Maria Romana Allegri

Ubi Social, Ibi Ius

Fondamenti costituzionali dei *social network* e profili giuridici della responsabilità dei *provider*

FrancoAngeli
OPEN ACCESS

STUDI DI DIRITTO PUBBLICO

Collana diretta da **Roberto Bin**, **Fulvio Cortese** e **Aldo Sandulli**
coordinata da **Simone Penasa** e **Andrea Sandri**

La Collana promuove la rivisitazione dei paradigmi disciplinari delle materie pubblicistiche e l'approfondimento critico delle nozioni teoriche che ne sono il fondamento, anche per verificarne la persistente adeguatezza.
A tal fine la Collana intende favorire la dialettica interdisciplinare, la contaminazione stilistica, lo scambio di approcci e di vedute: poiché il diritto costituzionale non può estraniarsi dall'approfondimento delle questioni delle amministrazioni pubbliche, né l'organizzazione e il funzionamento di queste ultime possono ancora essere adeguatamente indagati senza considerare l'espansione e i modi di interpretazione e di garanzia dell'effettività dei diritti inviolabili e delle libertà fondamentali. In entrambe le materie, poi, il punto di vista interno deve integrarsi nel contesto europeo e internazionale.
La Collana, oltre a pubblicare monografie scientifiche di giovani o affermati studiosi (**STUDI E RICERCHE**), presenta una sezione (**MINIMA GIURIDICA**) di saggi brevi destinata ad approfondimenti agili e trasversali, di carattere propriamente teorico o storico-culturale con l'obiettivo di sollecitare anche gli interpreti più maturi ad illustrare le specificità che il ragionamento giuridico manifesta nello studio del diritto pubblico e le sue più recenti evoluzioni.
La Collana, inoltre, ospita volumi collettanei (sezione **SCRITTI DI DIRITTO PUBBLICO**) volti a soddisfare l'esigenza, sempre più avvertita, di confronto tra differenti saperi e di orientamento alla lettura critica di problemi attuali e cruciali delle discipline pubblicistiche.
La Collana, inoltre, si propone di assecondare l'innovazione su cui si è ormai incamminata la valutazione della ricerca universitaria. La comunità scientifica, infatti, sente oggi l'esigenza che la valutazione non sia più soltanto un compito riservato al sistema dei concorsi universitari, ma si diffonda come responsabilità dell'intero corpo accademico.
Tutti i volumi, pertanto, saranno soggetti ad un'accurata procedura di valutazione, adeguata ai criteri fissati dalle discipline di riferimento.

Maria Romana Allegri

Ubi Social, Ibi Ius

Fondamenti costituzionali dei *social network* e profili giuridici della responsabilità dei *provider*

FrancoAngeli
OPEN ACCESS

SDP Studi di Diritto Pubblico

Il volume è stato pubblicato con il contributo del Dipartimento di Comunicazione e Ricerca Sociale della Sapienza Università di Roma.

INDICE

Introduzione pag. 9

Definire l'oggetto di studio: incursioni nella letteratura sociologica » 15

1. *Social media*, *social network* e *user-generated content* » 15

2. Relazioni umane, informazione e comunicazione nella *network society* » 19

I *social network* in una prospettiva costituzionalistica » 29

1. Le *social network communities* come formazioni sociali *ex* art. 2 Cost. » 29

2. Le *social network communities* come associazioni *ex* art. 18 Cost. » 37

3. L'attività di *social networking* come riunione *ex* art. 17 Cost. » 44

La responsabilità civile degli intermediari digitali per gli illeciti commessi dagli utenti » 53

1. L'impianto normativo: la direttiva n. 2000/31/Ce e il d. lgs. n. 70/2003 » 53

1.1. Le tre categorie di intermediari digitali » 55

1.2. Gli obblighi gravanti sugli Isp e le limitazioni di responsabilità » 58

1.3. L'evoluzione del ruolo degli Isp » 60

2. La giurisprudenza della Corte di giustizia dell'Unione europea: irresponsabilità dell'Isp neutrale e illegittimità degli obblighi di sorveglianza preventiva » 61

3. La giurisprudenza italiana: la discussa categoria del c. d. "*hosting* attivo" che non beneficia dell'esenzione da responsabilità pag. 65

Il trattamento dei dati personali da parte degli intermediari digitali: vincoli e responsabilità » 75
1. L'impianto normativo » 75
1.1 Dalla privacy *all'*habeas data » 75
1.2. Il fondamento costituzionale del diritto alla riservatezza » 77
1.3. La normativa sul trattamento dei dati personali e la "esenzione domestica" » 80
1.4. Il nuovo regolamento europeo sulla protezione dei dati personali » 82
1.5. L'applicazione della normativa sulla protezione dei dati personali ai social network sites » 86
1.6. La tutela dell'identità personale nel caso dei falsi account » 89
1.7. La profilazione degli utenti » 91
1.8. Il diritto all'oblio » 94
2. Licenze d'uso e *privacy policies* dei *social network* » 99
2.1. Le licenze d'uso come contratti sinallagmatici » 99
2.2. La dichiarata (ma insostenibile) estraneità dei social network provider *rispetto alle condotte degli utenti* » 101
2.3. Bring Your Own Identity » 105
3. Profili giurisprudenziali sul trattamento dei dati personali da parte dei *provider*: il caso *Google c. ViviDown* » 105
4. Spunti dalla giurisprudenza italiana: la responsabilità di *Facebook* per la mancata rimozione di contenuti lesivi della *privacy* e della dignità personale » 110
5. La responsabilità dei motori di ricerca per il trattamento dei dati personali: il caso *Google Spain* » 114
6. *Excursus*: il rapporto fra libertà di cronaca e diritto all'oblio nella giurisprudenza della Corte di Cassazione » 125

La responsabilità "editoriale" degli intermediari digitali per i contenuti diffamatori prodotti dagli utenti » 131
1. Analogie e sinergie fra *social network* ed editoria tradizionale » 131

2. La Corte di Giustizia dell'Unione europea nel caso *Papasavvas c. O Fileleftheros* pag. 134
3. La giurisprudenza della Corte europea dei diritti dell'uomo sulla responsabilità dell'editore *online* per i contenuti *user-generated* » 136
3.1. Il caso Delfi » 138
3.2. Il caso Mte e Index c. Ungheria » 147
3.3. Il caso Pihl c. Svezia » 149
4. Orientamenti giurisprudenziali della Corte di Cassazione in tema di responsabilità editoriale nel caso delle pubblicazioni *online* » 152

Profili di responsabilità penale degli intermediari digitali in prospettiva *de jure condendo* » 159
1. Il concorso nel reato » 159
2. Il reato omissivo improprio » 166

Strategie di contrasto alla diffusione delle manifestazioni di odio e delle notizie false tramite i *social network* » 175
1. Il contrasto allo *hate speech*: repressione penale e sistemi di autoregolamentazione » 175
2. Libera manifestazione del pensiero, dovere di verità e notizie false » 187
2.1. La verità come bene giuridico costituzionalmente protetto » 189
2.2. L'obbligo della verità nella professione giornalistica » 192
2.3. La diffusione notizie false come pericolo per l'ordine pubblico » 196
2.4. Tentativi di reazione alla proliferazione delle fake news *e dell'odio* online » 200
3. Le indicazioni della Commissione europea per contrastare la diffusione di contenuti illeciti in Internet » 206

Conclusioni » 213

Riferimenti bibliografici » 227

INTRODUZIONE

A gennaio 2017 la metà della popolazione mondiale risultava disporre di una connessione a Internet, il 10% in più rispetto all'anno precedente. Il 37% della popolazione mondiale (cioè 2,8 miliardi di persone) utilizzava piattaforme di *social networking* – con un incremento del 21% rispetto all'anno precedente – e più di un terzo di questi vi accedeva tramite dispositivi mobili. Le piattaforme più frequentate risultavano essere *Facebook*, *Whatsapp* e *YouTube*, seguite da altre meno note in Italia, mentre *Instagram* e *Twitter* si posizionavano rispettivamente al nono e al decimo posto. In Italia, sempre all'inizio del 2017, il 66% della popolazione (circa 39 milioni di persone) disponeva di una connessione a Internet, il 4% in più rispetto al 2016. Ben 31 milioni di persone (il 52% della popolazione) utilizzavano i *social media* (tre milioni in più rispetto all'anno precedente), moltissimi dei quali (28 milioni) anche mediante dispositivi mobili. L'86% degli utenti dei *social network* vi accedeva quotidianamente. Le piattaforme più utilizzate risultavano essere *YouTube*, *Facebook*, *Whatsapp*, *Instagram* e *Twitter*. La maggior parte degli utenti italiani dei *social network* aveva fra 18 e 55 anni, i minorenni rappresentavano circa l'1% e gli ultra-cinquantacinquenni poco più del 2%.

Questi dati, contenuti in un recente rapporto pubblicato dall'agenzia creativa *We Are Social*[1], sono i più aggiornati fra quelli disponibili al momento e appaiono impressionanti non solo per l'entità dei numeri, ma anche perché danno evidenza di un fenomeno in continua crescita, che inevitabilmente cattura l'attenzione di chi lo osserva dal punto di vista delle più diverse discipline. L'attenzione del giurista, allora, non può che soffermarsi sulle norme – quelle già esistenti o quelle auspicabili in prospettiva *de jure condendo* – che regolano o dovrebbero regolare i *social media*: un oggetto di studio assai complesso, sia perché oggi "tutto diventa *social*" e quindi la definizione stessa di *social network* assume contorni sfuggenti, sia perché i

[1] https://wearesocial.com/it/blog/2017/01/digital-in-2017-in-italia-e-nel-mondo.

diversi attori in campo giocano ruoli che tendono a mescolarsi e a sovrapporsi, rendendo rapidamente inadeguate e obsolete le categorie previste nel diritto positivo.

Gli utenti non si limitano più ad utilizzare un servizio per ricevere contenuti, come nel caso dei tradizionali mezzi di comunicazione *one-to-many,* ma in qualche modo producono essi stessi il servizio – consistente nella condivisione di informazioni – attraverso la rete di interconnessioni su cui il *social medium* è costruito. Inoltre, gli utenti non si limitano più a fruire di contenuti eteroprodotti ed eterodiffusi, ma si fanno essi stessi produttori e disseminatori di informazioni all'interno di in un percorso reticolare. I *provider* non svolgono più solo un ruolo di intermediazione neutrale, come presupposto dalla normativa tuttora vigente, ma sempre più spesso intervengono – con procedure non sempre trasparenti – nell'organizzazione e nella gestione dei contenuti. La loro attività quindi può essere paragonata – con qualche approssimazione, ma non infondatamente – a quella degli editori tradizionali, riflessione che impone un radicale ripensamento delle loro responsabilità. Il prodotto dell'attività di condivisione, cioè l'informazione, non acquista significato solo in virtù del suo contenuto, ma anche – o forse soprattutto – in virtù del suo "posizionamento", cioè del numero e della qualità delle interazioni fra utenti prodotte intorno ad essa: l'autorevolezza della fonte e l'attendibilità della notizia cedono il passo alla "viralità" del messaggio, sganciando totalmente l'esercizio del diritto alla libera manifestazione del pensiero dai suoi effetti, cioè dal contenuto che si condivide. La circolazione di notizie false e distorte e di contenuti che incitano all'odio e alla violenza, allora, rischia di rendere la libertà di informazione, da sempre considerata irrinunciabile baluardo di ogni ordinamento democratico, un pericolo per la democrazia, a meno che la stessa tecnologia che ha prodotto tali distorsioni non riesca ad approntare anche adeguati rimedi per correggerle.

Lo scopo di questo libro è proprio quello di capire, attraverso lo studio dei *social network* e in particolare del regime di responsabilità previsto per gli intermediari digitali, se e in che modo il diritto possa offrire soluzioni valide per ovviare ai principali problemi che l'enorme diffusione dei *social network* pone con intensità sempre maggiore, fino a che punto i rimedi esclusivamente tecnici possano risultare efficaci e se e come possa essere composta l'inevitabile tensione fra eteronormazione e *self-regulation*. Il timore, infatti, è che ogni sforzo compiuto attraverso gli istituti del diritto positivo venga vanificato a causa della rapidità con cui le innovazioni tecnologiche modificano l'aspetto e i confini del fenomeno che si vorrebbe regolamentare, nonché della sua dimensione globale e transnazionale, dinanzi alla quale gli ordinamenti giuridici nazionali appaiono inadeguati. Tuttavia,

pensare di affidare alla sola opera interpretativa dei giudici il compito di adeguare l'ordinamento giuridico vigente agli scenari della contemporaneità, oppure puntare solo sulle pratiche di responsabilizzazione degli utenti e di auto-regolamentazione dei gestori delle piattaforme, può provocare incertezza, disomogeneità nella tutela dei diritti individuali e persino abusi.

Al fine di una migliore comprensione del fenomeno che si intende studiare, è bene che la riflessione giuridica si arricchisca anche dell'apporto di altri saperi. Quindi, nel primo capitolo del libro si ricorre agli studi prodotti principalmente nell'ambito della sociologia della comunicazione per comprendere cosa sono e come funzionano i *social network* nell'ambito del contesto più generale dei *social media*, quale impatto essi abbiano sul modo di relazionarsi fra le persone e sulla circolazione delle informazioni, e cosa si intende esattamente per contenuti *user-generated*.

Il secondo capitolo affronta invece il tema in una prospettiva costituzionalistica, dapprima considerando i *social network* come "formazioni sociali" *ex* art. Cost., poi valutando l'ipotesi della loro analogia con una delle formazioni sociali di rilevanza costituzionale, cioè le associazioni di cui all'art. 18 Cost., infine esaminando la possibilità che, nel momento in cui varie persone interagiscono fra loro attraverso un'attività di *social networking*, quest'ultima possa essere paragonata a una riunione *ex* art. 17 Cost. e quindi debba svolgersi in modo pacifico, tale da non turbare la sicurezza e l'incolumità pubbliche.

Il terzo capitolo si concentra, in particolare, sull'estensione della responsabilità civile degli intermediari digitali per i contenuti prodotti dagli utenti che circolano nei *social network*, alla luce della direttiva 2000/31/Ce e del decreto legislativo che in Italia ne ha dato attuazione (n. 70/2003). Si vedrà, allora, come la presunta posizione di neutralità dell'*hosting provider*, su cui si fonda il regime di limitazione della responsabilità, non corrisponde più al ruolo che i *provider* svolgono effettivamente oggi, in un contesto tecnologico molto più evoluto rispetto al periodo in cui le norme vigenti sono state approvate. Ciò ha dato vita ad una giurisprudenza, sia a livello europeo che nazionale, piuttosto oscillante e a tratti innovativa, che non nasconde però la difficoltà di dover interpretare e applicare oggi norme non più al passo con i tempi. Il problema è che ogni tentativo di gravare gli intermediari digitali di responsabilità relative agli illeciti commessi dagli utenti attraverso la messa in circolazione di taluni contenuti si scontra con la questione dell'assoluta inopportunità di affidare a soggetti privati poteri censori.

Il quarto capitolo muove dalla constatazione che oggi le questioni inerenti il trattamento dei dati personali sempre più hanno a che fare con la possibilità di mantenere il controllo sulle "tracce digitali" che ciascuno di

noi lascia in Rete. Attraverso tali tracce è possibile ricostruire importanti aspetti della personalità individuale; il fatto che la loro circolazione sfugga al controllo della persona cui i dati si riferiscono lede il diritto soggettivo di decidere che cosa far conoscere agli altri di se stesso, fino a che punto e quanto a lungo. Il problema è che con l'iscrizione ad un *social network* l'utente sottoscrive un contratto con il quale, spesso senza averne piena consapevolezza, permette al gestore della piattaforma e agli altri utenti l'accesso alle informazioni inserire nel proprio profilo *social*. Tramite queste informazioni, che ben difficilmente potranno più essere cancellate una volta immesse in un circuito di condivisione con altri, il *provider* può organizzare e presentare a ciascun utente una serie di contenuti informativi selezionati in base alle preferenze individuali, oltre a trarre profitto dalle inserzioni pubblicitarie mirate. Ci si chiede, allora, anche alla luce del nuovo regolamento europeo sul trattamento dei dati personali, in vigore dal 25 maggio 2018, e con l'ausilio di alcuni noti casi giurisprudenziali, se sia corretto investire unicamente l'utente del *social network* di ogni responsabilità relativa alla circolazione delle informazioni personali, o se non sia piuttosto opportuno investirne anche gli intermediari digitali in qualche forma.

Il mutato ruolo dei *social network provider*, non più semplicemente neutrale ma proattivo, e le sinergie sempre più sviluppate fra i *social network* e il settore dell'editoria al fine di ampliare il bacino di utenza dell'informazione giornalistica, suggeriscono alcune analogie fra i gestori delle piattaforme di *social networking* e gli editori tradizionali, che le norme vigenti gravano di specifiche responsabilità sui contenuti pubblicati proprio in virtù della loro posizione, che comporta la supervisione dei contenuti. Questo è appunto il tema trattato nel quinto capitolo che, attraverso l'analisi della giurisprudenza della Corte europea dei diritti dell'uomo e, a livello italiano, della Corte di Cassazione, suggerisce alcune aperture in tal senso.

Un'altra questione, cui è dedicato il sesto capitolo, è quella della possibilità o dell'opportunità di gravare i *provider* anche di responsabilità penali nel caso in cui, attraverso i servizi da essi offerti. vengano compiuti dei reati. La responsabilità potrebbe essere loro ascritta a titolo di concorso con l'autore della condotta illecita oppure a titolo omissivo, nel caso in cui il *provider* non abbia preventivamente controllato i contenuti diffusi o non sia stato solerte nel rimuovere quelli illeciti. Entrambe le ipotesi trovano scarsi appigli nella giurisprudenza e presentano non pochi profili problematici, ma non sono del tutto infondate.

L'ultimo capitolo, infine, mira ad individuare quali strumenti normativi, accanto ai rimedi tecnici e alla *self-regulation* dei gestori delle piattaforme, possono contribuire a porre un argine alla diffusione attraverso i *social network* di contenuti incitanti all'odio e alla violenza e di informazioni false e

distorte. Si tratta di contenuti la cui diffusione influisce sulla formazione dell'opinione pubblica, in contrasto con il sistema democratico-pluralista, sia perché offendono la dignità umana e inducono alla discriminazione, sia perché ingenerano nel pubblico false credenze e convinzioni in modo incompatibile con il "dovere di verità", desumibile anche dall'interpretazione dell'art. 21 Cost., cui dovrebbe invece attenersi chi svolge il delicato compito di informare.

DEFINIRE L'OGGETTO DI STUDIO: INCURSIONI NELLA LETTERATURA SOCIOLOGICA

1. *Social media*, *social network* e *user-generated content*

Prima di affrontare il tema centrale di questa ricerca, occorre forse fare chiarezza sull'esatto significato di due espressioni – *social network* e *social media* – che spesso vengono usate come sinonimi, ma che in realtà andrebbero distinte. Parimenti, occorre definire cosa si intende esattamente per *user-generated content* (contenuti prodotti dagli utenti), che vanno distinti dai contenuti semplicemente *user-distributed*. A tal fine, può risultare utile la consultazione dei principali studi prodotti in ambito sociologico su questi temi, nella convinzione che, per una più completa ed efficace comprensione dei fenomeni che caratterizzano la società del nostro tempo, l'analisi giuridica non possa prescindere dall'apporto delle altre discipline.

Il termine *social network* (rete sociale) è stato utilizzato per la prima volta nel 1954 dall'antropologo australiano John Arundel Barnes[1] per indicare un reticolo di rapporti fra persone legate fra loro da rapporti di amicizia, parentela e conoscenza che ciascuno eredita o costruisce vivendo all'interno della società. Si tratta di una rete di relazioni fluttuanti, mutevoli e polivalenti, flessibile, senza confini, priva di organizzazione o coordinamento. In questo sistema reticolare, ogni persona è in contatto con un certo numero di altre persone che non necessariamente si conoscono fra loro; dunque, mentre alcuni sono in contatto diretto fra loro, altri hanno rapporti solo indiretti. Graficamente queste relazioni possono essere rappresentate attraverso punti uniti da linee: i punti rappresentano le persone e le linee i legami di interazione fra di esse.

[1] J. A. Barnes (1954), *Class and Committees in a Norwegian Island Parish*, in *Human Relations*, n. 7, pp. 39-58. Il saggio di Barnes, insieme a quello di altri Autori che si sono occupati di reti sociali, può essere letto in traduzione italiana in F. Piselli (1995) (a cura di), *Reti. L'analisi di network nelle scienze sociali*, Roma, Donzelli.

Questo è il tipo di relazione che intercorre non solo fra individui appartenenti a una determinata comunità sociale di natura fisica, come quella studiata da Barnes, ma anche in effetti fra coloro che oggi interagiscono grazie alle opportunità offerte da Internet, producendo e condividendo contenuti informativi di vario genere via Internet.

Lo sviluppo delle reti sociali attraverso Internet è stato reso possibile dall'avvento del cosiddetto *web 2.0*. Il termine *web 2.0* è comparso per la prima volta nel titolo di un ciclo di conferenze organizzate nel 2005 dall'editore americano Tim O'Reilly[2], dedicate ad una nuova generazione di applicazioni informatiche caratterizzate da una forte interazione fra sito Internet e utenti dei servizi, nonché degli gli utenti fra loro: dunque, gli utenti dei servizi via Internet tendono a trasformarsi da semplici fruitori dei contenuti in autori degli stessi (i cosiddetti *prosumers*[3]o anche *produsers*[4]) e a condividere tra loro tali contenuti in modo più semplice ed efficiente[5]. Grazie alle possibilità di interazione offerte dal *web 2.0* si è sviluppato un universo di comunicazione completamente nuovo, un nuovo *medium* costituito da reti di computer, il cui linguaggio è digitale, e i cui trasmettitori sono distribuiti globalmente e globalmente interattivi. Si può parlare allora, secondo Castells, di *network society*[6], il cui fondamento comunicativo è costituito dal sistema globale di reti di comunicazione orizzontale, attraverso cui avviene uno scambio multimodale di messaggi interattivi "da molti a molti", sincroni e asincroni. Ciò ha dato vita a una nuova forma di comunicazione "socializzata", di tipo multimodale, che Castells definisce "autocomunicazione di massa" (*mass self-communication*): un tipo di comunicazione autonomo a livello di generazione di contenuti, gestione dell'emissione e selezione della ricezione nell'ambito dell'interazione *many-to-many*[7].

[2] http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html.

[3] Secondo la definizione di E. Menduni (2008), *Voce "prosumer"*, in *Enciclopedia della scienza e della tecnica*, Roma, Treccani, questa espressione, coniata da Alvin Toffler nel libro *The third wave* (1980), è una crasi dei termini *producer* e *consumer* che indica un consumatore che è a sua volta produttore o, nell'atto stesso che consuma, contribuisce alla produzione.

[4] G. Boccia Artieri (2012), *Stati di connessione. Pubblici, cittadini e consumatori nella (Social) Network Society*, Milano, Franco Angeli, pp. 137-143.

[5] Z. Bauman (2002), *Il disagio della postmodernità*, Milano, Mondadori, ha parlato di "cooperativa di consumatori" a proposito della cultura nella postmodernità, in cui "autore" e "attore" sono due aspetti della stessa persona, e il cui asse portante non è la produzione di cultura, ma la produzione di un numero sempre maggiore di consumatori (partic. pp. 135, ma in generale sulla cultura della postmodernità pp. 126-138).

[6] M. Castells (2007), *Communication, Power and Counter-power in the Network Society*, in *International Journal of Communication*, n. 1, partic. pp. 246-248 (trad. it: http://www.caffeeuropa.it/socinrete/castells.pdf).

[7] *Ibid.*

La tecnologia *networked* ha la capacità di distribuire orizzontalmente messaggi cui la coscienza pubblica sente di potere dare fiducia[8]. Ecco dunque che gli attori sociali, singoli o organizzati, possono avvalersi delle opportunità offerte dalla tecnologia – e, in particolare, dei mezzi della *mass self-communication* – per perseguire i propri obiettivi e tentare di convincere l'opinione pubblica delle loro idee, attraverso continui scambi e interazioni fra i nuovi media e i media *mainstream*: gli attori che si battono per il cambiamento sociale si avvalgono spesso della piattaforma Internet quale strumento per influenzare l'agenda dei media tradizionali, mentre le élite politiche fanno uso sempre maggiore di metodi e strumenti della *mass self-communication*[9].

La rete Internet non rappresenta per le istanze sociali solo un mezzo di comunicazione, ma ne plasma anche la struttura organizzativa, che viene appunto costruita intorno alla comunicazione *networked*. La logica del *networking* consente addirittura di attribuire percettivamente una forma organizzativa anche a realtà non organizzate, sviluppando nuove forme di associazionismo "fluido" per le quali le relazioni sociali assurgono a dimensione costitutiva attraverso i *social network*[10]. Si è parlato di "scorciatoie sociali" per definire quei legami deboli (ad esempio, l'"amicizia" via *Facebook*) attraverso cui nei *social network* si formano le aggregazioni sociali[11].

Nel linguaggio corrente della contemporaneità, l'espressione *social network* sta ad indicare quelle reti sociali che nascono e si sviluppano attraverso il *web*, e questo è il senso con cui l'espressione verrà utilizzata in questo libro. Per essere precisi, però, quando si vogliono indicare i siti Internet che ospitano reti sociali sarebbe più corretto parlare di *social network sites* (Sns) o di *piattaforme di social networking*. Secondo la definizione di Boyd e Ellison[12], i *social network sites* sono servizi basati sul web che permettono agli individui: 1) di costruire un proprio profilo pubblico o semi-pubblico all'interno di un sistema circoscritto; 2) di articolare una lista di altri utenti con cui condividere connessioni; 3) di vedere e attraversare questa lista di contatti, come pure quelle di altri utenti del sistema. Per gli Autori, il fine principale degli utenti dei Sns non è tanto quello di espandere le proprie conoscenze, quanto piuttosto quello di rendere visibile il proprio

[8] Ivi, p. 251.
[9] Ivi, p. 252.
[10] Boccia Artieri (2012), cit. (partic. pp. 30-31).
[11] Boccia Artieri (2012), cit., pp. 105-107.
[12] D. M. Boyd e N. B. Ellison (2008), *Social Network Sites: Definition, History, and Scholarship*, in *Journal of Computer-Mediated Communication*, n. 13, p. 211.

profilo – e ovviamente le informazioni in esso contenute – ad un pubblico più o meno ampio e più o meno rigidamente selezionato.

Chiaramente, grazie al *web 2.0* non si sono sviluppati solo i *social network sites*, ma tutta la più vasta categoria dei *social media*, di cui i *social network* costituiscono in realtà un sottogruppo. Secondo la definizione di Kaplan e Haenlein[13], i *social media* sono un gruppo di applicazioni basate su Internet e costruite sui paradigmi ideologici e tecnologici del *web 2.0,* che permettono la creazione e lo scambio di contenuti generati dall'utente (*user-generated content* o Ugc)[14]. Dunque, tutte le applicazioni informatiche attraverso cui è possibile condividere testi, immagini, video e file audio, che riescono a raggiungere istantaneamente un pubblico globale, possono essere considerate *social media*, purché però in esse prevalga la condivisione di *user-generated content* accanto eventualmente anche a contenuti di altro tipo[15]. Sempre secondo Kaplan e Haenlein[16], che si basano su un documento di lavoro elaborato dall'Oece nel 2006[17], gli Ugc devono avere tre caratteristiche fondamentali: devono essere diffusi attraverso siti internet accessibili a tutti o comunque a un buon numero di utenti selezionati (escludendo quindi i contenuti veicolati attraverso *e-mail* o servizi di messaggeria istantanea); devono mostrare almeno un minimo sforzo creativo da parte dell'utente (escludendo quindi la mera diffusione di contenuti prodotti da altri); devono essere prodotti al di fuori delle pratiche professionali e commerciali (escludendo quindi i messaggi pubblicitari e altri contenuti prodotti solo con finalità commerciali). Una caratteristica propria dei contenuti diffusi attraverso i *social media* è quella di acquisire valore e significato spesso solo in relazione al contesto comunicativo in cui essi vengono diffusi e condivisi (cioè, attraverso i commenti degli altri utenti, le pratiche di *sharing*, i *like*, i *re-tweet*)[18].

