente ai sensi del § 36, comma (1), n. 1, della legge sugli illeciti amministrativi è l'Ufficio Federale di giustizia. Il Ministero Federale della giustizia e tutela dei consumatori, di concerto con il Ministero Federale degli interni, il Ministero dell'economia e l'energia e il Ministero dei trasporti e delle infrastrutture digitali fissa i principî amministrativi generali di cui l'autorità di regolamentazione deve tenere conto nell'accertare una violazione degli obblighi a carico dei gestori dei social network e nel determinare l'importo della relativa sanzione.

(5) L'autorità amministrativa competente può adottare un provvedimento basato sul fatto che i contenuti che non sono stati rimossi o sbloccati sono illeciti ai sensi del § 1, comma (3), previa decisione giudiziale che stabilisca la loro illiceità. Il tribunale competente a decidere sulla questione è quello chiamata a decidere sul ricorso avverso le relative sanzioni. La domanda di pronuncia pregiudiziale deve essere trasmessa al tribunale insieme alla dichiarazione del social network. La domanda può essere decisa anche senza udienza orale. La decisione non è impugnabile ed è vincolante per l'autorità amministrativa.

§ 5
Persona autorizzata a ricevere notifiche nella Repubblica Federale tedesca

(1) I gestori dei social network devono nominare una persona autorizzata a ricevere notifiche nella Repubblica Federale tedesca e darne notizia sulla loro piattaforma in un modo facilmente individuabile e immediatamente accessibile. È possibile notificare a tale soggetto i procedimenti di cui al § 4 o i procedimenti giudiziari per la diffusione di contenuti illeciti avviato innanzi i tribunali tedeschi, nonché i relativi atti di promovimento.

(2) Al fine di garantire la ricezione delle richieste di informazioni da parte delle autorità nazionali incaricate dell'applicazione della legge, i gestori dei social network devono individuare una persona residente in Germania autorizzata a ricevere tali richieste. La persona autorizzata è tenuta a rispondere alle richieste di informazioni ai sensi del primo periodo entro 48 ore dalla loro ricezione. Nel caso in cui le informazioni richieste non vengano fornite in maniera esaustiva, ne deve essere data motivazione.

§ 6
Disposizioni transitorie

(1) La pubblicazione del resoconto di cui al § 2 è obbligatoria a partire dal primo semestre 2018.

(2) Le procedure di cui al § 3 devono essere introdotte entro tre mesi dall'entrata in vigore della presente legge, e comunque entro tre mesi da quando i fornitori di un social network soddisfano i requisiti del § 1 solo in seguito.

Articolo 2
Modifiche alla Legge sulle telecomunicazioni (*Telemediengesetz*)

La legge sulle telecomunicazioni del 26 febbraio 2007, modificata per ultimo dall'articolo 1 della legge 21 luglio 2016, è modificata come segue:

1. Al paragrafo 14 sono aggiunte i seguenti commi da (3) a (5):

"(3) Inoltre, il prestatore di servizi può, in singoli casi, fornire informazioni
circa i dati degli abbonati in suo possesso, nella misura in cui ciò sia necessario per le richieste di tutela civile per violazione di diritti assoluti derivante da un contenuto illecito come definito nel § 1, comma (3) del NetzDG.

(4) L'ostensione delle informazioni ai sensi del comma (3) deve essere autorizzata dall'autorità giudiziaria, su richiesta dalla parte offesa. La competenza spetta al tribunale regionale, a prescindere del valore della domanda. E' territorialmente competente il tribunale civile nel cui distretto la parte offesa ha la residenza, il domicilio, o la sede. Le disposizioni della legge sui procedimenti in materia familiare
e in materia di giurisdizione volontaria si applicano conformemente.
Le spese giudiziarie sono a carico della parte offesa. Contro la decisione del tribunale regionale è ammesso ricorso in appello.

(5) Il prestatore di servizi è coinvolto come parte interessata nei procedimenti
di cui al comma (4). Può informare l'utente dell'avvio del procedimento".

2. Nel § 15, comma (5), il quarto periodo è formulato come segue:

"Il § 14, commi da 2 a 5 si applicano conformemente.

Articolo 3
Entrata in vigore

La presente legge entrerà in vigore il primo ottobre 2017.

media LAWS

ANNO 2017 - CODICE ISSN 2532-9146