[13] A. M. Kaplan e M. Haenlein (2010), *Users of The World, Unite! The Challenges and Opportunities of Social Media*, in *Business Horizons*, n. 53, p. 61.

[14] Sul crescente fenomeno della creazione di contenuti da parte degli utenti di Internet si veda L. Ranie e B. Wellman (2012), *Networked. Il nuovo sistema operativo sociale*, a cura di A. Marinelli e F. Comunello, Milano, Guerini, partic. pp. 295-324. Per una definizione di *user-generated content* e per le sue ripercussioni sul diritto d'autore si veda M. Scialdone (2013), *Il nuovo ruolo degli utenti nella generazione di contenuti creativi*, in *Diritto, mercato, tecnologia*, n. 4, pp. 8-19.

[15] Per esempio gli *user distributed content* (Udc), cioè i contenuti prodotti a livello professionale, che gli utenti dei *social media* provvedono a condividere e diffondere.

[16] Ranie e Wellman (2012), cit.

[17] Oecd/Ocde, Working Party on the Information Economy, *Participative Web: User-Created Content*, 12 April 2007 (Dsti/Iccp/Ie(2006)7/Final).

[18] Boccia Artieri (2012), cit., pp. 88-90.

Sulla base di queste definizioni, Kaplan e Haenlein distinguono vari tipi di *social media*: i progetti collaborativi (es. *Wikipedia*), i *blog*, le *content communities* i cui gli utenti caricano contenuti anche a prescindere dalla creazione di una pagina personale (es. *YouTube* o *Slideshare*), i giochi *online* che consentono l'interazione fra giocatori, i mondi virtuali che riproducono la vita reale (es. *Second Life*) e naturalmente le piattaforme di *social networking*, come *Facebook, Twitter o Instagram*. I *social network* sarebbero dunque, secondo questa classificazione, un sottoinsieme della più vasta categoria dei *social media*. La loro peculiarità sarebbe costituita dal fatto che ogni utente si caratterizza attraverso la creazione di un proprio profilo ricco di informazioni personali di vario tipo e costruisce l'interazione con gli altri utenti proprio a partire dal profilo personale. L'aspetto della condivisione delle informazioni personali, con le connesse problematiche relative alla tutela della *privacy*, costituisce dunque un aspetto che nei *social network* assume una rilevanza ben maggiore che negli altri tipi di *social media*, anche se certamente non esclusiva.

Le definizioni di Kaplan e Haenlein, risalenti a qualche anno fa, possono oggi apparire un po' troppo rigide. Infatti, il massiccio sviluppo dei *social media* che si è verificato negli ultimi anni ha inevitabilmente portato a una commissione fra i vari tipi. Si pensi, ad esempio, al fatto che le *content communities* (come era almeno originariamente *YouTube*) e persino molti giochi *online* stanno sempre più avvicinandosi al tipo dei *social network* basati sulla costruzione di pagine personali attraverso le quali gli utenti possono interagire fra loro. Oppure al fatto che, attraverso servizi di messaggeria istantanea come *WhatsApp*, è possibile condividere con gruppi di utenti selezionati più o meno ampi contenuti di vario genere, fra cui anche *user-generated content*. O anche al fatto che le piattaforme di *social networking* – evidentissimo il caso di *Facebook* – vengano sempre più spesso utilizzate da aziende o singoli utenti con finalità di promozione commerciale di beni o servizi. Senza contare che sono gli stessi gestori dei *social media* a realizzare notevoli introiti derivanti dalla vendita di spazi pubblicitari sulle piattaforme da essi gestiti, particolarmente appetibili per gli inserzionisti perché gli annunci pubblicitari possono raggiungere destinatari selezionati attraverso la profilazione delle loro caratteristiche, gusti e preferenze, che avviene spesso all'insaputa degli utenti delle piattaforme.

2. Relazioni umane, informazione e comunicazione nella *network society*

Nell'analisi di Riva, condotta nell'ambito della ricerca psicologica e sociale, nel *social networking* si incontrano tre diverse tendenze: «l'uso dei

nuovi media sia come strumento di supporto alla propria rete sociale (organizzazione e estensione), sia come strumento di espressione della propria identità sociale (descrizione e definizione), sia come strumento di analisi dell'identità sociale degli altri membri della rete (esplorazione e confronto)»[19]. Per l'Autore, «ciò che differenzia i *social network* ai nuovi media disponibili in precedenza è la capacità di rendere visibili e utilizzabili le proprie reti sociali. Infatti, attraverso di essi è possibile identificare opportunità personali, relazionali e professionali altrimenti non immediatamente evidenti»[20]. Dunque, «l'introduzione dei *social network* non implica una semplice "rivoluzione tecnologica", ma anche una riconfigurazione delle opportunità di mediazione culturale a disposizione dei loro utenti»[21]. Il *social network* può essere considerato uno strumento di *empowerment* personale, in quanto permette a ciascuno di controllare e modificare la propria identità sociale, scegliendo che cosa condividere con gli altri e come farlo, e sperimentando nuovi modi di essere[22]: il risultato è un'identità fluida, flessibile e precaria, mutevole e incerta[23]. D'altro canto, la comunicazione attraverso i *social network* è "disincarnata", poiché l'elemento fisico (il corpo) e i significati che esso porta con sé non partecipano all'interazione; gli utenti dei *social network*, quindi, sono privati di un importante punto di riferimento nel processo di apprendimento e comprensione delle emozioni altrui, cosa che favorisce lo sviluppo dell'"analfabetismo emotivo"[24].

Nei *social network* «l'esperienza individuale trova senso nella connessione sociale, in una comunicazione che è alla ricerca di un riflesso in quella della relazione con gli altri (*like*, commento, condivisione)»[25]. L'esperienza acquista dunque valore solo attraverso lo *sharing*[26]. Grazie all'aumento delle relazioni sociali attraverso le reti di comunicazione, si sta creando «un concreto accesso generalizzato allo stato di contingenza del mondo, cioè a quell'orizzonte di possibilità in sé né necessarie né impossibili, che attraverso queste tecnologie di comunicazione diventano appunto accessibili e concretamente gestibili: possiamo infatti pensarci, comunicativamente, in una perenne connessione potenziale tra persone, cose e fatti, una connessione da poter attivare e gestire in tempo reale e a distanza attraverso gli strumenti del comunicare che pervadono la nostra vita quotidia-

[19] G. Riva (2010), *I social network*, Bologna, Il Mulino, p. 15.
[20] Ivi, p. 17.
[21] Ivi, p. 29.
[22] Ivi, p. 143.
[23] Ivi, p. 149 e 158.
[24] Ivi, p. 150.
[25] Boccia Artieri (2012), cit., p. 57.
[26] *Ibid.*

na»[27]. Queste dinamiche non generano però, come si potrebbe pensare *prima facie*, fenomeni di appartenenza dell'individuo a gruppi coesi e a sistemi di relazioni stabili, ma provocano ciò che Ranie e Wellman hanno definito come *networked individualism*, precisando che «nel mondo degli individui *networked* è la persona che si trova al centro, non la famiglia, l'unità lavorativa, il vicinato o il gruppo sociale»[28]. Dunque, persone come moltitudine di individui connessi mediante legami deboli e non come membri integrati di un gruppo[29].

Questa debolezza dei legami fra persone rientra nel più vasto fenomeno che Bauman ha rappresentato come "modernità liquida"[30], che investe anche la vita di relazioni: stiamo attraversando una fase di sfrenata deregolamentazione e flessibilizzazione dei rapporti sociali, in cui la priorità di ogni individuo è il consumo inteso come immediata soddisfazione di desideri autoreferenziali; l'incontro fra persone avviene in luoghi (ma anche in "nonluoghi"[31], come Internet) che facilitano l'incontro fra estranei[32], soddi-

[27] Ivi, p. 63.

[28] Ranie e Wellman (2012), cit., p. 25.

[29] Ivi, p. 32. Anche M. Castells (2009), *Comunicazione e potere*, Milano, Università Bocconi, p. 461, ha parlato a tale proposito di "individualismo reticolare", intendendo con tale espressione una cultura caratteristica della società in rete, che «ricostruisce le relazioni sociali sulla base di individui autodefiniti che mirano a interagire con gli altri seguendo le proprie scelte, i propri valori e interessi, trascendendo attribuzione, tradizione e gerarchia».

[30] Z. Bauman (2011), *Modernità liquida*, Roma-Bari, Laterza. Per illustrare il concetto di modernità liquida può essere utile riportare un brano tratto da p. XIII della prefazione: «La "liquidità" della nostra condizione è riconducibile soprattutto a ciò che è compendiato nel termine "deregolamentazione": alla separazione del potere (capacità di fare) dalla politica (capacità di decidere cosa fare), e di conseguenza a un'assenza o debolezza delle agenzie (cioè a un'inadeguatezza degli strumenti rispetto agli obiettivi) e al "policentrisimo" dell'azione in un pianeta integrato da una fitta ragnatela di interdipendenze. In parole povere, in condizione di "liquidità" tutto è possibile, ma nulla può essere fatto con certezza. L'incertezza è il risultato combinato del sentimento di ignoranza (impossibilità di sapere ciò che accadrà) e di impotenza (impossibilità di evitare che accada) e di una paura sfuggente e diffusa, definita in modo vago e difficile da localizzare: una paura che fluttua alla disperata ricerca di un punto fermo. Vivere nelle condizioni liquido-moderne è come camminare su un campo minato: tutti sanno che uno scoppio può verificarsi ovunque e in qualsiasi momento, ma nessuno sa dove e quando».

[31] Ivi, p. 113: «… i nonluoghi accettano l'inevitabilità di una loro frequentazione da parte di elementi estranei e dunque fanno tutto il possibile per rendere la loro presenza "meramente fisica", vale a dire del tutto irrilevante dal punto di vista sociale: cancellare, azzerare, rendere nulle le soggettività idiosincratiche dei loro "passeggeri"».

[32] Ivi, p. 104: «Gli estranei si incontrano nel modo che è loro consono; un incontro tra estranei è del tutto diverso da quello fra parenti, amici o conoscenti. Nell'incontro tra estranei, non si riprende il filo lì dove lo si era lasciato al termine del precedente, non c'è alcun aggiornamento sulle pene, le tribolazioni o le gioie vissute nel frattempo, niente da ricordare o raccontare. L'incontro tra estranei è un evento *privo di un passato*».

sfacendo il bisogno umano di creare nuove comunità – intese essenzialmente come somma di singole individualità[33] – che possano offrire riparo dalle crescenti insicurezze rappresentate del mondo fluido moderno[34], fermo restando che i presupposti dell'appartenenza posso essere in qualsiasi momento messi in discussione e rinegoziati, rendendo anche il "neocomunitarianisimo" un processo fluido[35]. Come Bauman ha ribadito anni dopo, «le "comunità" che si fondano su Internet non sono pensate per durare, e ancor meno per essere commensurate alla durata del tempo. Accedervi è facile, ma altrettanto facile è abbandonarle nell'attimo in cui l'attenzione, le simpatie o le antipatie, lo stato d'animo o le mode ci spingono altrove»[36]. Queste comunità *networked*, però, impongono «un prezzo da pagare in termini di sicurezza, che le comunità di un tempo erogavano, e che i *network* non riescono invece a garantire credibilmente»[37].

Tornando all'analisi di Ranie e Wellman, i legami deboli e destrutturati che caratterizzano le relazioni *networked* si vanno ripercuotendo anche sulle tradizionali formazioni sociali: ad esempio, la composizione delle famiglie e l'attribuzione dei ruoli e delle responsabilità al loro interno stanno trasformando i nuclei familiari da gruppi in *network*[38]; più in generale, tutte le forme strutturate di associazionismo vengono progressivamente soppiantate da *network* aperti e informali[39]; la cultura diviene frammentata e di-

[33] Ivi, p. 33: «Per l'individuo, lo spazio pubblico non è molto più che un maxischermo su cui le preoccupazioni private vengono proiettate e ingrandite senza per questo cessare di essere private o acquisire nuove qualità collettive; lo spazio pubblico è il luogo in cui si rende pubblica confessione di segreti e intimità privati».

[34] Ivi, partic. pp. 198-199.

[35] Ivi, p. 235: «… le comunità in questione tendono ad essere effimere, transitorie, incentrare su un unico aspetto o finalità. Il loro arco vitale è breve e al contempo pieno di parole senza senso. Il loro potere emana non dalla loro durata prevista ma, paradossalmente, dalla loro precarietà e incertezza del futuro, dalla vigilanza e dall'investimento emotivo che la loro fragile esistenza reclama a gran voce. La definizione "comunità guardaroba" coglie bene alcuni dei suoi tratti salienti». E a p. 236: «Le comunità guardaroba hanno bisogno di uno spettacolo che ridesti interessi simili sopiti in individui per altri versi diversi tra loro e quindi aggreghi tutti questi individui per un lasso di tempo durante il quale altri interessi – quelli che li dividono anziché unirli – vengono temporaneamente accantonati, sopiti o messi a tacere».

[36] Z. Bauman (2013), *Danni collaterali*, Roma-Bari, Laterza, p. 102.

[37] Ivi, p. 103. Castells (2009), cit., p. 461, esprime un concetto analogo: «… in un mondo di valori e norme in flusso costante, in una società del rischio, la gente si sente incerta e vulnerabile mentre gli individui cercano rifugio in comunità che rispondano alle loro identità […]. Queste comunità spesso diventano trincee di resistenza contro un ordine sociale percepito come estraneo e imposto con la forza, quando le istituzioni che prima davano sicurezza (lo stato, la chiesa, la famiglia) non funzionano più a dovere».

[38] Ranie e Wellman (2012), cit., p. 53.

[39] Ivi, p. 55.

spersa su più canali e più piattaforme[40]. Lo sviluppo delle nuove tecnologie, e soprattutto la disponibilità della connessione ad Internet in ogni luogo e in ogni momento, ha accorciato le distanze fra gli individui, consentendo loro una costante «presenza connessa, presenza assente e assenza presente», in cui i confini fra spazio pubblico e spazio privato tendono a sfumare[41]. Man mano che i *network* divengono più estesi e diversificati, le persone – che tendono a partecipare a più *network* – entrano in contatto con una gran varietà di ambienti sociali, di informazioni e di contatti[42]. Tuttavia, inevitabilmente l'attenzione e l'impegno che i singoli individui possono dedicare a un così ampio spettro di relazioni *networked*, tutte simultaneamente compresenti nello spazio e nel tempo, subiscono una riduzione, limitandosi a forme di «attenzione parziale continua»[43].

Bauman ha ben evidenziato il fatto che l'incredibile aumento del flusso di informazioni determinato da Internet non può generare anche una parallela espansione dell'attenzione umana: «al contrario, l'adattamento alle condizioni create da Internet rende l'attenzione fragile, e soprattutto incostante, incapace di concentrarsi a lungo: allenata e abituata a "navigare", ma non a spingersi in profondità; a "fare *zapping*" tra i canali, ma non ad aspettarsi che una qualsiasi delle trame percorse si riveli in tutta la sua ampiezza e profondità. In breve, l'attenzione tende ad abituarsi a scivolare sulla superficie molto più rapidamente del tempo che le sarebbe necessario per farsi un'idea di ciò che si nasconde più in fondo»[44].

Il progresso tecnologico, parallelamente all'enorme incremento delle informazioni di cui ciascuno di noi può disporre, ha posto alla portata di tutti la possibilità di filtrare le informazioni, in modo che ciascuno possa ricevere solo quelle che effettivamente desidera, evitando tutte le altre[45]. Come giustamente ha rilevato Sunstein[46], e come ormai più di un ventennio fa

[40] Ivi, p. 56.

[41] Ivi, pp. 158-161.

[42] Ivi, pp. 197-198.

[43] Ivi, p. 166.

[44] Bauman (2013), cit., p. 101.

[45] Castells (2009), cit., p. 208, scrive in proposito: «Comincerò riaffermando che la gente tende a credere in ciò a cui vuole credere. Filtra le informazioni per adattarle a giudizi preconcetti. È molto più riluttante ad accettare dati di fatto che contraddicono le proprie certezze che non quelli che rafforzano le proprie convinzioni». E a p. 210: «Si direbbe che le informazioni in se stesse non alterano le opinioni a meno che non vi sia un eccezionale livello di dissonanza cognitiva. Questo perché la gente sceglie le informazioni in base ai propri *frame* cognitivi».

[46] C. R. Sunstein (2003), *Republic.com. Cittadini informati o consumatori di informazioni?*, Bologna, Il Mulino.

aveva preconizzato Negroponte (*The Daily Me*)[47], il flusso comunicativo diventa personalizzato. Tale fenomeno non è del tutto spontaneo, ma è in qualche modo guidato dagli operatori economici, per i quali «l'attenzione dei consumatori è il bene cruciale (e carente) nel mercato che va emergendo»[48]. Infatti, come già rilevato da Castells, «per tutte le organizzazioni mediatiche, che siano concentrate sulla comunicazione di massa o sulla autocomunicazione di massa, o su entrambe, la chiave è espandere influenza e risorse espandendo e approfondendo il proprio pubblico. Diversi canali media identificano il proprio pubblico secondo specifiche strategie. Così, lo scopo non è semplicemente conquistare *share* di pubblico, ma anche conquistare un *target* specifico di spettatori/utenti»[49].

Poiché, come si è visto, l'attenzione degli individui/consumatori tende a disperdersi nella multiforme varietà del flusso informativo, la reazione a tale dispersione è inevitabilmente la personalizzazione delle comunicazioni. In questo processo, i gestori di motori di ricerca e di piattaforme di *social networking* svolgono un ruolo cruciale perché, disponendo delle informazioni relative ai gusti e alle preferenze dei propri utenti, riescono a rendere questa personalizzazione particolarmente efficace. In questo modo però, l'universo di informazioni cui ciascun individuo può potenzialmente accedere viene ristretto solo a ciò che, in base alle rilevazioni algoritmiche, si presume sia di suo interesse. Gli utenti dei *social network* e dei motori di ricerca sono per lo più inconsapevoli delle modalità di applicazione e di funzionamento di tali algoritmi, tanto più che essi, per ragioni connesse alla protezione della proprietà intellettuali, tendono a non essere disvelati dagli intermediari digitali che ne fanno uso[50]. Eppure questi algoritmi, come la "scatola nera" presente sugli aeroplani, registrano, aggregano ed analizzano tutte le "tracce digitali" disseminate nel web, al fine di somministrare agli

[47] N. Negroponte (1995), *Essere digitali*, Milano, Sperling & Kupfer, p. 159: «Immaginate un futuro in cui il vostro agente sia in grado di leggere tutti i giornali e le notizie di agenzia, e di captare le trasmissioni radio e Tv di tutto il pianeta, per poi farne una sintesi personalizzata. Questo tipo di giornale viene stampato in un'unica copia. […] Supponiamo che un giornale metta tutta la sua redazione a vostra disposizione per preparare un numero apposta per voi. Vi sarebbero notizie da prima pagina mescolate con storie "meno importanti" relative a vostri conoscenti, a gente che incontrerete domani, e a posti dove state per andare o da dove siete appena tornati. Vi si parlerebbe di aziende che conoscete. A queste condizioni sareste disposti a pagare una copia del *Boston Globe* di 10 pagine assai più di una di cento pagine, se avete la ragionevole sicurezza che vi fornirà il sottoinsieme di informazioni che desiderate. Ne consumereste ogni *bit* (per così dire). Chiamatelo *The Daily Me*».

[48] Sunstein (2003), cit., p. 33.

[49] Castells (2009), cit., p. 244.

[50] G. Pitruzzella (2017), *La libertà di informazione nell'era di Internet*, in G. Pitruzzella, O. Pollicino e S. Quintarelli, *Parole e potere. Libertà d'espressione, hate speech e fake news*, Milano, Egea, partic. pp. 64-67.

utenti pubblicità tagliata su misura, nonché di predire comportamenti futuri per predisporre nuove strategie di *marketing*. Si è detto che «the power to include, exclude, and rank is the power to ensure that certain public impressions become permanent, while others remain fleeting»; in altre parole, è il potere di creare una "reputazione" che, nella moderna economia digitale, è la chiave del successo: «the success of individuals, businesses, and their products depends, heavily on the synthesis of data and perceptions into *reputation*»[51]. Il problema è che questa reputazione è determinata da algoritmi segreti che organizzano dati inaccessibili: per questo significativamente è stata utilizzata la metafora della *Black Box Society* per indicare un sistema – non solo economico, ma anche sociale – che registra tutti i movimenti che avvengono *online*, ma che è assolutamente opaco rispetto a ciò che avviene al suo interno[52].

Non si può disconoscere che la "ricchezza delle reti" rappresenta una grande opportunità, perché consente di sviluppare, grazie alle piattaforme collaborative, una produzione sociale, orizzontale, basata sui beni comuni, che può rappresentare una alternativa economica alla tradizionale economia di mercato fondata sulle gerarchie manageriali delle aziende e sulla protezione della proprietà intellettuale[53]. Tuttavia, questa visione largamente ottimistica – secondo cui la *network economy* condurrà ad un'economia più aperta e dinamica, a una cultura meno gerarchica e più condivisa, a una democrazia più aperta e partecipata, e una società globale potenzialmente più equa e solidale – va contemperata con la riflessione per cui le informazioni che transitano attraverso la Rete, data la loro enorme quantità, necessitano di essere organizzate per poter essere davvero fruite; ecco, allora, che nel tempo alcuni (pochi) soggetti – i grandi motori di ricerca e i maggiori *social network* – hanno acquisito il ruolo di *gatekeepers* dell'informazione, cioè di intermediari digitali fra i produttori delle informazioni e gli utenti finali.

Ciò ha trasformato Internet da uno spazio sconfinato di libera informazione a uno spazio controllato da poche grandi *tech-companies*, che controllano e filtrano l'accesso alle informazioni e la loro diffusione attraverso l'utilizzo di algoritmi[54]. Gli algoritmi permettono il trattamento automatico o semi-automatico di una vasta mole di dati, velocizzando e ottimizzando le

[51] Citazioni tratte dal libro di F. Pasquale indicato nella nota successiva, p. 12.

[52] F. Pasquale (2015), *The Black Box Society. The Secret Algorithms That Control Money and Information*, Cambridge (Massachusetts) and London (England), Harvard University Press.

[53] Y. Benkler (2006), *The Wealth of Networks. How Social Production Transforms Markets and Freedom*, New Haven and London, Yale University Press.

[54] E. B. Laidlaw (2015), *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility*, Cambridge University Press. Si veda anche Pitruzzella (2017), cit., partic. pp. 58-60.

correlazioni fra di essi, oltre le umane capacità di elaborazione, previsione e estrazione di informazioni (*data mining*). Sempre più frequentemente, quindi, i processi decisionali sono governati da algoritmi (*algoritmic decision making*)[55].

Al di là dell'impatto sull'economia, l'effetto negativo di tali dinamiche per la democrazia nel suo complesso emerge con evidenza: «se alle persone viene negato l'accesso a pareri contrastanti su argomenti di interesse pubblico e se, da parte loro, c'è come risultato una mancanza di interesse per questi punti di vista, si verifica una mancanza di libertà, qualunque sia la natura delle loro preferenze e scelte»[56]. Al contrario, si accresce notevolmente «la predisposizione delle persone ad ascoltare l'eco della propria voce e a isolarsi dagli altri. Un'importante conseguenza è l'esistenza delle *cybercascades* – processi di scambio delle informazioni nei quali un certo fatto o punto di vista si diffonde semplicemente perché così tante persone sembrano crederci»[57]. Proprio come avviene, infatti, all'interno dei *social network*, grazie ai quali taluni contenuti possono diffondersi al punto tale da divenire "virali". I *social network*, del resto, altro non sono che «comunità fondate sulla condivisione degli interessi»[58], dunque comunità piuttosto omogenee in termini di interessi e prospettive, a differenza delle interazioni che avvengono nel mondo reale, che invece costringono spesso gli individui a doversi confrontare con la diversità. In questo tipo di comunità virtuali «molte persone continuano per lo più ad ascoltare un'eco amplificata e ripetuta della loro stessa voce»[59], con inevitabili ripercussioni sulla crescita di fenomeni quali la diffusione di notizie false, l'intolleranza e l'estremizzazione delle idee[60].

[55] S. Calzolaio (2017b), *Protezione dei dati personali*, in *Digesto delle discipline pubblicistiche. Aggiornamento*, Torino, Utet, pp. 594-635, partic. p. 599.

[56] Sunstein (2003), cit., p. 126.

[57] Ivi, pp. 63-64.

[58] Ivi, p. 71.

[59] Ivi, p. 78.

[60] A proposito di quest'ultimo aspetto, Sunstein (2003), cit., ha posto l'accendo sul fenomeno della cosiddetta "polarizzazione di gruppo": «dopo un dibattito, l'opinione tende a spostarsi verso un punto estremo nella direzione in cui i membri del gruppo erano originariamente orientati. Per quanto riguarda internet e le nuove tecnologie di comunicazione, questo significa che gruppi di persone della stessa area ideologica, al termine di una discussione fra loro, finiranno per pensare la stessa cosa che pensavano prima, ma in forma più estremistica» (ivi, p. 82). Infatti, «internet continua ad essere per molti un terreno fertile per l'estremismo, proprio perché persone della stessa area di pensiero trattano tra di loro con grande frequenza e facilità, e spesso senza sentire alcuna controparte. Un'esposizione ripetuta a una posizione estrema, unita all'idea che molte altre persone condividano quella posizione, prevedibilmente porterà le persone che vi sono esposte, e forse già propense, a credere in essa» (ivi, p. 87).

Le dinamiche sempre più marcate di personalizzazione delle informazioni da parte dei colossi del *web*, realizzate attraverso algoritmi dal funzionamento non trasparente, porta ciascuno di noi a vivere all'interno di una "bolla di filtri"[61], un microcosmo fatto di sole notizie gradevoli, attinenti ai nostri interessi e conformi alle nostre convinzioni, che riduce la diversità dei punti di vista, limita la scoperta di fonti di creatività e innovazione e restringe il libero scambio delle idee. Certamente le pratiche di personalizzazione possono apparire vantaggiose per gli utenti, perché facilitano la navigazione e il reperimento in Rete proprio dell'informazione che si desidera, al prezzo però di essere sottoposti ad un continuo condizionamento delle proprie scelte, che non riguarda solo o beni di consumo da acquistare, ma si estende anche all'universo ideologico, influenzando il nostro modo di pensare.

La dimensione in cui viviamo, caratterizzata da mezzi di comunicazione articolati in modo reticolare, le cui dinamiche plasmano il pensiero degli individui e, dunque, la loro capacità di esercitare delle scelte, condizionando la loro libertà, produce effetti che travalicano la sfera individuale. Muovendo dalle considerazioni di Habermas sulla formazione dell'opinione pubblica e della sfera pubblica nel corso dei secoli[62], accompagnando il processo di consolidamento dello Stato liberal-democratico, si può certamente affermare che oggi la comunicazione è divenuta gradualmente il nuovo spazio pubblico della società, poiché il processo di formazione dell'opinione pubblica si è spostato dalle istituzioni politiche dello Stato-nazione, oggi in crisi di legittimità, all'universo della comunicazione. Le élite dominanti, dunque, sono oggi quelle che arrivano ad affermare il proprio dominio sulla comunicazione[63]. Per questo, chiedersi quale è il ruolo rivestito, in questo processo, dagli intermediari digitali e quali sono – o potrebbero/dovrebbero essere – le loro responsabilità acquista un significato

[61] E. Pariser (2012), *Il filtro. Quello che Internet ci nasconde*, Milano, Il Saggiatore. Scrive l'Autore a p. 69: «L'effetto deformante è uno dei rischi che comportano i filtri personalizzati. Come una lente, la bolla dei filtri trasforma in modo impercettibile la nostra esperienza del mondo, controllando quello che vediamo e non vediamo. Interferisce nel rapporto tra i nostri processi mentali e l'ambiente esterno. Per certi versi, può fungere da utile lente di ingrandimento e allargare la nostra visione di un settore della conoscenza poco noto. Ma al tempo stesso, i filtri personalizzati limitano le informazioni alle quali siamo esposti e quindi influiscono sul nostro modo di pensare e di apprendere. Possono sconvolgere il delicato equilibrio cognitivo che ci aiuta a prendere le decisioni giuste e ad avere nuove idee. E poiché la creatività è anche frutto di questa interazione fra mente e ambiente, possono impedire l'innovazione. Se vogliamo sapere com'è veramente, dobbiamo capire come i filtri condizionano e deformano la nostra visione del mondo».

[62] J. Habermas (1988), *Storia e critica dell'opinione pubblica*, Roma-Bari, Laterza.

[63] Castells (2007), cit., partic. conclusioni.

"pubblico", che va al di là del problema di riuscire a garantire un'efficace protezione dei diritti individuali.

Le grandi *web companies*, infatti, sembrano essere diventati i nuovi *gatekeepers* dell'informazione, occupando il posto tradizionalmente spettante ai soggetti pubblici. Sono oggi soggetti privati quelli che influiscono su come i singoli individui interagiscono in Rete, condividendo idee e opinioni. Sono soggetti privati quelli che detengono – in modo spesso poco trasparente, le tecnologie che governano il funzionamento delle piattaforme informatiche e, pertanto, sono le scelte di tali attori privati a condizionare in modo sempre più evidente la libertà di espressione individuale e la formazione dell'opinione pubblica. Come non chiedersi, allora, se sia giusto che soggetti privati, in assenza di garanzie pubblicistiche e in regime di irresponsabilità, possano essere chiamati a operare il delicato bilanciamento fra i diritti fondamentali individuali, decidendo quali contenuti presenti in Rete vadano conservati, segnalati oppure rimossi.

I *SOCIAL NETWORK* IN UNA PROSPETTIVA COSTITUZIONALISTICA

1. Le *social network communities* come formazioni sociali *ex* art. 2 Cost.

In uno scritto di qualche anno fa, dedicato principalmente alla configurazione di Internet nell'ordinamento giuridico italiano e al fondamento costituzionale del diritto di accesso a Internet, Paolo Passaglia si interrogava anche sull'opportunità di considerare la comunità di tutti gli utenti di Internet alla stregua di una formazione sociale *ex* art. 2 Cost., definendola «una qualificazione problematica, ma non impossibile», considerando che in Rete possono concretizzarsi legami interpersonali relativamente stabili[1].

Muovendo dalle considerazioni di Emanuele Rossi sulle formazioni sociali nella Costituzione italiana[2], formulate in un'epoca precedente alla diffusione di Internet, Passaglia rinveniva nella comunità degli internauti i tre elementi fondamentali che Rossi riteneva propri delle formazioni sociali[3] – quello materiale, cioè l'insieme delle persone fisiche; quello teleologico, cioè lo scopo dello sviluppo della persona umana; quello psicologico, cioè la volontà di accedere ad Internet per esercitare le potenzialità espressive insite in tale mezzo o anche semplicemente per fruirne passivamente – nonché due ulteriori requisiti indicati anch'essi nell'analisi di Rossi, ovvero l'interesse specifico di cui la formazione sociale è portatrice, consistente per Passaglia nella comunicazione e nella condivisione, e la particolarità di tale interesse qualificato rispetto all'interesse generale dello Stato[4].

[1] P. Passaglia (2014), *Internet nella Costituzione italiana: considerazioni introduttive*, in M. Nisticò e P. Passaglia (a cura di), *Internet e Costituzione*, Torino, Giappichelli, pp. 37 ss.

[2] E. Rossi (1989), *Le formazioni sociali nella Costituzione italiana*, Padova, Cedam.

[3] Ivi, pp. 151-152.

[4] Ivi, pp. 120-121: «… le formazioni sociali *ex* art. 2 si caratterizzano per il fatto di perseguire interessi che, pur considerati talora strettamente collegati a quelli statali, rimangono tuttavia affidati alla iniziativa dei privati e per i quali l'azione dello stato si limita a stimolare e ad indirizzare il vincolo comunitario ritenuto necessario per la loro soddisfazione».

L'estensione della nozione di formazione sociale al gruppo costituito da tutti gli utenti di Internet non sembra però del tutto appropriata. In primo luogo, è evidente come la via tracciata dal rapidissimo progresso tecnologico sia quella di una diffusione ubiquitaria di Internet, considerando non solo il crescente numero di persone che accedono consapevolmente alla Rete, ma anche quello di coloro che più o meno inconsapevolmente fruiscono di servizi o di oggetti a loro volta *Internet-based*, se non altro perché è sempre più difficile individuare quelli che non lo sono[5]. Se oggi, in una realtà come quella italiana o europea, talune barriere anagrafiche, culturali o economiche escludono ancora parte delle persone dall'accesso a Internet, è un dato di fatto che il *digital divide* si va progressivamente riducendo e che la digitalizzazione è un fenomeno che non interessa solo i Paesi più sviluppati, ma anche quelli in via di sviluppo. Non è forse lontano il momento in cui, volendo individuare l'esistenza di una formazione sociale in relazione ad Internet, la scelta dovrà necessariamente ricadere sul ristretto gruppo di coloro che si ostinano a non volerne usufruire, anziché sulla larghissima maggioranza degli internauti, che sempre più tende a coincidere con l'intera comunità umana.

Un altro aspetto problematico risiede nel requisito teleologico: secondo Rossi, la formazione sociale deve avere lo scopo di contribuire allo sviluppo della persona umana, come richiesto dall'art. 2 Cost., ma deve farlo perseguendo un interesse collettivo che deve risultare trascendente rispetto all'interesse dei singoli membri della formazione sociale, nonché particolare rispetto all'interesse generale dello Stato. Ora, considerando l'infinita vastità degli scopi, interessi, aspirazioni che si possono perseguire attraverso Internet, tanto da poter dire che nessuna finalità connessa a un qualsiasi aspetto della vita umana ne sia esclusa, l'unico scopo comune in grado di ricomprenderli tutti è appunto quello generalissimo dello sviluppo della persona umana. Ma si tratta di uno scopo tanto generale da essere proprio

[5] Si pensi alla progressiva diffusione dell'*Internet of Things*, su cui si veda E. C. Pallone (2016), "*Internet of Things" e l'importanza del diritto alla privacy tra opportunità e rischi*, in *Ciberspazio e diritto*, n. 1-2, pp. 163-183. A p. 164 l'Autrice evidenzia che «si va delineando una società caratterizzata da oggetti di uso quotidiano dotati di sensori in grado di rilevare, raccogliere e trasmettere dati relativamente all'utilizzo che viene fatto di quell'oggetto intelligente (*smart thing*), anche e soprattutto in correlazione con altri oggetti con le medesime capacità». Sullo IoT si vedano anche i documenti prodotti dallo *European Research Cluster on the Internet of Things* (Ierc), consultabili all'indirizzo http://www.-internet-of-things-research.eu/documents.htm, nonché l'*Opinion 8/2014 on Recent Developments on the Internet of Things* (16 settembre 2014) ad opera dell'*Article 29 Data Protection Working Party*, che è un organismo consultivo istituito in base all'art. 29 della direttiva europea 95/46/Ce. Va segnalato, infine, che con decisione del 10 agosto 2010 la Commissione europea ha istituito un gruppo di esperti specificamente dedicato allo IoT (E02514).

di qualsiasi formazione sociale, ivi compreso lo Stato stesso. In altre parole, se lo scopo diviene omnicomprensivo e perseguito dalla generalità dei consociati, esso perde la sua funzione di discrimine fra le diverse formazioni sociali, giungendo a ricomprenderle tutte.

Qualche altro rilievo critico emerge infine in relazione all'elemento psicologico individuato da Rossi, cioè la consapevolezza di ciascuno dei componenti di far parte di una formazione sociale. La consapevolezza non necessariamente coincide con la volontarietà, potendo ben esistere formazioni sociali "naturali" (ad esempio la famiglia) o costituite sulla base di un certo grado di coattività (ad esempio la scuola o il carcere); tuttavia si richiede che i componenti di una formazione sociale siano consci di far parte di un gruppo che possiede taluni caratteri distintivi rispetto alle altre formazioni sociali. Ora, considerando che Internet ha carattere ubiquitario, omnicomprensivo e sconfinato rispetto agli scopi perseguibili, è sempre meno probabile che gli internauti percepiscano se stessi come parte di una aggregazione distinta da altre.

Qualcuno[6] infatti ha contestato apertamente la qualificazione di una presunta "comunità degli utenti di Internet" come formazione sociale. Secondo questa analisi, Internet altro non sarebbe che un insieme di apparati tecnologici attraverso cui una molteplicità di soggetti svolge attività disparate, senza finalità comuni o regole condivise; non si capisce, allora, «per quale motivo il semplice fatto di utilizzare uno strumento di comunicazione, informazione o espressione debba essere letto come sintomatico della appartenenza del soggetto ad una comunità, a meno che di "comunità" o di "formazione sociale" non si voglia dare una accezione a tal punto generica dal divenire, probabilmente, del tutto inutile»[7].

Il ragionamento di Passaglia, però, è suggestivo per il fatto che può essere riprodotto ed applicato, se non all'intera comunità degli utenti di Internet, almeno alle ben più ristrette e delimitate *social network communities*, cioè le comunità di coloro che sono iscritti ai vari *social network*. Il termine inglese *communities* è certamente caratterizzato da una maggiore immediatezza rispetto alla "paludata" locuzione *formazioni sociali* contenuta nell'art. 2 Cost., ma può essere interessante ricordare che nella relazione sui principi relativi ai rapporti civili presentata da Giorgio la Pira alla prima sottocommissione dell'Assemblea costituente ricorreva piuttosto l'espressione «comunità naturali attraverso le quali la personalità umana ordinatamente si svolge». Successivamente Giuseppe Dossetti, nell'ordine

[6] M. Cuniberti (2015), *Tecnologie digitali e libertà politiche*, in *Il diritto dell'informazione e dell'informatica*, n. 2, p. 280.

[7] *Ibid.*

del giorno proposto alla prima sottocommissione il 9 settembre 1946 e mai votato, suggerì l'espressione «comunità intermedie disposte secondo una naturale gradualità», attraverso le quali le persone «sono destinate a completarsi e perfezionarsi a vicenda mediante una reciproca solidarietà economica e spirituale». Per quanto alla fine il testo definitivo dell'art. 2 sia stato approvato[8] utilizzando l'espressione *formazioni sociali*, preferita da alcuni deputati, fra cui soprattutto Aldo Moro[9], il concetto di comunità ne costituisce comunque il fondamento.

Le *social network communities* – intendendo con tale espressione non la comunità di tutti gli utenti dei *social network* generalmente intesa, ma le molteplici comunità costituite dagli iscritti alle singole piattaforme di condivisione – integrano certamente il primo dei requisiti richiesti nel ragionamento di Rossi e Passaglia, cioè quello delle persone fisiche partecipanti alle varie *communities*. Costoro costituiranno sempre e comunque gruppi distinti rispetto alla generalità degli individui per il fatto che non tutti utilizzano le piattaforme di *social networking* e, in ogni caso, non tutti le utilizzano tutte indistintamente.

Per quanto riguarda l'elemento teleologico, certamente ciascuna delle *social network communities* ha l'implicita finalità di contribuire allo sviluppo della persona umana, ma ciascuna lo fa con modalità particolari e finalità specifiche cui gli iscritti ad ogni *social network* aderiscono al momento della sottoscrizione dei *terms of use* del servizio. La finalità di ciascuna di queste formazioni sociali è dunque individuata con sufficiente precisione e consapevolmente accettata e condivisa dagli iscritti alla piattaforma.

Poiché l'iscrizione a un *social network* è un atto che si compie volontariamente, pur se molti non hanno piena consapevolezza delle implicazioni

[8] Assemblea costituente, seduta pomeridiana del 22 marzo 1947.

[9] Così si espresse Aldo Moro in Assemblea costituente, nella seduta del 22 marzo 1947: «Invece di parlare, come nella primitiva formulazione, di diritti essenziali e degli individui e delle formazioni sociali, noi diciamo attualmente che la Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità. […] Facendo riferimento all'uomo come titolare di un diritto che trova una sua espressione nella formazione sociale, noi possiamo chiarire nettamente il carattere umanistico che essenzialmente spetta alle formazioni sociali che noi vogliamo vedere garantite in questo articolo della Costituzione. E da un altro punto di vista, il parlare in questo caso di diritti dell'uomo, sia come singolo, e sia nelle formazioni sociali, mette in chiaro che la tutela accordata a queste formazioni è niente altro che una ulteriore esplicazione, uno svolgimento dei diritti di autonomia, di dignità e di libertà che sono stati riconosciuti e garantiti in questo articolo costituzionale all'uomo come tale. […] La libertà dell'uomo è pienamente garantita, se l'uomo è libero di formare degli aggregati sociali e di svilupparsi in essi. Lo Stato veramente democratico riconosce e garantisce non soltanto i diritti dell'uomo isolato, che sarebbe in realtà una astrazione, ma i diritti dell'uomo associato secondo una libera vocazione sociale».

che la partecipazione a un *social network* può avere dal punto di vista del trattamento dei dati personali e delle possibili violazioni della sfera privata e della reputazione individuale[10], è soddisfatto anche il requisito psicologico, consistente nell'adesione volontaria alla formazione sociale e nella piena coscienza di farne parte.

L'interesse di cui la formazione sociale deve essere portatrice, che deve essere trascendente rispetto all'interesse dei suoi singoli componenti, consiste essenzialmente nella condivisione di informazioni, che avviene secondo le modalità previste da ogni singolo *social network*. Ovviamente la condivisione è anche e soprattutto un interesse individuale, che però non potrebbe realizzarsi se non all'interno di una comunità composta da persone tutte desiderose di condividere informazioni. Condividere non significa solo esprimersi. La libertà di espressione può essere realizzata anche utilizzando un mezzo di comunicazione tradizionale del tipo *one-to-many* (la carta stampata, la radio, la televisione), attraverso il quale il proprio pensiero può essere comunicato simultaneamente a una indistinta pluralità di destinatari, dai quali non necessariamente si riceve un *feed-back*. Invece, la condivisione del tipo *many-to-many* presuppone non solo la diffusione dei propri contenuti, ma anche la contestuale ricezione di contenuti prodotti da altri, rispetto ai quali si è chiamati ad esprimere il proprio indice di gradimento e a renderne partecipi altri iscritti alla piattaforma. La condivisione è dunque uno scambio di informazioni, di reciproci rapporti di *do ut des*, che possono avvenire solo all'interno di un contesto sociale organizzato. L'interesse della *social network community*, ulteriore rispetto a quello dei singoli suoi membri, è dunque quello che questo continuo scambio resti vivo e continui ad autoalimentarsi, perché la condivisione è la ragione stessa dell'esistenza della formazione sociale e la sua cessazione ne rappresenterebbe la "morte".

L'interesse della *community*, consistente nella condivisione, è inoltre indipendente dall'interesse generale dello Stato. Infatti, l'interesse alla condi-

[10] Numerosi studi condotti negli Stati Uniti hanno mostrato che le condotte di condivisione di informazioni tenute sui *social network* non implicano la consapevolezza, da parte degli utenti, della divulgazione che i dati contenuti negli stessi possono avere. Si può allora parlare di un vero e proprio *privacy paradox*, ovvero della discrasia tra quanto gli utenti asseriscono di conoscere in merito alle impostazioni della *privacy* dei loro *account* e come essi reagiscono dinanzi alle inattese conseguenze dovute a violazioni della *privacy*. Su questo: S. B. Barnes (2006), *A privacy paradox: Social networking in the United States*, in *First Monday*, n. 9, (http://firstmonday.org/article/view/1394/1312). Altri studi, per lo più americani, relativi alla mancanza di consapevolezza, da parte degli utenti, delle implicazioni conseguenti all'adesione a un modello di apertura totale delle impostazioni sulla *privacy* nei propri *account* sono citati da A. R. Popoli (2014), *Social network e concreta protezione dei dati sensibili: luci ed ombre di una difficile convivenza*, in *Il diritto dell'informazione e dell'informatica*, n. 6, pp. 981-1017.

visione sussiste di per sé, come condizione di esistenza stessa della *community*, ed è del tutto indipendente da ciò che si condivide. Proprio su questo assunto si fonda, del resto, l'asserita neutralità – e quindi irresponsabilità – del gestore della piattaforma (il *social network provider*) rispetto alle condotte degli utenti, in base alla direttiva europea sul commercio elettronico, come si vedrà meglio nelle pagine successive. La condivisione si configura, dunque, come un interesse proprio della formazione sociale, non solo indipendente da quello statuale, ma che addirittura può essere in contrasto con esso. I contenuti condivisi, infatti, possono essere tali da ledere i diritti individuali, che lo Stato ha certamente interesse a proteggere, come si evince dal dettato costituzionale; inoltre, essi possono essere anche tali da mettere a repentaglio la sicurezza e l'incolumità pubblica più volte richiamate in Costituzione (si pensi, ad esempio, all'uso che le organizzazioni terroristiche fanno dei *social network* a scopo di propaganda e di reclutamento di nuovi adepti) o da attentare all'ordine pubblico inteso in senso costituzionalmente orientato[11], come avviene nel caso della diffusione incontrollata di notizie false o distorte, di discorsi di incitamento all'odio e alla violenza, oppure di taluni reati che attraverso i *social network* possono essere commessi con maggiore facilità, amplificando l'offensività delle relative condotte.

[11] Il concetto di ordine pubblico è stato inizialmente interpretato dalla Corte costituzionale come «preservazione delle strutture giuridiche della convivenza sociale, instaurate mediante le leggi, da ogni attentato a modificarle o a renderle inoperanti mediante l'uso o la minaccia illegale della forza» (sentenza n. 19 del 1962, relativa a all'art. 656 c.p., concernente la pubblicazione o diffusione di notizie false, esagerate o tendenziose atte a turbare l'ordine pubblico), oppure come «ordine pubblico costituzionale […] che deve essere assicurato appunto per consentire a tutti il godimento effettivo dei diritti inviolabili dell'uomo», poiché «anche diritti primari e fondamentali […] debbono venir contemperati con le esigenze di una tollerabile convivenza», altrimenti «la garanzia dei diritti inviolabili dell'uomo diventerebbe illusoria per tutti, se ciascuno potesse esercitarli fuori dell'ambito delle leggi, della civile regolamentazione, del ragionevole costume» (sentenza n. 168 del 1971, relativa al reato di inosservanza dei provvedimenti dell'autorità per ragione d'ordine pubblico, di cui all'art. 650 c. p.). Più recentemente (sentenza n. 218 del 1988 in materia di polizia delle miniere), la Corte ha confinato la nozione di ordine pubblico all'ambito materiale, identificando in esso «le funzioni primariamente dirette a tutelare beni fondamentali, quali l'integrità fisica e psichica delle persone, la sicurezza dei possessi e il rispetto o la garanzia di ogni altro bene giuridico di fondamentale importanza per l'esistenza e lo svolgimento dell'ordinamento». In seguito alla costituzionalizzazione del concetto di «ordine e sicurezza pubblica», introdotto nel 2001 nell'art. 117 Cost. comma 2, lett. h, la Corte costituzionale, al fine di chiarire la nozione di ordine pubblico e sicurezza pubblica contenuta nell'art. 159 del d. lgs. n. 112/1998, la ha qualificata come «non qualsiasi interesse pubblico alla cui cura siano preposte le pubbliche amministrazioni, ma soltanto quegli interessi essenziali al mantenimento di una ordinata convivenza civile» (sentenza n. 290 del 2001).

In base al ragionamento che si è seguito fin qui, non sembra vi siano ostacoli a far rientrare pienamente le *social network communities* nell'ambito delle formazioni sociali menzionate nell'art. 2 Cost[12]. Se è così, però, queste comunità devono essere considerate un fenomeno giuridicamente rilevante, nel senso che proprio grazie all'art. 2 Cost. si giustifica l'azione dei pubblici poteri atta a tutelare i diritti inviolabili dei membri della *community* in caso di lesioni derivanti dall'attività di condivisione di informazioni immanente alla comunità. Ciò che avviene all'interno della *community* non corrisponde a una sfera di autonomia privata intangibile, proprio perché l'art. 2 Cost. esige di tutelare i diritti individuali anche all'interno delle formazioni sociali[13].

La protezione dei diritti inviolabili dell'uomo all'interno delle formazioni sociali ad opera delle autorità pubbliche – non solo giurisdizionali, ma anche autorità amministrative indipendenti aventi funzione di garanzia – può avvenire non solo nei confronti di violazioni compiute da altri membri della comunità appartenenti alla categoria degli utenti dei *social network*, ma anche nei confronti dei soggetti che all'interno della *community* sono posti in posizione per così dire "apicale", cioè i gestori delle piattaforme. La nozione di formazione sociale, infatti, non presuppone affatto che tutti i sui membri siano posti sullo stesso piano. Al contrario, quanto più una formazione sociale è dotata di un'organizzazione stabile, tanto più si avverte l'esigenza di suddividere le funzioni al suo interno, prevedendo un potere di comando che detta le norme di comportamento legate ai fini associativi ed eventualmente faccia valere sanzioni nei confronti di chi viola la disciplina di gruppo; quindi non tutte le parti godono di analoghe sfere di libertà: talune si trovano in posizione dominante e altre in posizione più debole[14]. Il *social network provider*, dunque, è membro costitutivo – anzi, indispensabile – della formazione sociale, ed è tenuto al pari degli altri membri al rispetto dei diritti individuali di tutti gli aderenti.

Se al *provider* non è richiesta alcuna forma di monitoraggio o filtraggio preventivo dei contenuti *user-generated*, perché ciò corrisponderebbe a una

[12] Così anche P. Marsocci (2015), *Cittadinanza digitale e potenziamento della partecipazione politica attraverso il web: un mito così recente già da sfatare?*, in *Rivista Aic*, p. 16.

[13] Già F. Galgano (1976), *Delle associazioni non riconosciute e dei comitati*, in A. Scialoja e G. Branca (a cura di), *Commentario del codice civile*, Bologna, Zanichelli, evidenziava che l'entrata in vigore dell'art. 2 Cost., superando la distinzione di matrice civilistica fra associazioni riconosciute e non riconosciute, «ha fatto venire meno il presupposto previsto dal codice civile, secondo il quale solo a seguito del riconoscimento le situazioni giuridiche interne all'associazione acquistano "rilevanza" per lo stato e debbono essere regolate dal diritto statuale» (citazione tratta da Rossi (1989), cit., p. 168).

[14] Rossi (1989), cit., pp. 160-161.

forma di "censura privata"[15] in netto contrasto con il diritto inviolabile alla libera espressione del pensiero, ad esso è richiesto però di attivarsi per rimuovere *ex post* i contenuti illeciti, o in ottemperanza a un ordine delle competenti autorità giudiziarie e amministrative oppure anche semplicemente su richiesta del titolare del diritto leso, qualora l'illiceità dei contenuti sia manifesta. Inoltre, se tutti i membri della formazione sociale sono tenuti al rispetto delle regole che hanno accettato al momento dell'ingresso nella *community*, anche il gestore della piattaforma è tenuto al rispetto di quanto dichiarato nei *terms of use* del servizio, in particolare per quanto riguarda le modalità e finalità del trattamento dei dati personali e il rispetto del principio di non discriminazione per quanto riguarda l'accesso degli utenti alla *community* o l'esclusione dalla stessa in caso di comportamenti scorretti.

L'art. 2 Cost. presuppone altresì, in base al principio pluralista in esso contenuto, la tutela dei diritti *delle* formazioni sociali come soggetti collettivi. Non può trattarsi certamente di diritti opponibili a quelli degli individui che le compongono, giacché – vale la pena di ribadirlo – è l'individuo e non la formazione sociale il soggetto dell'art. 2 Cost. Tuttavia, la Costituzione repubblicana ha riconosciuto la dimensione della socialità come elemento imprescindibile di estrinsecazione dei diritti individuali e, conseguentemente, il principio per cui ad una restrizione delle libertà dei soggetti collettivi corrisponderebbe inevitabilmente una restrizione della sfera di libertà dell'individuo. Per questo motivo l'ordinamento giuridico, sia dal punto di vista del diritto positivo che da quello dell'interpretazione giurisprudenziale, deve necessariamente considerare il problema del *quantum* di regolamentazione può essere imposta alle *social network communities* senza che venga intaccata la loro stessa *raison d'être* consistente nella libera condivisione di informazioni. Per le stesse ragioni, proprio al fine di preservare la libertà delle interazioni sociali che avvengono nelle *communities*, non può essere trascurata la necessità di una regolamentazione che, in attuazione dell'art. 41 Cost., indirizzando e coordinando l'iniziativa economica privata a fini sociali, pur preservandone la libertà, tuteli le comunità degli utenti dei *social network* dalle pressioni e dai condizionamenti derivanti dai preponderanti interessi economici dei grandi *provider*.

In sintesi, in base alle riflessioni fin qui formulate non si ravvisano ostacoli alla configurazione delle *social network communities* alla stregua di formazioni sociali ex art. 2 Cost. Questa ricostruzione ha il pregio di offrire

[15] Sulla privatizzazione della censura ad opera degli intermediari digitali e sui rischi che ciò comporta si veda M. Bettoni (2011), *Profili giuridici della privatizzazione della censura*, in *Ciberspazio e diritto*, n. 4, pp. 363-383.

un fondamento costituzionale ad eventuali norme poste a garanzia che il *social network provider* – anch'esso da considerarsi membro della formazione sociale – non abusi della propria posizione di preminenza, rispettando i diritti individuali di tutti gli aderenti alla *community* pur nel rispetto della sua libertà di iniziativa economica.

2. Le *social network communities* come associazioni *ex* art. 18 Cost.

Posta l'equiparazione delle *social network communities* alle formazioni sociali *ex* art. 2 Cost., occorre verificare la loro eventuale corrispondenza a qualcuna delle formazioni sociali aventi rilevanza costituzionale, in particolare alle associazioni di cui all'art. 18 Cost.

La nozione di formazione sociale è molto più estesa di quella di associazione[16] e comprende tanto le organizzazioni collettive costituite su base volontaria, come le associazioni o le società, quanto quelle necessarie, quali gli enti pubblici territoriali o la famiglia. L'associazione, dunque, è una particolare declinazione della vasta categoria delle formazioni sociali, che Pace definisce come «realtà spirituale dotata di vita propria»[17], ma non necessariamente di soggettività giuridica.

Se negli anni immediatamente successivi all'entrata in vigore della Costituzione prevaleva l'idea delle associazioni non riconosciute quali ordinamenti originari, fondati sulla libera volontà degli associati e viventi in una condizione di irrilevanza per lo Stato[18], oppure immuni dalla giurisdizione statale in virtù del principio di autonomia contrattuale[19], nel corso degli anni Settanta la pretesa di associazioni *legibus solutae* inizia ad essere considerata una minaccia per la libertà dell'individuo[20].

Sebbene l'ordinamento giuridico vigente non preveda alcuna norma che definisca la nozione di associazione, la dottrina dominante ha individuato alcuni requisiti propri di ogni associazione[21]: l'elemento soggettivo (una

[16] F. Galgano (2010), *Trattato di diritto civile. Volume primo*, Padova, Cedam, p. 211 ss. Sul rapporto fra formazioni sociali (*ex* art. 2 Cost.) e associazioni (*ex* art. 18 Cost.) si veda G. Guzzetta (2003), *Il diritto costituzionale di associarsi. Libertà, autonomia, promozione*, Milano, Giuffrè, pp. 167-195.

[17] A. Pace (1977), *Art. 17-18*, in G. Branca (a cura di), *Commentario della Costituzione*, Bologna, Zanichelli, pp. 196-197.

[18] Così S. Romano (1945), *L'ordinamento giuridico*, Firenze, Sansoni.

[19] Così P. Rescigno (1966), *Persona e comunità: saggi di diritto privato*, Bologna, Il Mulino.

[20] Galgano (2010), cit., p. 2013.

[21] Sulla nozione costituzionale di associazione si veda Guzzetta (2003), cit. Sui requisiti della fattispecie si veda partic. Pace (1997), cit., p. 199.

collettività di persone fisiche), quello volontaristico (la libera volontà di costituire un'associazione, di aderirvi e di agire al suo interno), quello teleologico (lo scopo comune che le persone intendono perseguire attraverso l'associazione)[22], quello oggettivo (la prestazione offerta da ciascun associato) e infine quello materiale (la struttura organizzativa dell'associazione stessa, che prevede normalmente la costituzione di organi rappresentativi e forme di suddivisione dei compiti fra gli associati). Questi elementi concorrono a formare una concezione delle associazioni come «organizzazioni plurisoggettive contrassegnate da un vincolo finalistico»[23]. L'elemento della comunanza del fine è quello che soprattutto vale a caratterizzare le associazioni come tali e a definire i confini ideali di tale fenomeno[24].

I medesimi elementi, in effetti, sono propri anche delle *social network communities*: la volontà di entrare a farne parte viene espressa liberamente al momento della sottoscrizione delle clausole d'uso; lo scopo comune consiste, come si è già detto, nella condivisione di informazioni e proprio in quanto tale presuppone la plurisoggettività; le finalità di condivisione implicano prestazioni da parte degli "associati" in termini di produzione di contenuti, messa a disposizioni degli stessi, pratiche di *sharing*, *tagging* e espressione del gradimento[25]. Qualche difficoltà può sussistere in relazione all'individuazione della struttura organizzativa, che nel caso delle *social network communities* è assai evanescente. Tuttavia, pur in assenza di organi rappresentativi della volontà degli associati, può rinvenirsi una qualche forma di suddivisione dei compiti fra i membri della *community*, se non altro perché, a fronte di una molteplicità di *user* posti tutti quanti su un piano di parità, esiste un soggetto – il gestore della piattaforma – su cui gravano specifici compiti e responsabilità. Peraltro, non necessariamente l'associazione presuppone che la sua organizzazione interna sia il frutto della volontà negoziale fra gli associati né la stabilità dell'organizzazione è considerata da tutti un requisito indefettibile né, infine, l'incontro fra le volontà degli associati deve per forza concretizzarsi in vincoli giuridicamente efficaci, ben potendo questi ultimi rimanere rilevanti solo sul

[22] Per Guzzetta (2003), cit., pp. 104-105, l'elemento teleologico potrebbe consistere anche nella volontà di associarsi in sé e per sé (l'associazione stessa come fine).

[23] A. Pace (1988), *Problematica delle libertà costituzionali. Lezioni. Parte speciale II*, Padova, Cedam, p. 335.

[24] Guzzetta (2003), cit., p. 91.

[25] Non va dimenticato che, attraverso la pressione dei tasti di apprezzamento e di condivisione, si possono comunicare dati relativi all'origine razziale ed etnica, alle convinzioni religiose, filosofiche o di altro genere, alle opinioni politiche, all'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché dati idonei a rivelare lo stato di salute e la vita sessuale (dati sensibili). Sulle implicazioni dei tasti di apprezzamento e di condivisione si veda Popoli (2014), cit., par. 2.4.

piano sociale o su quello delle cosiddette "obbligazioni naturali"[26]. Inoltre, è da escludersi che la presenza di un atto costitutivo o di uno statuto siano elementi distintivi delle associazioni poiché, non essendovi obblighi di legge in tal senso, la volontà degli aderenti può essere manifestata in qualsiasi forma, anche oralmente[27].

Un altro aspetto su cui vale la pena di soffermarsi è quello della «autonoma consistenza del fenomeno associativo […] rispetto alla sommatoria delle forze degli aderenti»[28]. L'associazione, cioè, dovrebbe essere una realtà distinta e indipendente dalle singole volontà che la hanno costituita. Con riferimento ai *social network*, questo requisito può considerarsi sussistente, dal momento che la vita della *community* è in effetti relativamente indipendente dalla manifestazione delle volontà individuali dei suoi membri, considerando che l'entrata di nuovi membri nella *community*, la fuoriuscita di alcuni di essi o i singoli comportamenti individuali all'interno del *social network* non incidono, se non marginalmente, nella vita del gruppo. Ciò che manca, semmai, è quel requisito immateriale dell'associazione che taluni ritengano debba integrare gli elementi materiali sopra descritti, cioè il legame ideale che unisce gli appartenenti al gruppo[29]. La condivisione di informazioni attraverso le interazioni *social*, infatti, tende a configurarsi più come fine materiale che come legame ideale.

Il vincolo giuridico che lega fra loro gli associati è un atto negoziale di natura contrattuale, che può essere ricondotto alla fattispecie del contratto plurilaterale con comunione di scopo, nel quale le prestazioni di tutte le parti sono dirette a uno scopo comune[30]; nel caso dei *social network*, secondo qualcuno le clausole accettate dagli utenti al momento dell'iscrizione possono integrare anche la fattispecie del contratto di rete plurilaterale[31], pensato per legare fra loro soggetti indipendenti (solitamente imprenditori) che intendono "fare sistema", anche se la ricostruzione più convincente è quella del contratto di somministrazione o di appalto di servizi *ex* art. 1677 del codice civile[32]. Il contenuto del contratto associativo può essere libera-

[26] Guzzetta (2003), cit., pp. 74-82.

[27] P. Caretti e G. Tarli Barbieri (2017), *I diritti fondamentali*, Torino, Giappichelli, p. 474.

[28] Guzzetta (2003), cit., p. 15.

[29] Guzzetta (2003), p. 16.

[30] Artt. 1420, 1446, 1459 e 1466 del Codice civile.

[31] Art. 3 commi 4-*ter* e 4-*quinquies* della legge 9 aprile 2009, n. 33.

[32] Sulla natura del contratto si vedano, oltre a Popoli (2014), cit., anche: S. A. Cerrato (2011), *I rapporti contrattuali (anche associativi) tra i soggetti del social network*, in *Aida. Annali del diritto d'autore, della cultura e dello spettacolo*, partic. pp. 182-183; S. Sica e G. Giannone Codiglione (2012), *Social network sites e il "labirinto" delle responsabilità*, in *Giurisprudenza di merito*, n. 12, partic. pp. 2718-2719.

mente determinato dalle parti (art. 1322 c. c.), fermo restando che, anche nel caso dei contratti atipici, le norme dettate in via generale per i contratti dal codice civile non sono derogabili dall'autonomia delle parti (art. 1323 c. c.). Poiché non è prevista alcuna forma specifica per l'atto costitutivo di un'associazione non riconosciuta, occorre valutare se le clausole d'uso che gli utenti sottoscrivono al momento dell'iscrizione a un *social network* possano essere considerate alla stregua di un contratto associativo.

In effetti, l'aspetto contrattuale rappresenta l'elemento di maggiore debolezza nella ricostruzione eventualmente tesa ad assimilare le *social network communities* ad associazioni non riconosciute, per via del fatto che nei contratti – variamente denominati come «condizioni d'uso» (*Face-book),* «termini di servizio» (*Twitter*e *Google*), «contratto di licenza» (*LinkedIn*) – non vi è alcun riferimento ad un vincolo associativo né agli scopi che la presunta associazione sarebbe chiamata a perseguire. Il tenore delle clausole porta piuttosto a considerare queste licenze alla stregua di contratti di appalto o di somministrazione di servizi in cui la causa del negozio giuridico, a dispetto della pretesa gratuità della fornitura del servizio, consiste in realtà in un interesse patrimoniale, posto che l'utente diviene un'entità di rilevanza economica nel momento in cui il gestore della piattaforma utilizza i dati relativi agli utenti per attrarre inserzioni pubblicitarie a fini di profitto. Secondo questa ricostruzione, i rapporti "orizzontali" fra gli utenti della piattaforma si esaurirebbero sul piano dell'interazione sociale e umana, giuridicamente irrilevante[33].

Se, dunque, la sottoscrizione dei termini del servizio non corrisponde in alcun modo all'adesione a una associazione, l'ipotesi iniziale sembra non trovi conferma. Risulterebbe così automaticamente superato il problema che qualcuno ha sollevato[34] circa l'incompatibilità fra il divieto di associazioni segrete di cui all'art. 18 Cost. – cioè di quelle associazioni che, essendo dirette ad interferire con i pubblici poteri, nascondono la propria esistenza, occultando i nomi dei propri associati, la sede delle riunioni e le finalità perseguite[35] – e il fatto che tanto la direttiva sul commercio elettronico

[33] Cerrato (2011), cit., p. 186, qualifica le interazioni fra gli utenti del *social network* come rapporti "di cortesia" senza alcun carattere negoziale. Tuttavia, è possibile, secondo l'Autore (partic. p. 190), che il vincolo di "amicizia" si trasformi in un rapporto contrattuale, nei casi in cui l'interazione sia preordinata all'accesso a contenuti e informazioni presenti nelle pagine personali di taluni utenti al fine di soddisfare un interesse economicamente rilevante, anche se non necessariamente di natura patrimoniale, di qualcuno di essi.

[34] S. Sassi (2013), *La libertà di associazione nel "nuovo ecosistema mediatico": spunti problematici sull'applicazione dell'art. 18 della Costituzione. Il (recente) caso dell'associazione xenofoba on-line*, in Aa. Vv., *Da Internet ai Social Network. Il diritto di ricevere e comunicare informazioni e idee*, Rimini, Maggioli, partic. pp. 100 ss.

[35] Art. 1 della legge 25 gennaio 1982, n. 17.

quanto il nuovo regolamento europeo n. 2016/679 consentono agli utenti di Internet l'anonimato[36] e la pseudonimizzazione[37].

Il tema del diritto all'anonimato – che non sembra essere garantito nel vigente ordinamento giuridico – richiederebbe in realtà un approfondimento ben maggiore di queste poche righe[38]. Certamente, il ricondurre le *social network communities* nella categoria delle associazioni potrebbe tradursi in una restrizione degli spazi di libertà individuale, perché quelle forme di mobilitazione collettiva che utilizzano Internet rivendicando l'anonimato rischierebbero di incappare nel divieto costituzionale[39]. Tuttavia, non va trascurato il fatto che il requisito della segretezza posto dall'art. 18 Cost. va inteso in stretta connessione con le finalità che l'associazione persegue: nei limiti in cui l'associazione non ha finalità politiche, e non tende tramite la segretezza a formare "uno Stato nello Stato", l'associazione non potrà essere considerata illecita solo in quanto segreta; lo sarà, però, qualora tramite la segretezza persegua fini vietati ai singoli dalla legge penale[40]. Inoltre, Pace ha sottolineato che la segretezza costituzionalmente proibita deve «avvolgere l'associazione nel suo complesso»: deve cioè trattarsi di una segretezza intenzionalmente voluta dagli associati non solo nei confronti delle

[36] Il *considerando* n. 14 della direttiva n. 200/31/Ce precisa che «la presente direttiva non può impedire l'utilizzazione anonima di reti aperte quali Internet». In effetti, però, nel momento in cui si accede alla Rete tramite un servizio di comunicazione elettronica, l'anonimato non può essere garantito, sia perché per usufruire del servizio di connessione a Internet il contraente è tenuto a fornire le proprie generalità, sia perché l'accesso a Internet avviene attraverso un indirizzo Ip statico o dinamico che identifica il terminale da cui avviene l'accesso in Rete. Tuttavia, l'effettivo utente del servizio di connessione può benissimo non coincidere con il contraente. Inoltre, sebbene normalmente le piattaforme di *social networking* richiedano l'identificazione di coloro che vogliono usufruirne – richiedendo non solo l'auto-identificazione dell'utente attraverso la dichiarazione delle proprie generalità, ma spesso alcuni elementi di identificazione aggiuntivi, quali l'indirizzo *e-mail* o il numero del telefono cellulare – non vi è alcuna garanzia che i dati forniti corrispondano effettivamente al vero.

[37] All'art. 4, comma 5, il regolamento consente la presudonimizzazione, ovvero il «trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile». Si veda in proposito S. Calzolaio (2017a), *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in *Federalismi.it*, n. 24, p. 11 ss.

[38] Si vedano sul tema dell'anonimato *online*: M. Betzu (2011), *Anonimato e responsablità in* Internet, in *Costituzionalismo*.it, n. 2, pp. 1-25; M. Manetti (2014), *Libertà di pensiero e anonimato in Rete*, in *Osservatorio costituzionale Aic*, n. 1, pp.1-11; E. Pelino (2008), *L'anonimato su Internet*, in G. Finocchiaro (a cura di), *Diritto all'anonimato*, Padova, Cedam, pp. 289-320.

[39] Cuniberti (2015), cit., p. 281.

[40] Pace (1988), cit., p. 361.

autorità pubbliche, ma dell'intera collettività; la segretezza deve inoltre riguardare l'esistenza stessa dell'associazione e non soltanto i suoi fini o l'identità degli aderenti[41].

Cuniberti ha definito «un errore di prospettiva» l'estensione analogica della nozione costituzionale di associazione alle *social network communities*: «il ragionare di associazioni "in rete" come una realtà in qualche modo autonoma o distinta rispetto alle altre associazioni rischia di condurre ad esiti distorsivi, e persino controproducenti, nel momento in cui si pretende di attribuire la dignità costituzionale di associazione a tutte quelle variegate forme di aggregazione, spesso del tutto fluide e contingenti, che si vengono a formare in rete, ed in particolare nei c. d. *social network*, e che talora vengono designate, nello stesso (ingannevole e tutt'altro che neutro) linguaggio dei *social network*, con il termine ambiguo di *communities*»; si tratterebbe di una distorsione sia perché dalla volontà di iscriversi a un *social network* non può desumersi automaticamente la corrispondente volontà di costituire un vincolo associativo, sia perché spesso si tratta di aggregazioni fluide e prive di una stabile struttura organizzativa, sia perché, infine, in una associazione i fini perseguiti dal suo fondatore e dai successivi aderenti devono essere comuni, mentre in un *social network* il gestore della piattaforma persegue un fine esclusivamente commerciale, diverso comunque da quello degli utenti[42].

Tuttavia, prendendo in esame nello specifico il fenomeno dei "gruppi" di utenti[43] che possono essere creati all'interno di un *social network*, non si può del tutto escludere la possibilità che il gruppo assuma talvolta una rilevanza autonoma rispetto all'agire dei suoi componenti, che il suo fondatore subordini l'adesione allo stesso all'accettazione di determinate regole di comportamento e che tale regolamento ricalchi in qualche modo i tratti fondamentali dello statuto di un'associazione[44].

Qualche ulteriore spunto in tal senso sembra provenire dalla giurisprudenza penale. Infatti, «nei tempi più recenti, il diritto penale, non solo italiano, è stato investito dall'emersione di figure di associazioni criminose, tipicamente di portata transnazionale, nelle quali, anche in ragione dell'evoluzione delle tecnologie dell'informazione nel mondo globalizzato, l'accordo di partecipazione a tali associazioni non appare più semplicemente ricostruibile nei termini di accordo o scambio di consenso: difetta, in tale

[41] Pace (1977), cit., pp. 271-18.

[42] Cuniberti (2015), cit., p. 281.

[43] Il riferimento è al fenomeno della creazione di pagine virtuali dedicate a un determinato personaggio, prodotto, evento o esperienza, attraverso cui coloro che sono particolarmente interessati al tema possono confrontarsi e scambiare opinioni.

[44] Cerrato (2011), cit., pp. 205-206.

fattispecie di manifestazione di volontà partecipativa, un incontro dialogico tra la proposta,la controproposta e l'accettazione»[45]. Ciò ha condotto il giudice di legittimità a ritenere, in tema di associazione per delinquere finalizzata allo scambio di materiale pedopornografico, che l'elemento oggettivo della fattispecie sussista nel caso di «una comunità virtuale in Internet, stabile ed organizzata, regolata dalle disposizioni dettate dal promotore e gestore, volta allo scambio ed alla divulgazione, tra gli attuali membri ed i futuri aderenti, di foto pedopornografiche» e che sia rinvenibile l'elemento soggettivo nel fatto che tutti gli aderenti al *consortium sceleris* fossero stati resi edotti dello scopo e delle finalità del gruppo, consistenti nello scambio virtuale di immagini pedoponografiche[46]. Analogamente, qualche anno dopo la suprema Corte ha affermato che, ai fini della configurabilità del delitto di associazione sovversiva con finalità di terrorismo internazionale, la necessità di una struttura organizzativa effettiva e tale da rendere possibile l'attuazione del programma criminale non implica necessariamente il riferimento a schemi organizzativi ordinari, essendo sufficiente che i modelli di aggregazione tra sodali integrino il *minimum* organizzativo richiesto a tale fine[47]. E ancora, la Corte ha ritenuto configurabile il delitto di associazione per delinquere finalizzata alla realizzazione di accessi abusivi a sistemi informatici da parte di un sodalizio criminoso operante esclusivamente in rete, anche quando non risulti individuabile l'esistenza di una struttura di vertice del gruppo[48].

Queste recenti tendenze espresse in ambito penalistico, soprattutto se confermate da più recente giurisprudenza, potrebbero rappresentare un appiglio – pur se per il momento assai scivoloso – per suffragare l'idea di una qualificazione delle *social network communities* alla stregua di associazioni non riconosciute, al di là della manifesta inadeguatezza delle clausole contrattuali.

Va da sé che, ai sensi dell'art. 18 Cost., i fini di siffatte *communities*/associazioni non potrebbero corrispondere a quelli che la legge penale vieta ai singoli. Poiché tale divieto sussiste solo per le associazioni propriamente dette, e non per le formazioni sociali in genere, sulle *communities* non considerate associazioni non graverebbe alcun vincolo costituzionale riguardo ai fini. Quindi, eventuali reati derivanti dalla condivisione di materiale illecito – dalla violazione dei diritti di proprietà intellettuale alla circolazione di materiale pedopornografico – sarebbero imputabili solo ai

[45] A. Gaglioti (2017), *La partecipazione ad associazioni con finalità di terrorismo internazionale e la dottrina degli scambi senza accordo*, in *Sicurezza e giustizia*, n. 2, p. 31.

[46] Corte di Cassazione, terza sezione penale, sentenza 2 dicembre 2004, n. 8296.

[47] Corte di Cassazione, quinta sezione penale, sentenza 11 giugno 2008, n. 31389.

[48] Corte di Cassazione, quinta sezione penale, sentenza 12 settembre 2013, n. 50620.

singoli autori delle condotte criminose, eventualmente in concorso fra loro, e non alla *community* complessivamente intesa. Questo, del resto, è l'orientamento dominante della giurisprudenza in materia penale, come si vedrà meglio più avanti nel capitolo dedicato a questo tema.

In sintesi, quanto scritto fin qui porta ad individuare nelle *social network communities* alcune caratteristiche che le rendono assimilabili alle associazioni ex art. 18 Cost., con qualche difficoltà però in relazione alla mancanza di un'espressa volontà di associarsi da parte degli aderenti. Il vantaggio di una siffatta ricostruzione risiederebbe principalmente nella possibilità di poter reprimere più efficacemente talune fattispecie criminose svolte in modo "associativo" attraverso Internet, facendo leva sul divieto costituzionale di fini associativi vietati ai singoli dalla legge penale.

3. L'attività di *social networking* come riunione *ex* art. 17 Cost.

In un'accezione classica, l'art. 17 Cost. tutela «il diritto di ciascuno di stare fisicamente con gli altri»[49]. La differenza fra riunione e associazione consiste nel fatto che, mentre le associazioni sono caratterizzate da una struttura organizzativa stabile, per le riunioni questo requisito non è richiesto: il vincolo fra coloro che si riuniscono non è di tipo giuridico, come nell'associazione, ma solo di tipo materiale, consistente cioè nello stare fisicamente insieme[50]. Quindi, elemento necessario e sufficiente per qualificare una riunione ai sensi dell'art. 17 Cost. è la «volontaria compresenza fisica di più persone nello stesso luogo»[51], tanto da poter dire che la compresenza fisica costituisce la *conditio sine qua non* della riunione[52]. Si ha invece un assembramento quando più persone si riuniscono non volontariamente, ma casualmente[53]; tuttavia, l'assembramento può essere assimilato alla riunione nei casi in cui almeno lo scopo per via del quale più persone convengono nello stesso luogo sia comune a tutte (come accade, ad esempio, quando si forma una fila di persone che intendono usufruire di un medesimo bene o servizio)[54]. In sintesi, dunque, l'art. 17 Cost. si riferisce a tutte le forme di compresenza fisica volontaria, anche non concertate[55].

[49] Pace (1988), cit., p. 291.
[50] Ivi, p. 302.
[51] A. Pace (1967), *La libertà di riunione nella costituzione italiana*, Milano, Giuffrè, pp. 32 e 46.
[52] Pace (1988), cit., p. 304.
[53] Pace (1967), cit., p. 17.
[54] Ivi, p. 23.
[55] Pace (1988), cit., p. 298.

Secondo questo ragionamento, l'elemento su cui si fonda la libertà di riunione è quello fisico: la compresenza delle persone deve essere appunto fisica e deve realizzarsi in un luogo fisico; i limiti cui la libertà di riunione è soggetta sono graduati in base al luogo in cui la riunione si svolge, che può essere privato, aperto al pubblico o pubblico[56]; il requisito dello svolgimento pacifico e senza armi va riferito alla necessità di preservare l'ordine pubblico inteso in senso materiale[57]. È possibile, però, prescindere dal presupposto della compresenza fisica e immaginare che lo "stare insieme" in un *social network* sia equiparabile a una riunione?[58]

Per la verità, l'accento posto sull'elemento fisico rappresenta il principale ostacolo alla qualificazione dell'attività di *social networking* alla stregua di una riunione. Infatti, per quanto sia possibile – anzi, non infrequente – che i membri di una *community* siano contemporaneamente interconnessi allo scopo di condividere contenuti di vario tipo, volendo attualizzare il pensiero di Alessandro Pace questo fenomeno, certamente caratterizzato da volontarietà e plurisoggettività, potrebbe essere considerato una riunione solo a patto di considerare Internet, o più precisamente il *social network*, come un "luogo".

Non è scontato, infatti, che il concetto di luogo si identifichi con lo spazio fisico. Già Aristotele ne aveva dato una definizione – luogo come "limite immobile primo del contenente" – che ne coglieva in qualche modo l'immaterialità[59]. Nella filosofia aristotelica, il *tòpos* include il duplice si-

[56] Secondo Pace (1967), cit., p. 88, le riunioni in luogo privato non necessitano di preavviso e possono essere sciolte solo in caso di reati; quelle in luogo aperto al pubblico non necessitano di preavviso, ma possono essere sciolte per qualsiasi caso di turbativa dell'ordine pubblico (anche consistente in reati); quelle in luogo pubblico necessitano di preavviso e possono essere sciolte per qualsiasi ragione di tutela della sicurezza, dell'incolumità pubblica e del buon costume.

[57] Pace (1967), cit., pp. 159 ss; Pace (1988), cit., p. 306.

[58] P. Marsocci (2011), *Lo spazio di Internet nel costituzionalismo*, in *Costituzionalismo.it*, n. 2, p. 14.

[59] Aristotele (1967), *La Fisica*, Napoli, Loffredo, pp. 89-90: «Sembra poi che sia una questione grave e difficile comprendere il concetto di luogo, non solo perché esso presenta l'apparenza della materia e della forma, ma anche perché lo spostamento della cosa trasportata ha luogo nell'interno dello stesso contenente, che resta in riposo; appare infatti che il luogo possa essere un intervallo intermedio diverso dalle grandezze che si muovono. Vi contribuisce in qualche modo anche l'aria, che sembra essere incorporea; appare infatti che il luogo sia costituito non soltanto dai limiti del vaso, ma anche dall'intermedio fra questi limiti, come se fosse un vuoto. D'altronde, come il vaso è un luogo trasportabile, così anche il luogo è un vaso immobile; perciò quando ciò che è all'interno si muove e muta di posto in un contenente a sua volta in movimento, ad esempio una nave in un fiume, si serve di questo contenente come di un vaso, piuttosto che come di un luogo; il luogo, invece, vuol essere immobile; perciò il fiume tutto intero è piuttosto un luogo, poiché tutto intero è immobile. Sicché il luogo è il limite immobile primo del contenente»

gnificato di esistenza ed essenza: da un lato, un luogo è tale in quanto esiste fisicamente e quindi è materiale e misurabile; dall'altro, è l'uomo che attribuisce un senso e un significato a tale luogo. La prima definizione di luogo che si legge nel dizionario è quella di «parte dello spazio, idealmente o materialmente circoscritta»[60] oppure di «parte di spazio delimitata, considerata in funzione di ciò che in essa si colloca»[61]. Non è questa la sede per una trattazione filosofica del concetto di luogo, che richiederebbe maggiori competenze e approfondimento. Appare tuttavia evidente come queste definizioni di luogo possono riferirsi – se non a Internet in generale, che può essere considerato uno spazio senza confini – all'ambiente delimitato e circoscritto dei *social network*. Del resto, anche l'antropologo Marc Augè, che ha definito il "luogo antropologico" come «il luogo in cui vi è una coincidenza perfetta tra disposizione spaziale e organizzazione sociale»[62] – in contrapposizione ai "nonluoghi" come spazi di passaggio «nei quali non esiste a priori alcun legame simbolico immediatamente decifrabile tra gli individui che li frequentano»[63] e «in cui non è possibile leggere né le relazioni sociali né i simboli dell'identità collettiva e della storia condivisa»[64] – si chiede se i *social network* non possano essere concepiti come antitesi ai "nonluoghi", in quanto creano nuovi tipi di relazioni ed identità[65]. Non si nega così che la norma giuridica sia inconcepibile senza determinazioni di luogo e di tempo e che il luogo debba essere delimitato da confini in funzione inclusiva ed esclusiva[66], ma si accoglie piuttosto una nozione kelseniana della dimensione spazio-temporale, avulsa dall'elemento fisico, per la quale «fra le quattro sfere di validità di una norma, quella personale e quella materiale hanno la precedenza su quella territoriale e su quella temporale. […] Dire che una norma è valida per un dato territorio significa che essa concerne il comportamento umano che si verifica entro quel territorio. […] Qualsiasi territorio e qualsiasi tempo in cui si verifica un comportamento umano possono costituire la sfera territoriale e quella temporale di validità delle norme»[67]. Si può allora condividere l'idea per cui «lo spazio è

[60] Vocabolario *online* Treccani.

[61] F. Sabatini e V. Coletti (2008), *Dizionario della lingua italiana*, Firenze, Sansoni.

[62] M. Augè (2015) Voce "*Nonluogo*", in *Enciclopedia italiana*", Appendice IX, Roma, Treccani.

[63] *Ibid.*

[64] *Ibid.*

[65] *Ibid.*

[66] N. Irti (2004), *Voce "Geo-diritto*", in *Enciclopedia del Novecento*, supplemento III, Roma, Treccani. Ma per Id. (2001), *Norma e luoghi. Problemi di geo-diritto*, Roma-Bari, Laterza, pp. 65-66, lo spazio telematico è un "non-luogo".

[67] H. Kelsen (2000), *Teoria generale del diritto e dello Stato*, Milano, Etas, p. 43.

un'entità geografica, mentre il luogo è un'entità socio-culturale»[68]. In questa accezione, il *social network* può essere considerato come luogo aperto al pubblico[69], per il fatto che l'accesso alla piattaforma è consentito a tutti previa registrazione ed identificazione.

In tal senso si è espressa appunto la Corte di Cassazione nel 2014[70], stabilendo che ai fini della configurabilità del reato di molestie o disturbo alle persone (art. 660 c. p.) *Facebook* va considerato un luogo aperto al pubblico, in quanto luogo virtuale (piazza immateriale) aperto all'accesso di chiunque utilizzi la rete. Secondo i giudici della Cassazione, si tratterebbe di un'interpretazione estensiva «che la lettera della legge non impedisce di escludere dalla nozione di luogo e che, a fronte della rivoluzione portata alle forme di aggregazione e alle tradizionali nozioni di comunità sociale, la sua *ratio* impone, anzi, di considerare»[71]. È anche possibile, però, che un ristretto gruppo di utenti di un *social network* decidano di "riunirsi" virtualmente in forma riservata, per condividere informazioni in modo esclusivo: ci si chiede, allora, se in tali casi la nozione di luogo debba piuttosto coincidere con quella di luogo privato[72]. La distinzione non è di poco mo-

[68] S. Zamagni e P. Venturi (2017), *Da spazi a luoghi*, short paper n. 13, in *www.aiccon.it*. Anche Marsocci (2011), cit., sottolineando che Internet è una realtà artificiale, costruita dalle relazione fra gli individui (p. 4), evidenzia poi, richiamando Lawrence Lessig, che l'organizzazione di un ambiente artificiale immateriale, quale è Internet, può essere considerata un'architettura che, al pari dell'architettura urbana, è un degli strumenti di regolazione della convivenza civile, determinando modalità particolari di esercizio e garanzia dei diritti (p. 5).

[69] A. Gardino Carli (1997), *Riunione (libertà di)*, in *Digesto delle discipline pubblicistiche*, vol. XIII, Torino, Utet, p. 483, un luogo aperto al pubblico è «quello separato materialmente dall'esterno e di regola destinato ad accogliere un numero indeterminato di persone, il cui ingresso, in genere libero, può essere subordinato da parte di chi ne dispone a certe condizioni che prescindono da valutazioni personali». Per Pace (1988), cit., p. 171, è un «luogo (non importa se chiuso o all'aperto; ma comunque) separato dall'esterno (ad es. un recinto) l'accesso al quale – per volontà di chi ne è in legittimo godimento – è consentito a chiunque, liberamente ovvero a patto che siano rispettate alcune condizioni …». Infine A. Papa (2009), *Espressione e diffusione del pensiero in Internet. Tutela dei diritti e progresso tecnologico*, Torino, Giappichelli, p. 35 ritiene che, nel caso degli "spazi riservati" in Internet, cioè quegli spazi virtuali in cui possono accedere solo utenti identificati e registrati, «la riconducibilità al concetto fisico di "luoghi aperti al pubblico" non appare del tutto inappropriata».

[70] Corte di Cassazione, prima sezione penale, sentenza 12 settembre 2014, n. 37596. Si veda il commento di L. Diotallevi (2014), *Reato di molestia e* Facebook*, tra divieto di analogia in materia penale, (presunta) interpretazione evolutiva dell'art. 17 Cost. e configurabilità di un diritto di accesso a Internet*, in *Giurisprudenza costituzionale*, n. 5, pp. 4104-4111.

[71] Citazione tratta dalla sentenza indicata nella nota precedente.

[72] A. Pirozzoli (2004), *La libertà di riunione in Internet*, in *Il diritto dell'informazione e dell'informatica*, n. 4-5, p. 560. Per Gardino Carli (1997), cit., p. 484, il luogo privato è

mento, perché la possibilità per le pubbliche autorità di intervenire per sciogliere una riunione in luogo privato sono limitate alla commissione di reati nel corso della riunione stessa, mentre per le riunioni in luogo aperto al pubblico è lecito l'intervento dei pubblici poteri al fine di impedire turbative dell'ordine pubblico, anche a prescindere dalla realizzazione di fattispecie criminose.

In effetti, la scelta della Cassazione di definire la piattaforma *Facebook* come "luogo" può essere considerata esorbitante rispetto a quanto sia consentito da una legittima interpretazione estensiva della fattispecie penale[73], poiché la Rete prescinde da ogni riferimento di ordine spaziale, tanto da poter essere considerata un "non-luogo"[74]. Inoltre, posto che l'art. 660 c. p. è teso a punire quei comportamenti astrattamente idonei a suscitare, da parte della persona direttamente offesa, reazioni violente, tali da incidere negativamente sull'ordine pubblico, ciò non potrebbe verificarsi in un ambiente immateriale quale è la Rete[75]. Tuttavia, questa seconda considerazione non è del tutto condivisibile, perché tralascia di considerare che la Cassazione ha attribuito la nozione di luogo non a Internet in generale, ma a *Facebook*, che è un ambiente *online* circoscritto e delimitato, per quanto molto vasto, nel cui ambito possono facilmente verificarsi comportamenti che turbano l'ordine pubblico inteso come ordinata convivenza civile.

Ulteriori rilievi critici considerano l'applicazione dell'art. 17 Cost. alle riunioni telematiche non come una interpretazione evolutiva del dettato costituzionale, ma come una scorretta sovra-interpretazione, con cui «si manipola un testo normativo al fine di ricavarne norme da esso non espresse» che sono «frutto di ragionamenti fondati su premesse dogmatiche o ideologiche, che prescindono totalmente dall'interpretazione degli enunciati»[76]. Secondo questa visione, le coordinate spaziali entro cui la Costituzione colloca la libertà di riunione non sono nella disponibilità dell'interprete, ma derivano da leggi scientifiche[77]. L'obiezione può apparire fondata, se non fosse per il fatto che sono proprio le scienze fisiche che, con Einstein, hanno stato demolito il concetto di spazio e di tempo assoluti e separati l'uno dall'altro, affermando invece il concetto di spazio-tempo come un solo co-

«quello, riservato all'uso esclusivo di privati, nel quale gli estranei possono entrare soltanto per invito personale, o comunque con l'accordo di chi ne ha il godimento».

[73] Diotallevi (2014), cit., pp. 4105 ss.

[74] *Ibid.* Ma l'Autore sembra non cogliere la differenza fra Internet, che in effetti prescinde da ogni delimitazione spaziale, e lo specifico ambito di un *social network*, che invece è delimitato.

[75] *Ibid.*

[76] M. Betzu (2012), *Interpretazione e sovra-interpretazione dei diritti costituzionali nel cyberspazio*, in *Rivista Aic*, n. 4, p. 3.

[77] Ivi, p. 5.

strutto unico e omogeneo, nel quale non c'è un sistema di riferimento privilegiato e per ogni evento le coordinate spaziali e temporali sono legate tra di loro. Né è condivisibile la seconda obiezione per la quale, poiché il ciberspazio non ha confini, si vorrebbe limitare l'efficacia dell'art. 17 Cost. al solo inciso «i cittadini hanno diritto di riunirsi liberamente», senza attribuire alcun rilievo alle successive disposizioni relative al luogo della riunione[78]: in realtà non è così, perché un *social network* – come si è più volte ricordato – è a tutti gli effetti uno ambiente delimitato da confini, equiparabile a un luogo aperto al pubblico. Infine, se si accoglie la tesi di Pace – ma non solo[79] – per cui la libertà di riunione è strumentale all'esercizio di altri diritti di libertà[80], atteggiandosi quindi a mezzo tramite cui si può manifestare liberamente il pensiero, si demolisce anche la terza obiezione per cui gli articoli 21 e 17 Cost. non possono riferirsi a un medesimo fenomeno[81]: non è così, in realtà, perché si tratta di due prospettive diverse da cui considerare il medesimo accadimento (quella della libertà individuale di esprimere il proprio pensiero anche nell'ambito di una riunione e quello delle modalità con cui la riunione deve sciogliersi per non turbare l'ordine pubblico e la sicurezza e l'incolumità pubbliche). Non c'è dubbio che la riunione virtuale sia principalmente un'interazione comunicativa, ma non per questo non può essere considerata anche come fenomeno sociale che può avere un impatto sull'ordinata convivenza civile e che, pertanto, deve soggiacere ad alcune regole che ne disciplinano lo svolgimento.

Al di là della configurazione della Rete come un luogo, è un fatto che la compresenza *online* di più individui non può essere equiparata allo "stare fisicamente insieme" richiesto da Pace, proprio per la mancanza della fisicità delle persone. Va aggiunto che, nella visione di Pace, desta preoccupazione la tendenza a dilatare l'ambito di applicabilità delle disposizioni costituzionali – in particolare dell'art. 17 Cost. – che sovrappone al dettato normativo l'approccio emotivo dell'interprete o la sua "gerarchia culturale"[82], trasformando così le garanzie costituzionali in mere dichiarazioni di principio[83], senza contare che «prescindendosi dal presupposto della fisica

[78] *Ibid.*

[79] Si veda anche P. Barile (1984), *Diritti dell'uomo e libertà fondamentali*, Bologna, Il Mulino, p. 182.

[80] Pace (1977), cit., p. 147.

[81] *Ibid.*

[82] A. Pace (2001), *Metodi interpretativi e costituzionalismo*, in *Quaderni costituzionali*, n. 1, partic. pp. 55-56.

[83] A. Pace (2006), *Considerazioni preliminari*, in A. Pace e M. Manetti, *Art. 21. La libertà di manifestazione del proprio pensiero*, in G. Branca (a cura di), *Commentario della Costituzione*, Bologna, Zanichelli, p. 2.

compresenza, si finisce per riaccreditare quel concetto di sicurezza pubblica in senso ideale contro la quale ci si era battuti con successo negli anni '60»[84].

Se però si vuole sostenere l'equivalenza fra riunione fisica e attività di *social networking*, ci si può appigliare ad altre definizioni della libertà di riunione meno incentrate sull'elemento fisico e più su quello psicologico o volontaristico, come ad esempio quella per cui si considera riunione «l'adunata spontanea di più persone, motivata da interessi, finalità o attività comuni, oppure da un desiderio di rapporti amichevoli»[85]. Oppure quella di Barile per cui la riunione è essenzialmente una forma di esercizio collettivo di libertà individuali[86], senza conferire particolare rilevanza all'elemento della fisicità[87].

La disciplina costituzionale della libertà di riunione nulla dice circa le finalità della riunione stessa[88], ma pone alcuni limiti relativamente alle modalità di svolgimento delle riunioni, che devono avvenire «pacificamente e senz'armi», in modo che possa essere protetto l'ordine pubblico inteso in senso materiale[89]. Ora, è evidente che una riunione *online* non può comportare l'uso di armi materialmente intese, ma può comunque avere carattere non pacifico e tale da turbare l'ordine pubblico[90]: si pensi, ad esempio, al proliferare dello *hate speech* (manifestazione di incitamento all'odio e alla violenza) nei *social network*. Potrebbero allora essere sciolte quelle riunioni virtuali che avvengono con modalità tali da turbare l'ordine pubblico; nel caso di un *social network*, non si potrebbe certo impedire la totalità delle interazioni che avvengono attraverso la piattaforma, ma si potrebbero ostacolare solo quelle aventi carattere non pacifico attraverso strumenti automatici o semi-automatici di filtraggio. Strumenti che, come si vedrà nelle pagine che seguono, non potrebbero mai essere di tipo preventivo, per non incoraggiare la diffusione di forme di "censura privata" affidata alla discrezionalità dei *provider*[91]. Inoltre, per Pace occorre distinguere fra le riunioni

[84] *Ibid*.

[85] Gardino Carli, (1997), cit., p. 480.

[86] Barile (1984), cit., p. 182.

[87] Conseguentemente, riguardo al requisito della "pacificità", Barile (1984), cit., p. 183, ritiene che la riunione non sia pacifica quando sia in atto un turbamento dell'ordine pubblico materiale tale da disturbare – anche se non fisicamente – i partecipanti alla riunione.

[88] La libertà di riunione è infatti strumentale all'esercizio di altre libertà costituzionalmente protette, prima fra tutte la libertà di manifestare il proprio pensiero. Di conseguenza, non essendo la riunione altro che un mezzo di manifestazione del pensiero, è consentito riunirsi per qualunque fine lecito. Così Pace (1967), cit., p. 48 e p. 56.

[89] Gardino Carli (1997), cit., p. 484; Pace (1967), cit., p. 159.

[90] Per Barile (1984), cit., p. 183, si ha turbamento dell'ordine pubblico materiale nel caso di «un disordine di grado tale da disturbare (anche se non "fisicamente") in modo allarmante i terzi non partecipanti».

[91] Sulla censura privata si veda Bettoni (2011), cit.

il cui carattere complessivo sia non pacifico e quelle in cui solo alcuni degli intervenuti si comportano in modo non pacifico o sono armati: in quest'ultimo caso, non sarebbe lecito sciogliere l'intera riunione, ma sarebbe sufficiente allontanare i convenuti che abbiano un atteggiamento inappropriato[92]. *Mutatis mutandis*, la disciplina costituzionale applicata alle riunioni telematiche prevedrebbe di inibire l'attività di *social networking* soltanto con riguardo a coloro che manifestano atteggiamenti lesivi dell'ordine pubblico, non di sciogliere l'intera *community*.

Nell'ambito della libertà di riunione, il ruolo del *social network provider* può essere paragonabile a quello di chi apre al pubblico un luogo di cui ha la disponibilità materiale, affinché possa svolgersi al suo interno una riunione[93]. Il ché non significa che i *provider* possano o debbano filtrare preventivamente i contenuti che transitano *online* tramite i servizi da essi offerti, così come, nella realtà fisica, il proprietario o possessore del luogo in cui la riunione si svolge non interviene preventivamente nell'orientare i contenuti che durante la riunione verranno espressi. Occorre quindi valutare caso per caso quale sia l'effettivo ruolo svolto dal *provider*: qualora quest'ultimo intervenga attivamente nell'organizzare le interazioni fra gli utenti e nella gestione dei contenuti condivisi, può essere considerato come un partecipante alla riunione telematica; qualora invece mantenga un atteggiamento neutro, estraneo alla svolgimento della riunione, non può essere considerato responsabile di ciò che avviene nello svolgimento della stessa, così come non lo è il titolare del luogo fisico al cui interno la riunione si svolge.

Non manca, però, chi si chiede quale utilità possa avere il ricondurre l'interazione fra più soggetti attraverso Internet alla categoria della libertà di riunione piuttosto che a quella della libertà di manifestazione del pensiero (art. 21 Cost.), che peraltro gode di una tutela più intensa, non contemplando alcun onere preventivo, né alcuna possibilità di divieto da parte delle autorità pubbliche[94]. La considerazione non è irragionevole. Tuttavia, poiché si sta qui discutendo non di riunioni attraverso Internet in generale, ma di una particolare forma di riunione *online* rappresentata dall'attività di *social networking,* all'obiezione si può rispondere che il tema qui non è tanto quello di preservare la libertà individuale di esprimere il proprio pensiero anche attraverso Internet, quanto quello di porre un argine alla diffusione incontrollata, tramite *social network*, di contenuti che possono recare pregiudizio all'ordine pubblico, quali i discorsi d'odio o le *fake news*[95], attra-

[92] Pace (1967), cit., pp. 159 ss.
[93] Pirozzoli (2004), cit., par. 3.4.
[94] Cuniberti (2015), cit., p. 281.
[95] Si veda l'ultimo capitolo di questo libro.

verso un'analogia con le riunioni che non si svolgono pacificamente. Peraltro, anche l'art. 17 Cost., in riferimento alle riunioni "fisiche", non fa alcun riferimento al pensiero che durante la riunione viene espresso o ai fini cui la riunione tende – poiché a ciò provvede appunto l'art. 21 Cost. – ma protegge solo il pacifico svolgimento della riunione a tutela della sicurezza e dell'incolumità di chi vi partecipa e della collettività in genere.

In sintesi, a patto di non focalizzarsi troppo sulla nozione fisica di luogo e sull'elemento della compresenza fisica fra le persone, l'attività di *social networking* può essere considerata una forma di riunione "immateriale" *ex* art. 17 Cost. Questa ricostruzione avrebbe il pregio di offrire un fondamento costituzionale all'inibizione di quelle riunioni *online* che si svolgono in modo non pacifico, provocando turbamento dell'ordine pubblico, anche nel caso in cui non sia possibile individuare i singoli responsabili delle manifestazioni non pacifiche.

LA RESPONSABILITÀ CIVILE DEGLI INTERMEDIARI DIGITALI PER GLI ILLECITI COMMESSI DAGLI UTENTI

1. L'impianto normativo: la direttiva n. 2000/31/Ce e il d. lgs. n. 70/2003

La sigla Isp (*Internet service provider* o fornitore/prestatore di servizi via Internet) si riferisce a qualsiasi persona fisica o giuridica che presta un servizio della società dell'informazione (art. 2 lett. b della direttiva *e-commerce*). Tali servizi sono definiti, con rimando all'art. 1 di una precedente direttiva risalente al 1998[1], come «qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi». L'estrema ampiezza di tale definizione consente di riferirla non solo ai fornitori dei servizi via Internet così come essi operavano agli inizi degli anni Duemila, ma anche ai soggetti che oggi prestano servizi di tipo più moderno ed evoluto, quali ad esempio i motori di ricerca e i *social network provider* (Snp). È vero che la definizione sopra riportata fa riferimento a servizi prestati "dietro retribuzione", mentre una delle caratteristiche salienti dei *social media* o dei motori di ricerca è la loro gratuita disponibilità; tuttavia, l'avverbio "normalmente" allude al fatto che la retribuzione non sia un requisito assolutamente necessario, ma solo un elemento frequentemente previsto dalla prassi (almeno nel momento in cui la direttiva è stata approvata).

Come è noto l'impianto normativo su cui si fonda il regime di responsabilità degli intermediari digitali[2], si fonda sull'ormai datata direttiva euro-

[1] Direttiva 98/34/Ce del 22 giugno 1998, *che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione*, modificata dalla direttiva 98/48/Ce del 20 luglio 1998.

[2] La dottrina su questo tema è piuttosto vasta. *Ex multis* si vedano: L. Bugiolacchi (2016), *Quale responsabilità per il motore di ricerca in caso di mancata de-indicizzazione su legittima richiesta dell'interessato?*, in *Responsabilità civile e previdenza*, n. 2, pp. 571-

pea sul commercio elettronico[3] (in particolare sugli artt. da 12 a 15), recepita in Italia con d. lgs. n. 70/2003[4] (in particolare artt. da 14 a 17). La direttiva europea è stata adottata con l'obiettivo di favorire la libera circolazione e la promozione dei "servizi della società dell'informazione", eliminando gli ostacoli allo sviluppo del commercio elettronico[5]. In quest'ottica, occorreva favorire l'attività dei fornitori di servizi (Isp) senza gravarli di oneri eccessivi – quali, ad esempio, la sorveglianza *ex ante* o *ex post* sui contenuti diffusi dagli utenti attraverso la rete Internet, al fine di prevenire o reprimere gli illeciti – che ne avrebbero rallentato lo sviluppo. In altre parole, la direttiva europea – e, conseguentemente, la normativa italiana di attuazione – non hanno posto gli Isp in una posizione di garanzia[6], quale ad esempio quella del direttore responsabile di una testata giornalistica, che avrebbe attribuito loro una responsabilità per gli illeciti commessi dagli utenti. Peral-

582; M. Cocuccio (2015), *La responsabilità civile per fatto illecito dell'Internet Service Provider*, in *Responsabilità civile e previdenza*, n. 4, pp. 1312-1330 (partic. pp. 1314-1320); M. De Cata (2010), *La responsabilità civile dell'internet service provider*, Milano, Giuffrè; L. Diotallevi (2012), *Internet e social network, tra "fisiologia" costituzionale e "patologia" applicativa*, in *Giurisprudenza di merito*, n. 12, pp. 2507-2521 (partic. pp. 2513-2517); M. Gambini (2011), *Gli hosting providers tra doveri di diligenza professionale e assenza di un obbligo generale di sorveglianza sulle informazioni memorizzate*, in *Costituzionalismo.it*, n. 2, pp. 1-43; F. Giovannella (2016), *La responsabilità civile degli Internet Service Provider*, in G. Pascuzzi (a cura di), *Il diritto nell'era digitale*, Bologna, Il Mulino, pp. 227-247; M. Mensi e P. Falletta (2015a), *Il diritto del web. Casi e materiali*, Padova, Cedam (partic. cap. 5); P. Pirruccio (2012), *Diritto d'autore e responsabilità del provider*, in *Giurisprudenza di merito*, n. 12, pp. 2591-2620 (partic. pp. 2595-2597); O. Pollicino (2014), *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider*, in *Percorsi costituzionali*, n. 1, pp. 45-74 (pubblicato anche in *Consulta Online*, 3 febbraio 2014); S. Sica e G. Giannone Codiglione (2012), *Social network sites e il "labirinto" delle responsabilità*, in *Giurisprudenza di merito*, n. 12, pp. 2714-2733; E. Tosi (2012), *La responsabilità civile per fatto illecito degli Internet Service Provider e dei motori di ricerca a margine dei recenti casi "Google Suggest" per errata programmazione del software di ricerca e "Yahoo! Italia" per "link" illecito in violazione dei diritti di proprietà intellettuale*, in *Rivista di diritto industriale*, n. 1, pp. 44-66; E. Tosi (2017), *Contrasti giurisprudenziali in materia di responsabilità civile degli hosting provider – passivi e attivi – tra tipizzazione normativa e interpretazione evolutiva applicata alle nuove figure soggettive dei motori di ricerca, social network e aggregatori di contenuti*, in *Rivista di diritto industriale*, n. 1, pp. 75-122.

[3] 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*.

[4] Decreto legislativo 9 aprile 2003, n. 70, *Attuazione della direttiva 2000/31/Ce relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno*.

[5] Commissione europea, Com(97) 157 del 15 aprile 1997, *Un'iniziativa europea in materia di commercio elettronico*.

[6] Sulle posizioni di garanzia si veda, in questo libro, il capitolo dedicato ai profili di responsabilità penale degli intermediari digitali.

tro, agli inizi degli anni Duemila i servizi offerti dagli Isp erano assai meno articolati rispetto al momento attuale e il loro ruolo era prevalentemente quello di intermediari digitali "passivi", che si limitavano ad offrire servizi di connessione ad Internet e ad ospitare i contenuti prodotti dagli utenti sui propri *server*, senza alcun ruolo nella creazione, nell'organizzazione o nella presentazione di tali contenuti.

Prima dell'entrata in vigore della direttiva europea sul commercio elettronico e del d. lgs. n. 70/2003, la responsabilità civile dell'Isp trovava fondamento solo nel quadro generale della responsabilità extracontrattuale di cui all'art. 2043 del codice civile. Secondo l'orientamento giurisprudenziale dominante, il *provider*, non gravato da obblighi di sorveglianza preventiva, sarebbe stato ritenuto responsabile solo nel caso in cui avesse fornito, con dolo o colpa, un cosciente apporto causale alla realizzazione dell'evento dannoso, contribuendo così alla determinazione del danno; tuttavia, qualche pronuncia di merito ha individuato la colpa del *provider* proprio nel non aver controllato il contenuto delle comunicazioni illecite[7]. Occorreva certamente un intervento legislativo che facesse chiarezza sul tipo di attività svolta dagli intermediari digitali e conseguentemente sul regime di responsabilità.

1.1. Le tre categorie di intermediari digitali

La direttiva del 2000 e il decreto legislativo di attuazione approvato nel 2003 prevedono essenzialmente tre categorie di intermediari digitali che, a seconda del livello del loro coinvolgimento nelle attività dell'utente, godono di diversi regimi di esenzione da responsabilità civile indiretta (cioè derivante dalle condotte degli utenti). La direttiva si applica a qualsiasi tipo di illecito, con pochissime eccezioni *ratione materiae* (fra cui, ad esempio, i giochi d'azzardo, le lotterie e le scommesse *online*), ma esclude dal suo campo di applicazione tutte le questioni che sorgono in relazione al trattamento dei dati personali, per cui è prevista una disciplina specifica[8]. Questa importante eccezione è riprodotta nel d. lgs. n. 70/2003, art. 1, comma 2, lett. b.

La prima categoria di intermediari digitali[9] comprende i prestatori di servizi di semplice trasporto (attività di *mere conduit)*, che forniscono

[7] G. Miceli (2017), *Profili evolutivi della responsabilità in Rete: il ruolo degli* Internet Service Provider *tra prevenzione e repressione*, in *MediaLaws. Rivista di diritto dei media*, n. 1, pp. 106-115, p. 111.

[8] Si veda, in questo libro, il capitolo dedicato ai vincoli e alle responsabilità degli intermediari digitali nel trattamento dei dati personali.

[9] Art. 12 della direttiva *e-commerce* e art. 14 del d. lgs. di attuazione.

l'accesso a una rete di comunicazione oppure trasmettono le informazioni fornite dagli utenti del servizio, eventualmente anche praticando una memorizzazione temporanea, intermedia e transitoria delle stesse al solo fine di consentirne l'effettiva trasmissione. Appartengono a questa categoria, ad esempio, i fornitori di servizi di connettività ad Internet. Questo tipo di Isp non è responsabile delle informazioni trasmesse a condizione che il suo atteggiamento rimanga passivo. In altre parole, a condizione che l'Isp non dia origine alla trasmissione, non selezioni il destinatario della trasmissione e non selezioni né modifichi le informazioni trasmesse.

La seconda categoria[10] corrisponde ai prestatori di servizi di memorizzazione temporanea (attività di *caching*), cioè la memorizzazione automatica, intermedia e temporanea di informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro delle stesse ad altri destinatari. Rientrano in questa categoria, ad esempio, i fornitori di servizi di posta elettronica o i motori di ricerca. Anche in questo caso, l'Isp che effettua il *caching* non è responsabile delle informazioni provvisoriamente memorizzate, purché però mantenga un atteggiamento passivo, ovvero non modifichi le informazioni, si conformi alle condizioni di accesso e alle norme di aggiornamento delle stesse, non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni. Tuttavia, l'irresponsabilità dell'Isp che svolge attività di *caching* viene meno nel momento in cui quest'ultimo non ottempera a quanto richiesto dal paragrafo contrassegnato dalla lettera *e*, che presuppone che l'Isp «agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione». Dunque, all'Isp di *caching* non è richiesto soltanto un atteggiamento passivo, ma sono imposti per legge anche obblighi di *facere,* al fine di mantenere una posizione di irresponsabilità, che prescindono dall'ordine dell'autorità competente (amministrativa o giudiziaria).

Va peraltro evidenziata l'ambiguità della locuzione "effettivamente a conoscenza"[11]. Come verrà meglio precisato più avanti attraverso l'esame della giurisprudenza, infatti, può risultare dubbio se occorra una conoscenza derivante da una notificazione in qualche modo (e in quale modo?) "qua-

[10] Art. 13 della direttiva *e-commerce* e art. 15 del d. lgs. di attuazione.

[11] Sulla nozione di "conoscenza effettiva" richiesta dalla normativa vigente si veda M. Montanari (2017), *La responsabilità delle piattaforme on-line (il caso Rosanna Cantone)*, in *Il diritto dell'informazione e dell'informatica*, n. 2, partic. pp. 274 ss.

lificata" oppure se sia sufficiente la mera conoscenza di fatto, che può essere difficile da dimostrare. La giurisprudenza sembra essere per lo più orientata nel senso di considerare efficace, ai fini dell'acquisizione della conoscenza da parte dell'Isp, la diffida di parte, anche in assenza di un ordine dell'autorità giudiziaria o amministrativa. Tuttavia, questa soluzione «può essere foriera di censure di responsabilità in capo all'Isp, nel caso in cui questi agisca sulla base di una diffida rivelatasi successivamente priva di fondamento»[12], anche perché né la direttiva europea né la normativa italiana di attuazione chiariscono in alcun modo questo aspetto.

Infine, appartengono alla terza categoria[13] i prestatori di servizi che memorizzano – non temporaneamente, ma durevolmente – le informazioni fornite dagli utenti (attività di *hosting*). Questa definizione può riferirsi, ad esempio, ai soggetti che consentono agli utenti di caricare (*upload*) i propri contenuti in uno spazio dedicato, come un sito Internet, un blog o anche una pagina personale di un *social network*. In questo caso, l'esclusione dalla responsabilità può applicarsi purché l'utente che fornisce i contenuti da memorizzare non agisca sotto l'autorità o il controllo dell'Isp. In altre parole, si presuppone che l'Isp si mantenga del tutto neutrale rispetto ai contenuti diffusi dagli utenti. Peraltro, l'irresponsabilità presuppone anche che l'Isp non sia «effettivamente a conoscenza» dell'illiceità delle attività degli utenti o delle informazioni da essi prodotte oppure di fatti e circostanze che rendono tali attività o informazioni illecite. Sull'ambiguità del riferimento all'effettiva conoscenza si veda quanto giù scritto *supra*[14]. Se ne deduce, quindi che, per il solo fatto di essere venuto a conoscenza dell'illiceità degli *user-generated/distributed content*, il *provider* non possa più essere considerato esente da responsabilità. Nel comma successivo (lettera *b*) è inoltre scritto che l'Isp, al fine di invocare l'irresponsabilità, deve agire immedia-

[12] Tosi (2012), cit., p. 53. Si veda anche Gambini (2011), cit., p. 12, che sostiene la tesi che sia imprescindibile la comunicazione formale da parte dell'autorità pubblica competente, perché «in assenza della comunicazione dell'autorità, dato che essi non disporrebbero di punti certi di riferimento per dirimere il dubbio sulla sussistenza dell'obbligo di rimozione». Inoltre, «valutazioni di tipo economico finiranno con il condizionare la decisione dei *provider*, i quali, in attesa dell'individuazione ad opera della giurisprudenza di criteri univoci cui attenersi, privilegeranno gli interessi dei soggetti patrimonialmente più affidabili, quali le grandi imprese, e ciò a scapito di quelli meno solvibili, a partire dai soggetti che utilizzano Internet come mezzo di espressione delle idee e a scopo non professionale».

[13] Art. 14 della direttiva *e-commerce* e art. 16 del d. lgs. di attuazione.

[14] Un'ulteriore ambiguità, sempre a proposito della conoscenza, deriva dalla lettera del testo normativo (d. lgs. n. 70/2003), che utilizza l'espressione "effettiva conoscenza" negli artt. 15 e 16 in riferimento all'illecito penale, l'espressione "al corrente di fatti manifestamente illegali" nell'art. 16 in riferimento all'illecito civile e infine menziona la semplice conoscenza nell'art. 17 in riferimento agli obblighi di informativa nei confronti delle competenti autorità. Cfr. sul punto Tosi (2012), cit., p. 54.

tamente per rimuovere le informazioni o per disabilitarne l'accesso «non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti». Ciò lascerebbe intendere – pur con qualche dubbio – che l'effettiva conoscenza possa essere raggiunta solo in seguito a una comunicazione "qualificata". Per la precisione, l'inciso «su comunicazione delle autorità competenti» non è presente nell'art. 14 della direttiva *e-commerce*, ma è stato aggiunto nel decreto legislativo di attuazione. Evidentemente, il legislatore italiano ha voluto allargare le maglie dell'esenzione di responsabilità del *provider*, anche se tendenzialmente la giurisprudenza di merito si è orientata nel senso di attribuire a quest'ultimo la responsabilità civile derivante alla conoscenza dell'illecito, indipendentemente da una comunicazione delle competenti autorità[15].

A tutti e tre i tipi di *provider*, come esplicitamente previsto dalla normativa, le competenti autorità giudiziarie o amministrative possano esigere, anche in via d'urgenza, di impedire o porre fine alle violazioni commesse attraverso i contenuti prodotti dagli utenti. Dunque, su richiesta dell'autorità sorge in capo all'Isp un obbligo di attivazione consistente nell'inibizione dell'accesso al contenuto illecito, il cui eventuale inadempimento comporta per l'Isp l'attribuzione di responsabilità civile (ultimo comma dell'art. 15 della direttiva *e-commerce* e dell'art. 17 del d. lgs. di attuazione). Sempre a richiesta delle competenti autorità, gli Isp sono tenuti a fornire senza indugio le informazioni in loro possesso atte ad identificare i destinatari dei servizi, al fine di individuare e prevenire attività illecite (comma 2 dell'art. 15 della direttiva *e-commerce* e comma 2 lett. *b* dell'art. 17 del d. lgs. di attuazione).

1.2. Gli obblighi gravanti sugli Isp e le limitazioni di responsabilità

La questione più spinosa riguarda, però, il comportamento che il *provider* deve assumere qualora si accorga del carattere illecito di talune attività o informazioni riferibili agli utenti dei servizi via Internet, a prescindere da ordini provenienti dalle competenti autorità. A ciò sono dedicati l'art. 15 della direttiva *e-commerce* e l'art. 17 del d. lgs. di attuazione. La normativa esclude che gli Isp possano essere assoggettati ad un obbligo generale di sorveglianza sulle informazioni trasmesse o memorizzate, o ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. Diversamente, i *provider* sarebbero gravati da oneri eccessivi che recherebbero grave intralcio alle loro attività, ostacolando lo sviluppo del commercio elettronico e, più in generale, di tutti i servizi della

[15] Giovannella (2016), cit., p. 231.

società dell'informazione. In realtà, più precisamente la normativa non sembra escludere obblighi di sorveglianza *tout court*, ma solo obblighi di sorveglianza *preventiva*. Infatti, non vengono esclusi – come evidenziato qui di seguito – obblighi di sorveglianza *passiva* insorgenti al momento dell'acquisizione della conoscenza del fatto illecito[16].

Dunque, la direttiva europea (art. 15, comma 2), consente che gli Stati membri possano assoggettare gli intermediari digitali ad obblighi di informativa nei confronti delle autorità giudiziaria o amministrativa relativamente ad attività illecite svolte attraverso Internet e all'identità dei loro autori. Così, la normativa italiana (art. 17, comma 3) ha previsto per l'Isp l'obbligo di informativa nei confronti delle autorità giudiziarie o amministrative, che deve essere assolto spontaneamente dal *provider* nel momento in cui acquisisce conoscenza del carattere illecito di talune informazioni o attività riferibili ai destinatari dei servizi, che possono pregiudicare i diritti dei terzi. L'inadempimento comporta per l'Isp attribuzione di responsabilità civile (art. 17 commi 2e 3 del d. lgs. n. 70/2003) di tipo extracontrattuale, *ex* artt. 2043[17] del Codice civile. La responsabilità verrebbe attribuita all'Isp a titolo di colpa se, accortosi della presenza di materiale "sospetto" sul sito, l'Isp si astenesse dall'accertarne l'illiceità e conseguentemente dal rimuoverlo; a titolo di dolo, invece, se, consapevole dell'antigiuridicità della condotta dell'utente, si astenesse dall'intervenire, segnalando il caso alle competenti autorità e procedendo alla rimozione dei contenuti. In quest'ultima ipotesi, può ravvisarsi anche un concorso del *provider* nell'illecito compiuto dall'utente, dando così luogo ad un'obbligazione risarcitoria solidale ai sensi dell'art. art. 2055[18]del codice civile.

Secondo una certa interpretazione, per la verità minoritaria[19], ferma restando l'assenza di un generale obbligo di sorveglianza preventiva in capo ai *provider*, l'accento andrebbe posto sulla natura potenzialmente pericolosa dell'attività da essi svolta, in quanto le condotte degli utenti mediante i servizi prestati dall'Isp possono essere fonte di pericolo per se stessi o per altri; quindi il *provider* avrebbe l'obbligo di adottare ogni possibile precauzione e cautela idonea ad evitare l'evento dannoso *ex* art. 2050 del codice

[16] Tosi (2012), cit., p. 52.

[17] Codice civile, art. 2043: «Qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno».

[18] Codice civile, art. 2055, comma 1: «Se il fatto dannoso è imputabile a più persone, tutte sono obbligate in solido al risarcimento del danno». Sulla questione della responsabilità solidale dell'Isp si veda P. Pirruccio (2012), cit., p. 2607.

[19] De Cata (2010), cit., pp. 94 ss.; Miceli (2017), cit.

civile[20]. L'orientamento giurisprudenziale dominante[21] considera attività pericolose[22], ai sensi dell'art. 2050 c.c., non solo quelle qualificate come tali dalla legge di pubblica sicurezza e da altre leggi speciali, ma anche quelle che, per la loro stessa natura o per le caratteristiche dei mezzi adoperati, comportino, in ragione della loro spiccata potenzialità offensiva, una rilevante possibilità del verificarsi di un danno. Il punto è che, ai fini dell'applicabilità dell'art. 2050 c. c., l'attività deve essere pericolosa in sé in base a un giudizio prognostico, non risultare pericolosa per via della condotta del responsabile, in base quindi a una valutazione *ex post* successiva al verificarsi dell'evento dannoso. È quindi dubbio se ogni attività degli Isp, in mancanza di una norma di legge che la qualifichi espressamente come pericolosa, possieda di per sé le suddette caratteristiche. La pericolosità può essere considerata inerente alla specifica ipotesi del trattamento dei dati personali, in base all'art. 15 comma 1 del d. lgs. n. 196/2003, secondo cui «chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 20150 del codice civile».

Al di là di questa fattispecie, contemplata appunto in una *lex specialis*, il dubbio continua a sussistere in relazione agli altri tipi di attività dell'Isp. Tra l'altro, in caso di attività pericolosa il danneggiante convenuto, per sottrarsi all'obbligazione risarcitoria *ex* art. 2050 c. c., dovrebbe dimostrare che, pur avendo posto in essere tutti i possibili accorgimenti e tutte le possibili precauzioni per neutralizzare il pericolo, l'evento dannoso si sarebbe verificato ugualmente, essendo imprevedibile o inevitabile. Ciò comporterebbe per l'Isp un onere probatorio assai gravoso, che va al di là della dimostrazione della normale diligenza, prudenza e perizia[23]. La soluzione interpretativa basata sull'art. 2050 c. c., dunque, non appare pienamente convincente.

1.3. L'evoluzione del ruolo degli Isp

Certamente, non può sfuggire come il ruolo degli Isp oggi sia profondamente cambiato, per via dell'evoluzione tecnologica, rispetto a quello prefigurato dalla normativa europea ed italiana dei primi anni Duemila,

[20] Codice civile, art. 2050: «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».

[21] Per tutte si vedano Corte di Cassazione, terza sezione civile, sentenza 18 maggio 2015, n. 10131, e sentenza 29 luglio 2015, n. 16052.

[22] G. Gentilini (2009), *Sulla responsabilità derivante dall'esercizio di attività pericolose. Alcune casistiche pratiche*, in *Diritto.it*, pp. 1-14.

[23] Così Gentilini (2009), cit. e De Cata (2010), cit. *Contra* Miceli (2017), cit., per il quale basterebbe la dimostrazione di aver agito con la massima diligenza, prudenza e perizia.

come emerge dall'analisi della giurisprudenza nelle pagine che seguono. È stato giustamente notato[24] come una spia di questo cambiamento possa essere rintracciata anche nella disciplina del Sistema Integrato delle Comunicazioni (Sic) di cui all'art. 43 del *Testo unico sui servizi di media audiovisivi e radiofonici* (Tusmar)[25]. Posto che un servizio di media audiovisivo è definito come quel servizio «che è sotto la responsabilità editoriale di un fornitore di servizi media e il cui obiettivo principale è la fornitura di programmi al fine di informare, intrattenere o istruire il grande pubblico, attraverso reti di comunicazioni elettroniche»[26], e che il fornitore di servizi di media è «la persona fisica o giuridica cui è riconducibile la responsabilità editoriale della scelta del contenuto audiovisivo del servizio di media audiovisivo e ne determina le modalità di organizzazione»[27], in una prima fase gli Isp, essendo considerati privi di responsabilità editoriale sui contenuti trasmessi tramite le piattaforme da essi gestite, non erano stati inclusi fra i soggetti i cui ricavi concorrevano a formare il Sic[28]. Infatti, la definizione del Sic si fondava sulla riconducibilità agli operatori attivi nei mercati rilevanti di una responsabilità di tipo editoriale rispetto alla produzione di un contenuto. Però più recentemente il Sic è stato integrato con gli introiti derivanti, per l'appunto, «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»[29]. L'assimilazione, sia pure sotto il solo profilo dei ricavi, degli Isp ai soggetti dotati di responsabilità editoriale sui contenuti (*content provider*) può essere considerato un segnale delle più evolute funzionalità dei *provider* nella gestione e nell'organizzazione dei contenuti informativi.

2. La giurisprudenza della Corte di giustizia dell'Unione europea: irresponsabilità dell'Isp neutrale e illegittimità degli obblighi di sorveglianza preventiva

Le sentenze che la Corte di giustizia dell'Unione europea ha emanato relativamente alla responsabilità civile degli Isp per gli illeciti commessi dagli utenti ha riguardato essenzialmente – anche se non esclusivamente –

[24] Pollicino (2014), cit.
[25] D. lgs. 31 luglio 2005, n. 177.
[26] Art. 2, comma 1, lett. *a* del Tusmar.
[27] Art. 2, comma 1, lett. *b* del Tusmar.
[28] Art. 2, comma 1, lett. *s* e art. 43 del Tusmar.
[29] Art. 3, comma 5-bis, della legge 16 luglio 2012, n. 103.

il campo del diritto d'autore[30]. Al di là della questione della protezione dei diritti di proprietà intellettuale e industriale che, per quanto assai importante, esula dal tema di cui qui si tratta, alcune sentenze risultano interessanti relativamente ai profili più direttamente connessi al regime della responsabilità degli intermediari digitali. In particolare, la Corte di Giustizia ha messo in evidenza principalmente due aspetti: quello dell'irresponsabilità del *provider*, a condizione che mantenga una posizione effettivamente neutrale rispetto ai comportamenti degli utenti, e quello dell'illegittimità di obblighi di sorveglianza preventiva in capo agli Isp. Entrambi gli aspetti si collegano non solo a quanto sancito dalla direttiva europea sul commercio elettronico ma anche, più in generale, alla tutela della libertà di informazione e al rispetto delle regole europee sul trattamento dei dati personali.

Fra le decisioni più rilevanti in tal senso si può ricordare quella del 2010 relativa alle cause riunite che hanno riguardato *Google France* in relazione al servizio a pagamento *AdWords*[31], attraverso cui gli operatori economici possono far apparire le proprie inserzioni pubblicitarie in forma di "links sponsorizzati" nel momento in cui gli internauti che effettuano ricerche mediante il motore di ricerca Google digitano parole-chiave coincidenti con quelle prescelte dall'inserzionista. Al di là delle questioni connesse con i diritti di utilizzazione del marchio comunitario, ciò che interessa di questa sentenza sono le riflessioni circa l'effettiva posizione di *Google*: il servizio *AdWords* comportava per *Google* un'attività di memorizzazione e trasporto di informazioni meramente tecnica, automatica e passiva, senza poter conoscere o controllare le informazioni memorizzate, in modo da poter applicare l'esenzione da responsabilità prevista dagli artt. 12 e 13 della direttiva *e-commerce*? La Corte ha attribuito al giudice nazionale la competenza a valutare l'effettiva neutralità del ruolo svolto da *Google* rilevando però che, per quanto *Google* tratti i dati inseriti dagli inserzionisti mediante i propri *software* e stabilisca le modalità di visualizzazione degli annunci pubblicitari, non necessariamente deve presumersi che essa conosca o controlli i dati inseriti dagli inserzionisti. Dunque, in quell'occasione la Corte di Giusti-

[30] Cocuccio (2015), cit., partic. pp. 1326-1329; Giovannella (2016), cit., partic. pp. 232-237; Pirruccio (2012), cit., pp. 2598-2599. E inoltre: L. Picotti (2012), *I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali*, in *Giurisprudenza di merito*, n. 12, partic. pp. 2544-2545; S. Scalzini (2012), *I servizi di online social network tra privacy, regole di utilizzo e violazione dei diritti dei terzi*, in *Giurisprudenza di merito*, n. 12, partic. pp. 2586-2587.

[31] Sentenza 23 marzo 2010, cause riunite C-236/08 (*Google France Sarl e Google Inc. c. Louis Vuitton Malletier Sa*), C-237/08 (*Google France Sarl c. Viaticum Sa e Luteciel Sarl*) e C-238/08 (*Google France Sarl c. Centre national de recherche en relations humaines (Cnrrh) Sarl e altri*).

zia è sembrata propendere per l'applicazione del regime di esenzione dalla responsabilità.

Anche il caso *L'Oreal Sa e altri c. eBay International Ag e altri*[32], di poco successivo, ha riguardato i diritti di utilizzo del marchio comunitario, nonché il problema dell'effettiva neutralità dell'Isp rispetto alle condotte degli utenti. Se, infatti, gli Stati membri non possono imporre ai *provider* un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite, essi possono però consentire che i titolari dei diritti di proprietà industriale chiedano e ottengano giudizialmente un provvedimento inibitorio contro un intermediario i cui servizi sono utilizzati da terzi per violare tali diritti. Nello specifico, il caso riguardava la commercializzazione attraverso un sito di vendite *online* (*eBay*) di prodotti cosmetici che la società *L'Oreal*, titolare dei diritti di proprietà industriale, non intendeva destinare alla commercializzazione. Trattandosi di prodotti offerti in vendita da soggetti privati attraverso i servizi offerti da *eBay*, occorreva accertare se *eBay*, in qualità di *hosting provider*, fosse civilmente responsabile delle condotte illecite dei suoi utenti ai sensi dell'art. 14 della direttiva *e-commerce*. Occorreva dunque accertare, ai fini dell'esenzione dalla responsabilità, se l'*hosting provider* giocasse ruolo davvero del neutrale rispetto alle condotte degli utenti e non fosse a conoscenza della loro illiceità. Per la Corte, la neutralità dell'Isp non può essere invocata se «il prestatore del servizio, anziché limitarsi ad una fornitura neutra di quest'ultimo, mediante un trattamento puramente tecnico e automatico dei dati forniti dai suoi clienti, svolge un ruolo attivo atto a conferirgli una conoscenza o un controllo di tali dati». Spetta al giudice nazionale accertare, nello specifico, la posizione di *eBay*, considerando però che il ruolo del fornitore di servizi si considera attivo «allorché presta un'assistenza che consiste in particolare nell'ottimizzare la presentazione delle offerte in vendita di cui trattasi o nel promuoverle».

In altre occasioni la giurisprudenza della Corte ha riguardato la questione dell'ammissibilità di obblighi di sorveglianza preventiva imposti agli intermediari digitali dalla autorità nazionali. Nella decisione sul caso *Scarlet Extended Sa c. Société belge des auteurs, compositeurs et éditeurs Scrl (Sabam)*[33] la Corte di Giustizia ha stabilito l'incompatibilità fra l'art. 15 della direttiva *e-commerce* e l'obbligo imposto dal giudice nazionale al *provider* di predisporre un sistema di filtraggio sistematico di tutte le comunicazioni che avvenivano tramite un sistema *peer-to-peer*, al fine di evi-

[32] Sentenza 12 luglio 2011, C-324/09.
[33] Sentenza 24 novembre 2011, C-70/10.

tare che gli utenti condividessero contenuti protetti dal diritto d'autore. La Corte ha evidenziato che un siffatto obbligo di sorveglianza preventiva, comportando costi altissimi a carico del fornitore dei servizi, non garantiva un giusto equilibrio fra l'esigenza di proteggere i diritti di proprietà intellettuale e la libertà di impresa dell'intermediario, oltre a comportare violazioni alla libertà di informazione degli utenti e alla protezione dei loro dati personali[34].

Mentre nel caso *Scarlet* la controversia coinvolgeva un *provider* di mero accesso, un successivo caso[35] ha visto la *Sabam* contrapposta al gestore di un *social network*, appartenente quindi alla categoria degli *hosting provider* (*Netlog*). Ma anche in questo caso, come nel precedente, la Corte ha statuito che «le autorità ed i giudici nazionali devono, in particolare, garantire un giusto equilibrio tra la tutela del diritto di proprietà intellettuale, di cui godono i titolari di diritti d'autore, e quella della libertà d'impresa». Ciò considerato, l'ingiunzione di predisporre un sistema di filtraggio dei contenuti caricati dagli utenti, essendo tale sistema complesso, costoso e permanente, causerebbe una grave violazione della libertà di impresa del prestatore di servizi di *hosting*, oltre a «ledere anche i diritti fondamentali degli utenti dei servizi di tale prestatore, ossia il loro diritto alla tutela dei dati personali e la loro libertà di ricevere o di comunicare informazioni». Infatti, il sistema «potrebbe non essere in grado di distinguere adeguatamente tra un contenuto illecito ed un contenuto lecito, sicché il suo impiego potrebbe produrre il risultato di bloccare comunicazioni aventi un contenuto lecito».

Infine, il più recente caso *Upc Telekabel c. Constantin e Wega*[36] non ha riguardato direttamente la responsabilità del *provider*, ma ha rilevanza in questo contesto poiché ha riguardato la possibilità per gli Stati membri dell'Unione europea di prevedere nel proprio ordinamento giuridico norme che consentano ai titolari dei diritti di proprietà intellettuale di chiedere alle competenti autorità nazionali provvedimenti inibitori nei confronti degli intermediari i cui servizi siano utilizzati da terzi per violare un diritto

[34] Rispetto a quest'ultimo profilo, la Corte ha evidenziato che gli indirizzi Ip sono stati personali e quindi coloro a cui tali dati si riferiscono devono essere adeguatamente informati delle modalità del loro trattamento. Su questa sentenza si veda il commento di M. Siano (2011), *La sentenza Scarlet della Corte di Giustizia: punti fermi e problemi aperti*, in F. Pizzetti (a cura di), *I diritti nella "rete" della rete. Il caso del diritto di autore*, Torino, Giappichelli, pp. 81-96.

[35] Sentenza 16 febbraio 2012, C-360-10, *Sabam c. Netlog*.

[36] Sentenza 27 marzo 2014, C-314-12, *Upc Telekabel Wien GmbH c. Constantin Film Verleih GmbH e Wega Filmproduktionsgesellschaft mbH*. Si veda il commento di E. Maggio (2016), *Il diritto d'autore. La responsabilità del fornitore di accesso a Internet*, in M. Bianca, A. Gambino e R. Messinetti (a cura di), *Libertà di manifestazione del pensiero e diritti fondamentali*, Milano, Giuffrè, pp. 159-167.

d'autore o diritti connessi. Si trattava, nello specifico, del caso due società di produzione cinematografica (*Constantin* e *Wega*) che avevano chiesto al giudice di ingiungere all'Isp *Telekabel* di bloccare un servizio che consentiva agli abbonati di fruire di film senza il consenso delle società titolari dei diritti di utilizzazione e economica. La Corte, ribadendo la necessità di garantire l'equilibrio fra i diversi diritti tutelati dal diritto dell'Unione europea (segnatamente, la libertà di impresa, la proprietà intellettuale e la libertà di informazione degli utenti di Internet), ha stabilito che «un soggetto che metta a disposizione del pubblico su un sito Internet materiali protetti senza l'accordo del titolare dei diritti […] utilizza i servizi del fornitore di accesso ad Internet dei soggetti che consultano tali materiali, il quale deve essere considerato un intermediario …». Per la Corte, il diritto dell'Unione europea non osta a che un giudice ingiunga a un fornitore di accesso ad Internet di impedire l'accesso ad un sito Internet che metta in rete materiali protetti senza il consenso dei titolari dei diritti. L'importante è che le misure adottate, anche se non idonee ad impedire con assoluta certezza le condotte illecite, siano ragionevoli, siano utili almeno a scoraggiare o a rendere più difficile la consultazione di materiali non autorizzati e soprattutto non privino gli utenti di Internet della possibilità di accedere ai contenuti disponibili lecitamente. Dunque, la Corte ha posto l'accento sulla necessità di garantire la proporzionalità, l'adeguatezza e la ragionevolezza delle misure eventualmente adottate.

3. La giurisprudenza italiana: la discussa categoria del c. d. "*hosting* attivo" che non beneficia dell'esenzione da responsabilità

Successivamente all'introduzione del d. lgs. n. 70/2003, in Italia la giurisprudenza di merito[37] ha privilegiato un approccio casistico, teso ad accertare l'effettivo ruolo svolto nelle diverse circostanze dagli intermediari digitali, in modo da escludere il beneficio della limitazione di responsabilità ogni qual volta è stato accertato che l'Isp abbia svolto un ruolo "attivo" in relazione ai comportamenti degli utenti, o fosse comunque a conoscenza della loro illiceità. Dalla prassi giurisprudenziale emerge la tendenza a valutare caso per caso le effettive responsabilità degli Isp, non solo in base ai criteri oggettivi fissati dal legislatore, ma anche in relazione alle circostanze

[37] Cocuccio (2015), cit., partic. pp. 1322-1326; Falletta (2015a), cit., partic. pp. 148-154; Giovannella (2016), cit., partic. pp. 237-242; Pirruccio (2012), cit., partic. pp. 2595-2611; Pollicino (2014), cit.; Tosi (2012), cit., partic. pp. 59 ss.); Tosi (2017), cit. E inoltre: P. Prandini (2016), *La responsabilità dei provider*, in M. Megale (a cura di), *ICT e diritto della società dell'informazione*, Torino, Giappichelli, pp. 263-285.

in cui si è verificato l'illecito, all'atteggiamento psicologico del prestatore del servizio e alla natura del rapporto fra quest'ultimo e l'utente[38]. Anche nella giurisprudenza italiana, come in quella della Corte di Giustizia dell'Unione europea, l'ambito delle violazioni al diritto d'autore è stato quello in cui principalmente ci si è esercitati nell'accertamento della responsabilità dei *provider*.

Fra le decisioni più significative, molte delle quali sono state emesse in sede di ricorso cautelare urgente *ex* art. 700 del Codice di procedura civile[39], si può ricordare l'ordinanza con cui il Tribunale di Roma nel 2009[40] ha inibito in via cautelare l'inserimento e la diffusione tramite la piattaforma *YouTube* di contenuti audiovisivi relativi alla trasmissione televisiva "Grande Fratello", di cui la *Rti* deteneva in esclusiva i diritti di utilizzazione economica. Sebbene *YouTube* rivendicasse la propria posizione di *hosting provider* neutrale e inconsapevole dell'illiceità dei contenuti caricati dagli utenti, il giudice ha ritenuto che la massiccia presenza di inserzioni pubblicitarie sulle pagine web in cui comparivano i video illecitamente inseriti, nonché le ripetute sollecitazioni da parte di *Rti* affinché il materiale illecito venisse rimosso, fossero elementi tale da dimostrare la posizione non neutrale del *provider* e la sua consapevolezza dell'illiceità dei contenuti audiovisivi in questione. In una successiva ordinanza del febbraio 2010[41], il medesimo tribunale, in considerazione del fatto che i video relativi alle puntate del "Grande Fratello" continuavano ad essere disponibili su *YouTube*, ha ribadito l'ordine inibitorio contro il quale *YouTube* aveva reclamato. Infatti, la condotta di *YouTube*, che aveva proseguito nella gestione dei contenuti video anche a fini pubblicitari, nonostante le ripetute diffide ed azioni giudiziarie iniziate da *Rti*, rendeva irragionevole sostenere la sua assoluta estraneità alla commissione dell'illecito. Pur senza pretendere dal *provider* un'attività preventiva di controllo e di accertamento degli contenuti caricati dagli utenti, il giudice non solo ha intimato all'intermediario digitale di rimuovere il materiale illecitamente trasmesso, avendo certamente avuto conoscenza di tale illiceità, ma ha anche sottolineato che, proprio in virtù della conoscenza inconfutabilmente acquisita, *YouTube* avrebbe dovuto provvedere a ciò spontaneamente, senza attendere l'ordine dell'autorità giudiziaria.

[38] Diotallevi (2012), cit., p. 2515.

[39] Codice di procedura civile, art. 700: «Fuori dei casi regolati nelle precedenti sezioni di questo capo, chi ha fondato motivo di temere che durante il tempo occorrente per far valere il suo diritto in via ordinaria, questo sia minacciato da un pregiudizio imminente e irreparabile, può chiedere con ricorso al giudice i provvedimenti d'urgenza, che appaiono, secondo le circostanze, più idonei ad assicurare provvisoriamente gli effetti della decisione sul merito».

[40] Tribunale di Roma, ordinanza 15-16 dicembre 2009, *Reti Televisive Italiane (Rti) s.p.a. c. Google Uk ltd. e YouTube Llc.*

[41] Tribunale di Roma, ordinanza 11 febbraio 2010.

Nel 2011 il Tribunale di Roma si è anche occupato della richiesta da parte di una società di produzione cinematografica (*Pfa Film*), titolare dei diritti di utilizzazione economica del film "About Elly", di inibire l'accesso ai *files* audiovisivi del film, che invece erano stati illecitamente resi disponibili tramite Internet e potevano essere raggiunti dagli utenti che interrogavano il motore di ricerca *Yahoo!*, gestito da *Google*[42]. Il Giudice ha ritenuto che, avendo la *Pfa Film* inviato ripetute diffide a *Yahoo!*, la posizione del motore di ricerca non potesse più essere considerata neutrale e *Yahoo!* non potesse rivendicare la non conoscenza dell'illiceità dei video come condizione di esclusione dalla responsabilità. Successivamente[43], in seguito a un reclamo presentato da *Yahoo!*, il giudice ha eccepito che «il titolare dei diritti che chiede all'intermediario della comunicazione, o al giudice di ordinare all'intermediario della comunicazione, di rimuovere un determinato contenuto o di renderlo inaccessibile, è tenuto a individuare puntualmente l'Url (*uniform resource locator*) del contenuto medesimo, non essendo sufficiente una denuncia generica circa la presenza in rete di alcuni contenuti illegittimi immessi da terzi non ben identificati […]». Dunque, l'acquisizione della conoscenza dell'illecito, in seguito alla quale il *provider* decade dal beneficio della limitazione della responsabilità, sorge solo in seguito a una diffida specifica e analitica, che indichi tutti gli Url riferiti ai contenuti illegittimi.

Nei due casi sopra commentati, la giurisprudenza ha elaborato la categoria dell'*hosting provider* "attivo", quello cioè che non può dirsi irresponsabile rispetto agli *user-generated/distributed content,* perché ha attivamente contribuito alla loro organizzazione e comunque non può non essere a conoscenza di eventuali elementi di illiceità in tali contenuti. Sulla stessa linea anche la decisione del Tribunale di Milano relativa alla controversia fra *Rti* e *Iol*, emessa nel giugno 2011[44]. Attraverso il portale *Iol*, che consentiva la condivisione di video fra utenti, venivano scambiati contenuti audiovisivi sui quali la *Rti* vantava diritti di utilizzazione economica e per questo la *Rti* chiedeva che a *Iol* fosse intimato di inibire l'accesso a tali contenuti. Il giudice milanese ha evidenziato il ruolo "attivo" di *Iol* poiché ai filmati risultavano associati molteplici messaggi pubblicitari sponsorizzati. Il portale *Iol* è stato dunque qualificato come «una diversa figura di prestatore di servizi, non completamente passivo e neutro rispetto all'organizzazione della gestione dei contenuti immessi dagli utenti (c.d. *hosting attivo*), organizza-

[42] Tribunale di Roma, ordinanza 22 marzo 2011, *Pfa Film s.r.l. c. Google Italia s.r.l. e Yahoo! Italia Inc.*

[43] Tribunale di Roma, ordinanza 11 luglio 2011.

[44] Tribunale di Milano, sentenza 7 giugno 2011, n. 7680, *Rti Italia spa c. Italia On Line srl (Iol).*

zione da cui trae anche sostengo finanziario in ragione dello sfruttamento pubblicitario connesso alla presentazione (organizzata) di tali contenuti. […] Nel caso di specie appare del tutto evidente la stretta connessione stabilita dal prestatore di servizi tra i contenuti immessi dagli utenti e la visualizzazione dei messaggi promozionali, posto che agli inserzionisti viene proposto un servizio che consente di visualizzare i messaggi pubblicitari in relazione agli specifici contenuti propri dei video immessi dagli utenti tramite l'utilizzazione di parole-chiave comuni». In aggiunta a ciò, il ruolo non neutrale di *Iol* emergeva anche dalle clausole contrattuali accettate dai suoi utenti: ad esempio, quella secondo cui l'utente cedeva a *Iol* il diritto e la licenza di «utilizzare, riprodurre, adattare, pubblicare, distribuire, riprodurre ed eseguire» video e fotografie caricati dagli utenti; oppure quella secondo cui *Iol* si impegnava nei confronti dei suoi utenti a «provvedere all'immediata rimozione di video o foto trasmessi dall'utente che risultassero in violazione di soggetti vantanti diritti sui contenuti trasmessi». Infine, alcuni servizi offerti da *Iol*, come ad esempio la visualizzazione automatica dei "video correlati" e la possibilità per gli utenti di segnalare contenuti eventualmente illeciti, contribuivano a qualificare Iol come un *hosting attivo*.

Argomentazioni simili sono state utilizzate dal Tribunale di Milano nella controversia fra *Rti* e *Yahoo!*[45]. Anche in questo caso, infatti, il giudice ha ritenuto che *Yahoo!* non potesse godere dell'esenzione da responsabilità, in quanto *hosting provider* attivo che traeva profitti dalle inserzioni pubblicitarie associate ai video caricati dagli utenti e contribuiva alla gestione di tali video in base alle clausole contrattuali accettate dagli utenti. In particolare, queste ultime attribuivano al *provider* il diritto di creare algoritmi dei video, modificarli o tradurli in appropriati format multimediali; il diritto di utilizzare, distribuire, riprodurre, modificare, re-mixare, adattare, estrarre, preparare opere derivate, riprodurre in pubblico e visualizzare pubblicamente i contenuti video su *Yahoo! Video*; il diritto di usare tali contenuti per attività pubblicitarie o per promozioni commerciali, e di visualizzare, rappresentare, riprodurre e distribuire i contenuti video su ogni formato media e attraverso qualsiasi canale media. Infine, ulteriore spia del ruolo non neutrale svolto dal *provider* era il servizio, visibile come *link* sotto ogni video pubblicato in rete, che consentiva al visitatore di segnalare al prestatore del servizio l'eventuale illiceità del contenuto immesso dall'utente.

Però, avendo *Yahoo! Italia* impugnato la sentenza, la Corte di appello di Milano si è pronunciata nel 2015, ribaltando completamente la decisione

[45] Tribunale di Milano, sentenza 9 settembre 2011, n. 10893, *Rti Italia spa c. Yahoo! Italia.*

del giudice di merito[46]. Il giudice di secondo grado ha infatti ritenuto che «le attuali tecnologie avanzate, in mancanza di altri elementi in grado di fare intravedere una vera e propria manipolazione dei dati immessi da parte dell'*hosting provider*, non siano da sole in grado di determinare il mutamento della natura del servizio di *hosting provider* di tipo passivo (secondo la classificazione utilizzata dalla giurisprudenza nazionale richiamata dalla sentenza appellata), in servizio di *hosting provider* di tipo attivo …». Dunque, nel caso di specie, a *Yahoo!* potevano ben applicarsi le previsioni di cui agli artt. 16 e 17 del d. lgs. n. 70/2003 sull'irresponsabilità del *provider*. Richiamando la giurisprudenza della Corte di Giustizia dell'Unione europea, e particolarmente il caso *L'Oreal c. eBay*[47], il giudice ha statuito che «non è certamente conforme all'interpretazione data dalla Corte di Giustizia individuare per l'*hosting provider* "evoluto" un regime di piena responsabilità per i dati immessi da terzi e non di limitazione della responsabilità …».

In conclusione, secondo la Corte d'Appello di Milano «deve ritenersi che, ragionando sulla base delle argomentazioni contenute nelle decisioni delle Corti europee, tutte nel senso sopra riferito, la nozione di *hosting provider* attivo risulti oggi sicuramente fuorviante e sicuramente da evitare concettualmente in quanto mal si addice ai servizi di "ospitalità in rete" in cui il prestatore non interviene in alcun modo sul contenuto caricato dagli utenti, limitandosi semmai a sfruttarne commercialmente la presenza sul sito, ove il contenuto viene mostrato così come è caricato dall'utente senza alcuna ulteriore elaborazione da parte del prestatore». Al *provider* non può essere richiesto alcun onere di sorveglianza preventiva, ma solo quello di segnalare alle competenti autorità e semmai di rimuovere i contenuti illeciti di cui sia venuto a conoscenza. Affinché il *provider* possa ottemperare al suo dovere di controllo e di rimozione *a posteriori*, è necessaria una richiesta (diffida) di rimozione dei contenuti illeciti proveniente dalla parte che assume essere titolare dei diritti. Tale diffida deve esser però specifica, e deve contenere l'indicazione esatta degli Url o dei *link* dei video da rimuovere. Il giudice ha dunque ritenuto che una diffida espressa in termini generici, attraverso la mera indicazione del titolo o del nome commerciale dell'opera considerata illecita, non fosse di per sé idonea a far insorgere in capo al *provider* una responsabilità di controllo e rimozione *a posteriori*. Secondo l'impostazione fatta propria dalla sentenza della Corte di Appello di Milano, le attività che il *provider* può svolgere rispetto agli *user-generated/distributed content*, via

[46] Corte di Appello di Milano, sentenza 7 gennaio 2015, n. 29. Cfr. L. Bugiolacchi (2015), *Ascesa e declino della figura del "provider attivo"? Riflessioni in tema di fondamento e limiti del regime privilegiato di responsabilità dell'hosting provider*, in *Responsabilità civile e previdenza*, n. 4, pp. 1261-1270.

[47] Sentenza 12 luglio 2011, C-324/09.

via più complesse in relazione all'evoluzione tecnologica, non sono in grado di modificare la qualificazione soggettiva dell'intermediario digitale, che deve essere considerato un *hosting provider* "puro" almeno fino a quando non interviene direttamente sui contenuti informativi caricati dagli utenti sulla piattaforma da lui gestita; in questo caso, però, il fornitore del servizio si trasforma in un *content provider*, come tale sottoposto alle comuni regole della responsabilità civile, e così la nozione di "*hosting* attivo" di creazione giurisprudenziale risulta superflua[48].

L'inesistenza di obblighi di sorveglianza preventiva in capo ai *provider* è stata sancita anche dal Tribunale di Roma nel caso *Calciolink*[49]. Nella fattispecie, la società *Rti Italia* del gruppo *Mediaset* aveva presentato un ricorso contro *Blogger* (una piattaforma di *Google*) sul quale era stata segnalata la presenza di un portale dedicato alla trasmissione in *streaming* di partite di calcio della Serie A, coperti dal *copyright Mediaset Premium*. Già prima della notifica, *Google* aveva già provveduto a rendere inaccessibili i contenuti illeciti e il sito *Calciolink* era stato oscurato. Tuttavia, la ricorrente pretendeva che il giudice ordinasse a *Google* di approntare un sistema di controllo atto ad impedire eventuali ulteriori diffusioni di contenuti illeciti. Il giudice, richiamando la giurisprudenza della Corte di Giustizia dell'Unione europea, ha ribadito che non si può imporre all'Isp di sorvegliare in tempo reale i contenuti che verranno immessi in futuro dagli utenti: si tratterebbe di un onere non esigibile per via della complessità tecnica e del costo di una simile attività, peraltro in contrasto con quanto sancito dalla direttiva europea sul commercio elettronico nonché con il diritto alla libera manifestazione del pensiero.

Per rimanere in ambito calcistico, può essere interessante accennare alla complessa vicenda di *Rojadirecta*, un portale spagnolo che – attraverso un'aggregazione di link a siti esterni dislocati in tutto il mondo – consentiva alla propria utenza di accedere gratuitamente a vari siti che trasmettevano in diretta partite di calcio e altri eventi sportivi. Nel 2010 il giudice spagnolo aveva ritenuto legittima l'attività di *Rojadirecta* poiché il servizio non poneva gli utenti in grado di decriptare i segnali televisivi delle emittenti titolari dei diritti audiovisivi sugli eventi sportivi trasmessi, ma si limitava ad aggregare una serie di *link* attraverso cui era possibile accedere a contenuti che in altre parti del mondo erano trasmessi lecitamente. Tuttavia nel 2011 la società *Mediaset*, titolare in esclusiva dei diritti di trasmissione di partite di calcio di serie A, otteneva dal Tribunale di Roma[50] un provve-

[48] Bugiolacchi (2015), cit., p. 1268.
[49] Tribunale di Roma, ordinanza 16 dicembre 2011, *Rti Italia spa c. Google Inc.*
[50] Tribunale di Roma, ordinanza 17 agosto 2011.

dimento cautelare inibitorio: il giudice ha ritenuto indubitabile la consapevolezza, da parte del resistente, dell'illiceità della sua condotta, non consistente in una mera attività di *linking*, ma finalizzata allo sfruttamento commerciale degli eventi trasmessi attraverso la vendita di spazi pubblicitari. La vicenda si è conclusa dinanzi al Tribunale di Milano il 13 gennaio 2016: il Tribunale ha disposto di disabilitare in modo assoluto l'accesso al sito (sia ai Dns sia agli indirizzi Ip associati).

Sulla controversia nozione di *hosting attivo*[51] può risultare interessante esaminare anche quanto deciso in diverse fasi dal Tribunale di Torino in merito alla controversia fra *Delta Tv* e *YouTube*. In prima battuta[52], il giudice ha rigettato la domanda cautelare di *Delta Tv* nei confronti *Google* e *YouTube*, finalizzata ad ottenere un'inibitoria urgente in relazione alla pubblicazione abusiva, su Y*ouTube*, di episodi di varie serie televisive di proprietà della ricorrente. In base alla considerazione che all'attività di *YouTube* potessero pienamente applicarsi le disposizioni del d. lgs. n. 70/2003 relative alla limitazione di responsabilità, secondo il giudice torinese *YouTube* sarebbe stata tenuta a rimuovere i contenuti solo a seguito di diffida specifica proveniente da *Delta Tv*, indicante singolarmente i vari Url. Però, con una successiva ordinanza collegiale del 23 giugno 2014, il Tribunale ha parzialmente riformato il provvedimento di prime cure, disponendo non solo l'obbligo per *Delta Tv* di rimuovere gli audiovisivi i cui Url erano stati indicati specificamente, ma anche «di impedire l'ulteriore caricamento sulla piattaforma *YouTube* dei medesimi materiali, impiegando a tal fine, a propria cura e spese, il *software Content Id*». Dunque, all'intermediario digitale è stato ordinato di utilizzare uno specifico *software* per attuare una forma di vigilanza preventiva; non si tratta però di una vigilanza *tout court*, ma di un controllo limitato ad evitare che un video già caricato e poi rimosso, in quanto lesivo del diritto d'autore, venga caricato nuovamente da altri utenti.

La sentenza di primo grado[53] ha condannato le parti convenute (*Google Inc*., *Youtube Llc* e *Google Ireland Holdings*) a ottemperare a quanto suindicato e a risarcire la parte attrice. Rileva, comunque, il fatto che il servizio di *videosharing* prestato da *YouTube* sia stato considerato dal giudice perfettamente assimilabile a quello di un *hosting provider* passivo. Infatti, il Tribunale ha ritenuto che «il punto di discrimine fra fornitore neutrale e fornitore non neutrale debba essere individuato nella manipolazione o trasformazione delle informazioni o dei contenuti trasmessi o memorizzati»; sebbene *YouTube* svolga attività di indicizzazione, organizzazione, e ge-

[51] Bugiolacchi (2015), cit.

[52] Tribunale di Torino, ordinanza 4 maggio 2014, *Delta Tv Programmes srl. c. YouTube Llc e Google Inc.*

[53] Tribunale di Torino, sentenza 7 aprile 2017, n. 1928.

stione dei video caricati da terzi, per il Tribunale torinese tali attività «non costituiscono affatto elaborazioni idonee a manipolare, alterare o comunque a incidere sui contenuti ospitati, trasmessi e visualizzati sulla piattaforma gestita dalle parti convenute. Esse sono tutte attività attinenti alla migliore utilizzazione, visualizzazione e sfruttamento commerciale dei contenuti, ma non certo elaborazioni che manipolano il contenuto del video condiviso fra più utenti. Il punto di discrimine è invero proprio questo: solo un intervento che modifichi il video caricato da terzi è idoneo a far venir meno l'esenzione di responsabilità […]».

La questione dell'esistenza o meno della categoria dell'*hosting provider attivo*, e quindi responsabile dei contenuti caricati dagli utenti, appare tuttora controversa e le soluzioni individuate dalla giurisprudenza di merito non conducono affatto in direzione univoca. Infatti, quanto deciso recentemente dal Tribunale di Roma[54], e interamente confermato in sede di appello[55], a proposito della controversia fra *Rti Italia* e la piattaforma americana *Break Media* contrasta decisamente con le due sentenze appena esaminate del Tribunale di Milano (casi *Rti c. Yahoo!* e *Delta Tvc. YouTube*). Nella fattispecie, *Rti Italia* lamentava una violazione dei propri diritti di sfruttamento economico di una serie di programmi televisivi pubblicati sul sito *Break.com* senza autorizzazione; la convenuta *Break Media* sosteneva invece che, essendo i contenuti caricati in piena autonomia dagli utenti, essa rivestiva il ruolo di *hosting provider* neutrale e quindi irresponsabile. Tuttavia il giudice romano, tanto in primo grado quanto in appello, ha ritenuto che *Break Media* fosse qualcosa di diverso dall'*hosting provider* "puro": una «moderna impresa globale»; un «aggregatore di contenuti» non «casualmente immessi dagli utenti, ma catalogati ed organizzati in specifiche categorie»; un modello di *business* che attribuisce ai contenuti «un ruolo determinante per il successo pubblicitario e di conseguenza economico» della piattaforma *Break.com*; un «sofisticato *content provider*» che seleziona i contenuti, dispone di un *team* editoriale, interviene direttamente su tali contenuti (per esempio, offendo agli utenti la possibilità di scegliere, all'interno di un programma, la parte che più interessa e di collegarla ai "video correlati"), prevede un meccanismo attraverso cui gli utenti possono segnalare i contenuti illegittimi. Tutto ciò considerato, risulta evidente l'inapplicabilità del regime di irresponsabilità previsto per gli Isp dall'art. 16 del d. lgs. n. 70/2003, «in armonia con la giurisprudenza ormai consolidata italiana e comunitaria che ha delineato il ruolo attivo dell'Isp» qualora si riscontri «un pur minimo contributo all'*editing* del materiale sulla rete

[54] Tribunale di Roma, sentenza 27 aprile 2016, n. 8437.
[55] Corte d'Appello di Roma, sentenza 29 aprile 2017, n. 2883.

lesivo di interessi tutelati». La responsabilità civile dell'Isp, con conseguente obbligazione risarcitoria, sorge in seguito alla conoscenza dell'illiceità dei contenuti conseguita «in qualsiasi modo»; nella fattispecie, trattandosi di programmi di successo e facilmente individuabili, è stata ritenuta sufficiente una diffida recante indicazione specifica della loro denominazione, non necessariamente anche i singoli Url.

Nello stesso periodo, sempre il Tribunale di Roma ha condannato la piattaforma digitale francese *Kewego* per l'uso illecito dei programmi televisivi *Mediaset*[56]. In questo caso, il Collegio giudicante ha ritenuto non decisiva, ai fini della decisione, accertare la qualificazione di *Kewego* come *host* attivo o passivo; ai fini dell'individuazione della responsabilità del *provider* appariva infatti sufficiente verificare se quest'ultimo fosse – o comunque potesse essere – a conoscenza dell'illiceità delle condotte dei suoi utenti. Per il tribunale romano, le diffide che *Kewego* aveva ricevuto da *Rti* erano dunque «idonee a consentire al destinatario di individuare con sufficiente puntualità i singoli contenuti multimediali che sarebbero stati illecitamente immessi sulla piattaforma della convenuta, avuto riguardo alla notorietà dei programmi in questione e alla agevole attività di reperimento di tali contenuti richiesta al *provider* a seguito della diffida». Questa decisione lascia supporre che l'irrisolta diatriba sul ruolo attivo o neutrale degli Isp possa considerarsi almeno in parte superata.

Dalla giurisprudenza fin qui esaminata emergono alcune perplessità circa la sussistenza della categoria degli *hosting provider* "attivi", non espressamente prevista dalla normativa in vigore. Quindi, accanto a sentenze che fondano la responsabilità del *provider* proprio su questa nozione, ve ne sono altre che ne prescindono completamente, soffermandosi piuttosto sull'elemento della "effettiva conoscenza" dell'illiceità dei contenuti da parte del gestore della piattaforma. Per concludere, è evidente che «in molti casi, infatti, l'attività degli Isp si avvicina effettivamente a quella editoriale. Tuttavia, dire che un *hosting* opera in modo "attivo", sottolineatura ricorrente in diverse pronunce delle corti nazionali e non solo, non significa ancora affermare con certezza che si tratti di un soggetto che esercita un'attività editoriale: il discrimine per considerare un'attività come rilevante ai fini del pluralismo rimane legato all'esistenza di un effettivo controllo sui contenuti»[57]. Questa eventuale trasformazione del ruolo dell'intermediario digitale va accertata caso per caso, valutando in che modo l'utilizzo di *software* e algoritmi gestionali da parte del *provider* produca effetti sui contenuti caricati dagli utenti tali da eccedere la sua presunta posizione di neutralità. Il fatto è che

[56] Tribunale di Roma, sentenza 5 maggio 2016, n. 24707, *Rti Italia c. Kit Digital France*.
[57] Pollicino (2014), cit., p.73.

ben raramente le piattaforme di aggregazione di contenuti (dai motori di ricerca alle reti sociali) sono pienamente trasparenti rispetto alle tecnologie utilizzate per la gestione dei contenuti stessi. Dunque, in assenza di un sufficiente grado di *technical disclosure*, il rischio è quello di una mancanza di uniformità dell'interpretazione giurisprudenziale. Sarebbe allora auspicabile una revisione della direttiva *e-commerce* alla luce dell'evoluzione tecnologica e delle nuove funzionalità degli intermediari digitali, in modo da aggiornare la disciplina della responsabilità[58].

[58] Bugiolacchi (2015), cit., pp. 1269-1270.

IL TRATTAMENTO DEI DATI PERSONALI DA PARTE DEGLI INTERMEDIARI DIGITALI: VINCOLI E RESPONSABILITÀ

1. L'impianto normativo

1.1 Dalla privacy *all'*habeas data

Il diritto alla *privacy*, che originariamente era visto come diritto dell'individuo borghese ad escludere gli altri dalla propria sfera privata (così nel saggio *The Right of Privacy* di Brandeis e Warren, 1890), ha assunto via via i connotati del diritto di ogni persona di mantenere il controllo sui dati che la riguardano, ovunque essi si trovino. Nella dimensione di Internet, l'accento è posto sul diritto di ognuno di mantenere il controllo – tenendoli nascosti o rivelandoli solo a destinatari selezionati – sui dati di carattere strettamente privato o, ancora, di ottenere la cancellazione dalla memoria digitale di informazioni ormai prive di qualsiasi valenza sociale. Questo passaggio dall'originario concetto di *privacy* a quello della protezione dei dati corrisponde anche a un mutamento profondo che, per via di Internet, si è avuto nella nostra rappresentazione sociale e nelle modalità di interferenza nella nostra sfera privata: ogni volta che compiamo un'azione attraverso la rete Internet – cosa che nella realtà odierna capita spessissimo, utilizzando uno dei numerosi dispositivi elettronici di cui non possiamo più fare a meno – lasciamo delle "tracce digitali" che possono essere trattate al fine di ricostruire la nostra personalità e identità[1]. Dobbiamo essere consapevoli, quindi, di vivere in una società in cui la nostra identità e la nostra rappresentazione sociale sono sempre più caratterizzate dalla dimensione "virtuale", e dipendono sempre meno da quella "fisica".

[1] S. Rodotà (2014), *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, Laterza, pp. 27-32. Sull'identità digitale che si forma attraverso i *social network* si veda anche S. Landini (2017), *Identità digitale tra tutela della persona e proprietà intellettuale*, in *Rivista di diritto industriale*, n. 4-5, pp. 180-200.

Si può allora parlare di *habeas data*[2], un diritto tutelato anche da alcune Costituzioni, soprattutto dei Paesi latino-americani[3], che costituisce il moderno sviluppo dell'*habeas corpus*, dal quale si è storicamente sviluppato il diritto alla libertà personale. *L'habeas data* a che fare con la smaterializzazione e la parcellizzazione della nostra identità in Internet, che può essere ricostituita solo attraverso la riaggregazione delle tracce che ciascuno di noi lascia in Rete, e che corrispondono a frammenti della nostra personalità. Di conseguenza, il diritto alla protezione dei dati personali si smarca dall'ambito del diritto alla riservatezza, protetto dall'art. 8 della *Convezione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, e acquista dignità di diritto autonomo. Non a caso, la *Carta dei diritti fondamentali dell'Unione europea*, che oggi ha acquisito efficacia giuridica pari a quella dei trattati istitutivi dell'Ue[4], dedica due articoli distinti al rispetto della vita privata e familiare (art. 7) e alla protezione dei dati di carattere personale (art. 8). Quest'ultimo diritto è sancito anche nell'art. 16 del vigente Trattato sul funzionamento dell'Unione europea (Tfue), che attribuisce alle Istituzioni dell'Unione uno specifico potere legislativo in materia di protezione delle persone fisiche con riguardo al trattamento di dati di carattere personale.

Il diritto individuale che oggi, nell'era di Internet, deve essere riconosciuto e tutelato è quindi quello di poter mantenere il controllo di questi frammenti, di consentire consapevolmente che altri ne facciano un uso conforme alla nostra volontà, di opporci ai trattamenti indesiderati, di poter cancellare le tracce digitali che riteniamo non ci rappresentino più correttamente o che semplicemente desideriamo mantenere nascoste a tutti o ad alcuni, di avere la garanzia che dalla riaggregazione dei frammenti non emerga una rappresentazione falsa o distorta della nostra identità o della nostra personalità. Infatti, grazie ai moderni algoritmi di ricerca, sempre più raffinati e performanti, «piccoli dettagli insignificanti della nostra vita *online* si uniscono, costruendo profili omnicomprensivi 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

[2] G. Scotti (2015), *Dall'habeas corpus all'habeas data: il diritto all'oblio e il diritto all'anonimato nella loro dimensione costituzionale*, in *Diritto.it*, 7 settembre 2015, pp. 1-28; S. Russo e A. Sciuto (2011), *Habeas data e informatica*, Milano, Giuffrè.

[3] L. E. Rozo Acuña (2002), *Habeas data costituzionale: nuova garanzia giurisdizionale del diritto pubblico latinoamericano*, in *Diritto pubblico comparato ed europeo*, n. 4, pp. 1921-1945; L. E. Rozo Acuña (2006), *Le garanzie costituzionali nel diritto pubblico dell'America Latina*, Torino, Giappichelli.

[4] *Ex* art. 6 del vigente *Trattato sull'Unione europea.*

di ricerca …»[5]. Tuttavia, gli stessi algoritmi di ricerca ritenuti responsabili di violazioni della *privacy* degli utenti di Internet potrebbero oggi essere utilizzati, proprio grazie alla loro estrema sofisticazione, anche per prevenire lesioni del diritto alla riservatezza, aiutando nel contempo titolari e responsabili del trattamento a mantenere aggiornati ed esatti i dati personali dei soggetti interessati[6].

Dunque, il termine *privacy* ha oggi acquisito una molteplicità di significati e vi è connesso un insieme di poteri che, prendendo le mosse dall'antico nucleo del diritto ad essere lasciati in pace (*the right to be left alone*), si sono diffusi nella società per consentire ai singoli il controllo sulle modalità di trattamento dei propri dati nei confronti di soggetti sia pubblici che privati che a tali dati hanno accesso[7]. In tale ottica, il diritto alla riservatezza assume una connotazione pluralistica: non un singolo diritto, ma un insieme di diritti, tutti riconducibili all'unità e all'integrità della persona umana, fra cui spiccano il diritto all'identità personale come rappresentazione veritiera della propria personalità, il diritto alla riservatezza del proprio domicilio, della propria corrispondenza, delle proprie comunicazioni in generale, il diritto alla protezione e al controllo dei propri dati personali, ovunque essi siano archiviati, ovvero il pieno controllo del proprio "corpo elettronico". La questione assume un importanza ancora maggiore in considerazione della progressiva e rapida diffusione dell'*Internet of Things*[8]: è evidente che un utilizzo massiccio ed inconsapevole di *smart objects* in grado di interagire fra loro in Rete e raccogliere informazioni e dati relativi al loro fruitore può condurre alla circolazione di informazioni di natura sensibile e influire sull'autodeterminazione dei soggetti coinvolti.

1.2. Il fondamento costituzionale del diritto alla riservatezza

Sebbene in Italia il dibattito dottrinale sulla tutela della riservatezza sia sorto già anteriormente all'entrata in vigore della Costituzione del 1948, nella Carta costituzionale non è stato inserito un articolo che vi si riferisca

[5] S. Leucci (2017), *Diritto all'oblio, verità, design tecnologico: una prospettiva di ricerca*, in *MediaLaws. Rivista di diritto dei media*, n. 1, p. 118.

[6] Ivi, p. 122.

[7] Sul fenomeno della c. d. *datification* – cioè il costante aumento della produzione di dati e la sempre crescente capacità di analizzarli tramite algoritmi, producendo nuova conoscenza – nonché sugli attori pubblici e privati che esercitano un potere su tali dati o traggono vantaggio dalla loro elaborazione si veda S. Calzolaio (2017b), *Protezione dei dati personali*, in *Digesto delle discipline pubblicistiche. Aggiornamento*, Torino, Utet, partic. pp. 594-603.

[8] Sul tema si veda E. C. Pallone (2016), "*Internet of Things" e l'importanza del diritto alla privacy tra opportunità e rischi*, in *Ciberspazio e diritto*, n. 1-2, pp. 163-183.

esplicitamente. Tuttavia, il diritto alla riservatezza è previsto dall'art. 8 della *Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali* del 1950 (Cedu)[9], cui la giurisprudenza costituzionale[10] ha attribuito il duplice ruolo di parametro interposto per vagliare la legittimità costituzionale delle norme interne e di criterio per l'interpretazione costituzionalmente orientata delle disposizioni interne, per il tramite dell'art. 117 Cost., comma 1. Analogo diritto è previsto dall'art. 19 della *Dichiarazione universale dei diritti dell'uomo* del 1948[11] e soprattutto dagli artt. 7[12] e 8[13] della *Carta dei diritti fondamentali dell'Unione europea*, che ha lo stesso valore giuridico dei Trattati[14] e, pertanto, efficacia superiore rispetto a norme di diritto interno eventualmente contrastanti. In ogni caso, fin dal 1975 la Corte di Cassazione[15] ha individuato in alcuni articoli della Costituzione

[9] Art. 8 Cedu: «1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute e della morale, o alla protezione dei diritti e delle libertà altrui».

[10] Corte costituzionale, sentenze 22 ottobre 2007, nn. 348 e 349.

[11] *Dichiarazione universale dei diritti dell'uomo*, art. 19: «Ogni individuo ha il diritto alla libertà di opinione e di espressione, incluso il diritto di non essere molestato per la propria opinione e quello di cercare, ricevere e diffondere informazioni e idee attraverso ogni mezzo e senza riguardo a frontiere».

[12] *Carta dei diritti fondamentali dell'Unione europea*, art. 7, *Rispetto della vita privata e della vita familiare*: «Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni».

[13] *Carta dei diritti fondamentali dell'Unione europea*, art. 8, *Protezione dei dati di carattere personale*: «1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. 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 persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

[14] Art. 6, comma 1, del Trattato istitutivo dell'Unione europea.

[15] Corte di Cassazione, sentenza 27 maggio 1975, n. 2129. Estratto dalla sentenza: «Con l'espressione "diritto alla riservatezza" – una delle prime e più usate formulazioni del fenomeno, che non può essere più abbandonata – sono indicate diverse ipotesi, che implicano un problema, non solo formale, ma anche di sostanza. Esse possono sintetizzarsi almeno in tre aspetti. Da una parte si tende a restringere rigorosamente l'ambito di questo diritto al riserbo della "intimità domestica", collegandola al concetto ed alla tutela del domicilio. A questa concezione corrisponde forse il "*the righe to be alone*" degli anglosassoni. All'opposto, vi sono formulazioni molto generiche – il "riserbo della vita privata" da qualsiasi ingerenza, o la c.d. "privatezza" (*privacy*) – cui corrisponderebbe un sostanziale ambito troppo vasto o indeterminato della sfera tutelabile. Una concezione intermedia, che riporta in limiti ragionevoli la portata di questo diritto, può identificarsi nelle formule che fanno riferimento ad una certa sfera della vita individuale e familiare, alla illesa intimità personale in certe mani-

italiana (in *primis* l'art. 2 Cost., interpretato come norma a fattispecie aperta[16], ma anche gli artt. 3, 27, 29 e 41) quali norme da cui ricavare i principi

festazioni della vita di relazione, a tutte quelle vicende, cioè, il cui carattere intimo è dato dal fatto che esse si svolgono in un domicilio ideale, non materialmente legato ai tradizionali rifugi della persona umana (le mura domestiche o la corrispondenza). Ora, questa Corte ritiene, ai fini della ricerca del fondamento normativo dei diritto soggettivo alla riservatezza, che – superate le vie finora seguite, e cioè quelle della *analogia iuris* o dei ricorso ai principi generali dell'ordinamento – sia possibile rinvenire una diretta tutela di tale interesse non soltanto riguardato nella prima ristretta accezione, ma anche per l'ambito indicato dalla terza concezione. […] Una tutela dei diritto alla riservatezza più ampia di quella circoscritta all'intimità domestica, non solo non contrasta con i principi costituzionali, ma trova in essi vari motivi di convalida. Questa Corte aveva ravvisato nell'art. 2 Cost. l'unico fondamento del diritto assoluto di personalità, che risulta violato dalla divulgazione di notizie della vita privata. Alla critica, secondo cui l'art. 2 enuncia solo in via generale la tutelabilità di diritti inviolabili, che trovano il loro riconoscimento effettivo in altre specifiche norme, deve precisarsi che questa Corte – deducendo dal citato articolo il "diritto *erga omnes* alla libertà di autodeterminazione" – intendeva porre l'accento – più che sul riferimento ai diritti inviolabili – sull'espressione della norma che riconosce all'uomo il rispetto della sua personalità, come singolo e nelle formazioni sociali ove tale personalità si svolge. Un duplice spunto di convalida al diritto di riservatezza si trae anche dall'art. 3 Cost. sia perché, riconoscendosi la dignità sociale del cittadino, si rende necessaria una sfera di autonomia che garantisca tale dignità, sia in quanto rientrano nei limiti di fatto della libertà ed eguaglianza dei cittadini anche quelle menomazioni cagionate dalle indebite ingerenze altrui nella sfera di autonomia di ogni persona. E, sotto questo profilo, va ricordata anche la inviolabilità della libertà personale (art. 13), intesa questa in un senso più ampio della libertà meramente fisica. Già si è notata la rilevanza che sul problema della riservatezza ha l'art. 14 della Costituzione, che riguarda, oltre la inviolabilità del domicilio, anche i limiti alle ispezioni, alle perquisizioni, agli accertamenti per motivi pubblici. Nella stessa linea si pone il successivo art. 15, relativo all'inviolabilità della libertà e della segretezza della corrispondenza. Anche dalla presunzione di innocenza dell'imputato sino alla condanna definitiva (art. 27 Cost.) dovrebbero trarsi dei conseguenti limiti alla diffusione di notizie – inutili e talvolta dannose alle esigenze di giustizia – sulle vicende dell'imputato e sui cd. "retroscena" dei delitti. Uno sviluppo dell'art. 2 è costituito dalla norma dell'art. 29, che riconosce il carattere originario e l'inviolabile autonomia della famiglia. Uno spunto, infine, si trae dal secondo comma dell'art. 41 Cost. laddove l'iniziativa economica trova un limite nel rispetto della libertà e della dignità umana».

[16] A. Barbera (1975), *Art. 2*, in *Commentario della Costituzione italiana*, a cura di G. Branca, Bologna, Zanichelli, partic. pp. 80-92; S. Mangiameli (2006), *Il contributo dell'esperienza costituzionale italiana alla dommatica europea della tutela dei diritti fondamentali*, in *Consulta Online,* pp. 1-56. *Contra* invece A. Pace (2001), *Metodi interpretativi e costituzionalismo*, in *Quaderni costituzionali*, n. 1, pp. 35-61, secondo cui la tutela della persona umana nella sua dimensione psico-fisica, con riferimento alle nuove tecnologie, non può essere realizzata mediante forzature interpretative del dettato costituzionale oppure applicando le norme costituzionali a fattispecie strutturalmente incompatibili con la disciplina da esse prevista. Anche per P. Barile (1984), *Diritti dell'uomo e libertà fondamentali*, Bologna, Il Mulino, l'interpretazione estensiva dell'art. 2 Cost. non è convincente (si vedano in particolare le pp. 54-56). *Idem* secondo P. Caretti e G. Tarli Barbieri (2017), *I diritti fondamentali*, Torino, Giappichelli (partic. pp. 179 ss.). Invece per F. Modugno (1995), *I "nuovi*

di «tutela della sfera privata del soggetto con conseguenti limitazioni ad altre garanzie costituzionali quali, per esempio, il diritto all'informazione». Il Giudice delle leggi ha chiarito, dunque, come l'esigenza di proteggere la sfera privata dei singoli individui costituisca un limite, fondato su norme costituzionali, alla libertà di manifestazione del pensiero e quindi alla divulgazione di notizie che a tale sfera privata attengano, soprattutto nel caso manchi o sia irrilevante l'interesse pubblico nei loro riguardi[17].

1.3. La normativa sul trattamento dei dati personali e la "esenzione domestica"

In relazione al tema centrale di questo studio, cioè la responsabilità degli intermediari digitali e specificamente dei gestori dei *social network*, va ribadito che le disposizioni della direttiva 2000/31/Ce sul commercio elettronico – comprese quelle relative alle limitazioni di responsabilità – non si applicano alle questioni relative alla protezione dei dati personali (*considerando* n. 14 e art. 1, comma 4, lett. *b*). La medesima eccezione è stata riprodotta nel d. lgs. n. 70/2003 (art. 1, comma 2, lett. *b*). Dunque, il regime speciale di responsabilità previsto per gli Isp dalla direttiva sul commercio elettronico non si estende anche all'attività di trattamento delle informazioni personali. Questa materia infatti è regolata dalle direttive europee specificamente approvate in quest'ambito (direttiva 95/46/Ce e successive modificazioni[18]) e, per quanto riguarda l'Italia, dalla normativa di attuazione di tali direttive[19], che nel

diritti" nella giurisprudenza costituzionale, Torino, Giappichelli, p. 2 ss., la questione interpretativa dell'art. 2 Cost. è inutile o scarsamente rilevante, perché eventuali nuovi diritti possono comunque essere considerati implicitamente ricompresi in quelli esplicitati dalla Carta costituzionale oppure strumentali ad essi.

[17] Sull'evoluzione della normativa e della giurisprudenza sulla tutela della *privacy* si vedano: F. Di Ciommo (2003), *Diritti della personalità, tra media tradizionali e avvento di Internet*, in G. Comandè (a cura di), *Persona e tutele giuridiche*, Torino, Giappichelli, pp. 3-47; D. Granara (2015), *Il fronte avanzato del diritto alla riservatezza*, in *Rivista Italiana di Diritto Pubblico Comunitario*, n. 3-4, pp. 897-915; S. Scagliarini (2017), *In tema di privacy: virtù e vizi della cultura giuridica*, in *Ars Interpretandi*, n. 1, pp. 49-66.

[18] Direttiva 95/46/Ce, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati; direttiva 97/66/Ce sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni; direttiva 2002/58/Ce relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, in parte modificata dalla successiva direttiva 2009/136/Ce.

[19] Legge 31 dicembre 1996, n. 675, e successive modificazioni (fra cui, in particolare, quella avvenuta con d. lgs. n. 171/1998), il d. lgs n. 69/2012.

2003 è stata raccolta nel *Codice in materia di protezione dei dati personali*[20], più volte in seguito aggiornato.

La disposizioni della direttiva n. 95/46/Ce non si applicano, però, ai trattamenti di dati personali effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico (la cosiddetta *household exemption* o "esenzione domestica" di cui all'art. 3, comma 2 della direttiva). Nel *considerando* n. 12 sono indicate, a titolo esemplificativo, due attività che possono rientrare nella *household exemption*, ovvero la corrispondenza e la compilazione di elenchi di indirizzi. Questa eccezione, dunque, è stata pensata al fine di non obbligare le singole persone fisiche che trattano dati di amici e conoscenti a sottostare agli adempimenti richiesti dalla direttiva, considerati troppo gravosi per coloro che trattano dati personali solo in ambito ristretto. Nella normativa italiana di attuazione (d. lgs. n. 196/2003, art. 5, comma 3), l'esenzione è stata resa opportunamente meno ampia, poiché viene presa in considerazione la possibilità che anche dati raccolti a fini personali possano poi essere comunicati ad altri o diffusi: quindi, il trattamento di dati personali, anche se effettuato da persone fisiche per fini esclusivamente personali, è soggetto all'applicazione del *Codice della privacy* se i dati sono destinati ad una comunicazione sistematica o alla diffusione; si applicano in ogni caso le disposizioni in tema di responsabilità e di sicurezza dei dati previsti dal Codice agli articoli 1[21] e 31[22].

L'esenzione domestica pone qualche problema in relazione ai *social network*, come ben evidenziato dall'*Article 29 Working Party* nel 2009[23]. Infatti, tutte le volte in cui l'attività degli utenti dei *social network* si estende oltre il piano strettamente personale – si pensi al caso di un'associazione che si serve di una piattaforma di *social networking* con finalità politiche, commerciali, benefiche ecc. – l'utente assume il ruolo di responsabile del trattamento dei dati, che comunica tali dati al *social network provider*, che diviene anch'esso responsabile del trattamento, e ad altri utenti, i quali potrebbero potenzialmente trasformarsi anch'essi in responsabili del trattamento. Quando ciò

[20] D. lgs. 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali*, che ha dato attuazione alla direttiva 2002/58/Ce. Il Codice negli anni successivi è stato vari volte modificato e aggiornato (ad esempio, con d. lgs. n. 69/2012 e con d. lgs. n. 151/2015).

[21] «Chiunque ha diritto alla protezione dei dati personali che lo riguardano».

[22] «I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta».

[23] Article 29 Data Protection Working Party, *Opinion 5/2009 on online social networking*, 12 giugno 2009 (01189/09/EN - WP 163).

avviene, tutti i soggetti responsabili del trattamento sono tenuti a rispettare tutte le regole che la direttiva prevede sulla protezione, sicurezza e conservazione dei dati, sugli obblighi di informativa e sul consenso del titolare dei dati. La difficoltà, però, consiste nell'individuare con chiarezza quali comportamenti degli utenti esattamente possano beneficiare della *household exemption* e quali invece no. Se la valutazione dell'applicabilità dell'esenzione domestica resta ancorata unicamente a dati quantitativi (il numero di contatti dell'utente), si rischia una certa arbitrarietà nel giudizio, essendo del tutto soggettiva, in assenza di parametri certi, la nozione di "molti contatti"[24]. Per non dire della «impossibilità di misurare i contatti di "secondo grado", nel senso che nulla esclude che un numero limitato di contatti possa rivelarsi comunque un veicolo di diffusione estremamente efficace, allorché uno dei pochi contatti abbia, a sua volta, un gran numero di collegamenti all'interno del *network*, con il che un dato "domestico" per chi lo immette diviene un dato "di dominio pubblico" per chi si limita all'attività di condivisione»[25].

1.4. Il nuovo regolamento europeo sulla protezione dei dati personali

A breve, però, l'impianto normativo fin qui descritto verrà interamente sostituito dal regolamento (Ue) n. 2016/679, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, applicabile a decorrere dal 25 maggio 2015 in tutta l'Unione europea, che abrogherà la direttiva n. 95/46/Ce, sostituendosi alle discipline nazionali[26].

L'esigenza di approvare un regolamento in luogo delle precedenti direttive è stata avvertita al fine di assicurare che le norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche, con riguardo al tratta-

[24] P. Passaglia (2016), *Privacy e nuove tecnologie, un rapporto difficile. Il caso emblematico dei social media tra regole generali e ricerca di una specificità*, in *Consulta Online*, n. 3, p. 337.

[25] Ivi, p. 338.

[26] M. Bassini (2016), *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in *Quaderni costituzionali*, n. 3, pp. 587-590; S. Calzolaio (2017a), *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in *Federalismi.it*, n. 24, pp. 1-21; S. Calzolaio (2017b), *Protezione dei dati personali*, in *Digesto delle discipline pubblicistiche. Aggiornamento*, Torino, Utet, partic. pp. 625 ss.; E. Pelino, L. Bolognini e C. Bistolfi (2016), *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Giuffrè; F. Pizzetti (2016), *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Torino, Giappichelli; M. G. Stanzione (2016), *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Europa e diritto privato*, n. 4, pp. 1249-1264.

mento dei dati personali, vengano applicate in modo uniforme, coerente e omogeneo in tutta l'Unione europea, eliminando le difformità nelle legislazioni nazionali, percepite come ostacoli alla circolazione dei dati personali all'interno dell'Unione e fonte di rischio e di incertezza. Il presupposto su cui si fonda l'impianto normativo è quello dell'intrinseca rischiosità dell'immissione di dati personali *online*: non solo, infatti, è praticamente impossibile inibire la circolazione di un dato personale una volta immesso in Internet, ma lo è anche evitare che esso venga incrociato con altre informazioni (personali e non), con modalità di trattamento e per finalità diverse da quelle previste originariamente. Per questo, l'accento viene posto sulla necessità di una valutazione sistematica, da parte del titolare/responsabile del trattamento, dei rischi attuali e potenziali del trattamento, operando così una ponderazione del presunto livello di rischiosità.

Pur se il regolamento risponde all'esigenza di strutturare uno *jus commune europeo*, tuttavia non incide sul *quantum* di normativizzazione, non sovvertendo la tendenza a lasciare ampi spazi all'autodisciplina, attraverso frequenti rinvii a codici di condotta[27]. Questa evidentemente è la risposta alla fluidità del contesto normativo relativo alla protezione dei dati personali, caratterizzato da un'intrinseca provvisorietà determinata dalla costante e rapida evoluzione tecnologica e dalla sempre più inestricabile commistione fra diversi livelli di regolamentazione, nazionali e sovranazionali.

La nuova disciplina si applicherà a tutti i trattamenti di dati personali effettuati da un titolare stabilito nel territorio dell'Unione europea, nonché da tutti i soggetti (titolari o responsabili) stabiliti fuori dall'Unione europea nel caso in cui il trattamento abbia ad oggetto i dati personali di coloro che si trovano nell'Unione europea oppure inerisca all'offerta di beni o servizi nel territorio dell'Unione oppure al monitoraggio di comportamenti di soggetti all'interno dell'Unione (art. 3 del regolamento). Quindi, i prestatori di servizi della società dell'informazione vi verranno assoggettati indipendentemente dal luogo di stabilimento, a differenza di quanto accade con la normativa attuale[28], che è applicabile solo ai soggetti stabiliti nell'Unione europea o che, qualora siano stabiliti al di fuori del territorio dell'Unione, utilizzino strumenti situati nel territorio dell'Unione. Dunque il "principio di origine" (art. 4, comma 1, lett. *c* della direttiva europea) verrà sostituito da un "principio di destinazione", o meglio "di prossimità", poiché al trattamento dei dati personali sarà applicabile la legge dello Stato membro nel quale sono residenti (o si trovano fisicamente) le persone alle quali sono

[27] Passaglia (2016), cit., p. 335.
[28] Art. 4 della direttiva 95/46/Ce e art. 5 del d. lgs. n. 196/2003.

dirette le offerte commerciali,o nei confronti delle quali sono effettuate azioni di *data tracking*, *data profiling* o *data mining*[29].

Si ricorda che, ai sensi dell'art. 4 comma 7 del nuovo regolamento europeo, il "titolare" del trattamento dei dati è «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali». Tale definizione, dunque, è applicabile a qualsiasi tipo di *provider*, compresi i gestori dei *social network*, purché possa essere dimostrata la sua attitudine a determinare finalità e mezzi del trattamento. Ai senti dell'art. 4 comma 8, è invece "responsabile" del trattamento «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento». La distinzione fra "titolare" e "responsabile" del trattamento dei dati non è presente nella disciplina attuale: la direttiva europea parla solo di *data controller*, tradotto in Italiano come "responsabile" del trattamento. Invece, il nuovo regolamento introduce una differenza fra il soggetto che determina le modalità e i mezzi del trattamento (il titolare) e quello che effettua il trattamento per conto del titolare (il responsabile). Questa distinzione può avere rilevanza nel caso del *provider* che affida ad un altro soggetto la responsabilità del trattamento dei dati (si pensi, ad esempio al rapporto fra la società "madre" *Google* e la controllata *YouTube*, oppure fra *Facebook* e le controllate *Instagram* e *WhatsApp*). Ma – e questo è l'aspetto più interessante – può servire ad inquadrare meglio anche il ruolo dei gestori dei *social network*. Infatti, anche qualora si dubitasse della qualificazione del *social network provider* come "titolare" del trattamento dei dati (in quanto in realtà è l'utente, e non il gestore della piattaforma, a determinare finalità e mezzi del trattamento), si può comunque applicare ad esso la qualifica di "responsabile" (in quanto tratta i dati personali in base al consenso prestato dagli utenti e alle modalità e finalità da essi definite).

Sia il titolare che il responsabile del trattamento possono essere soggetti ad obbligazioni risarcitorie per trattamento illecito dei dati personali. Infatti, secondo l'art. 82 del regolamento, «chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento», a meno che il titolare non dimostri che l'evento dannoso non è in alcun modo a lui imputabile, oppure il responsabile non dimostri che ha agito rispettando le istruzioni ricevute dal titolare.

[29] P. Piroddi (2015), *Profili internazional-privatistici della responsabilità del gestore di un motore di ricerca per il trattamento dei dati personali*, in G. Resta e V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE Press, p. 94.

Inoltre, gli Stati membri potranno infliggere sanzioni amministrative pecuniarie, purché proporzionate e dissuasive, nonché sanzioni di altro tipo – dunque anche penali – per violazioni diverse da quelle indicate nell'art. 82 (artt. 83-84 del regolamento). Nelle more dell'entrata in vigore del regolamento si continua ad applicare in Italia la disciplina vigente in materia di obbligazioni risarcitorie e sanzioni: i danni – non solo patrimoniali, ma anche non patrimoniali – causati per effetto del trattamento dei dati personali devono essere risarciti ai sensi dell'art. 2050 del Codice civile[30]; a talune fattispecie di comportamenti scorretti vengono applicate sanzioni amministrative pecuniarie[31], mentre altre violazioni più gravi sono considerate reati penali, puniti anche con pene detentive[32]. In particolare, l'art. 167 del *Codice della privacy* qualifica come reato l'illecito trattamento di dati personali e sensibili ai fini di trarne profitto per sé o per altri o di recare danno ad altri.

Il nuovo regolamento specifica con maggiore chiarezza l'ambito di applicazione dell'eccezione domestica, riprodotta nell'art. 2, comma 1, lett. *c*. Nel *Considerando* n. 18 è spiegato che il regolamento «non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale. Le attività a ca-

[30] Art. 15 comma 1 del d. lgs. n. 196/2003. Su questa disposizione taluni fondano l'equiparazione, in via interpretativa, fra il trattamento dei dati personali e le attività pericolose, arrivando alla conclusione che civilmente responsabili per Il trattamento dei dati personali effettuato senza le dovute cautele sarebbero non solo gli utenti di Internet che trattano i dati, ma anche l'intermediario digitale. Si veda sul punto G. Miceli (2017), *Profili evolutivi della responsabilità in Rete: il ruolo degli* Internet Service Provider *tra prevenzione e repressione*, in *MediaLaws. Rivista di diritto dei media*, n. 1, pp. 106-115. Il regolamento (Ue) n. 2016/679 non contiene, ovviamente, un esplicito riferimento al trattamento dei dati personali come attività pericolosa. Tuttavia, l'art. 24 comma 1 sembra alludervi, nel momento in cui dispone che «tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento». L'onere probatorio a carico del titolare del trattamento dei dati risulterebbe alleggerito, ai sensi del comma 3 del medesimo articolo, qualora quest'ultimo dimostrasse l'adesione a codici di condotta o meccanismi di certificazione. Qualcosa del genere è suggerita anche da Miceli (2017), cit., che, in prospettiva *de jure condendo*, auspica l'adesione spontanea degli Isp a un modello organizzativo mutuato dal "modello di organizzazione, gestione e controllo" di cui al d. lgs. n. 231/2001 sulla responsabilità amministrativa degli enti. Secondo l'Autore, l'adesione a un simile modello renderebbe più semplice per l'Isp la dimostrazione di aver adottato tutte le misure idonee ad evitare il danno, come indicato dall'art. 2050 c. c.

[31] Artt. 161-166 del d. lgs. n. 196/2003.

[32] Artt. 167-172 del d. lgs. n. 196/2003.

rattere personale o domestico potrebbero comprendere[33] la corrispondenza e gli indirizzari, o l'uso dei *social network* e attività *online* intraprese nel quadro di tali attività. Tuttavia, il presente regolamento si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico». In altre parole, la *household exemption* è applicabile alle sole persone fisiche utenti dei servizi (quindi anche utenti dei *social network*) a condizione che il trattamento dei dati non avvenga nell'ambito di attività professionali o commerciali; invece al fornitore del servizio (quindi al *provider*, compreso il *social network provider*) l'eccezione non si può applicare in alcun caso, proprio per il fatto che l'attività del *provider* è sempre di tipo professionale[34]. In questo modo, non appena il regolamento sarà applicabile, verrà sgombrato il campo dall'ambiguità che caratterizza la disciplina attualmente vigente, che obbliga ad una verifica caso per caso dell'effettivo ruolo degli Isp nel trattamento dei dati. Parimenti, sempre nell'ottica di evitare equivoci, è specificato nell'art. 2 comma 4 che il nuovo regolamento non pregiudica l'applicazione delle norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della direttiva 2000/31/Ce.

1.5. L'applicazione della normativa sulla protezione dei dati personali ai social network sites

Ciò considerato, occorre verificare in che modo la responsabilità per il trattamento dei dati personali degli utenti sia condivisa fra gli utenti stessi e

[33] Passaglia (2016), cit., p. 337, rileva come l'uso del condizionale con riferimento ai *social network* sia emblematico della rinuncia da parte del regolamento a disciplinare compiutamente e analiticamente un settore in crescente espansione come quello dei *social network*. A p. 339 l'Autore scrive: «l'estensione ai *social media* della normativa generale può apparire, per così dire, "rassicurante", nella misura in cui permette agli operatori di orientare le proprie condotte su schemi già consolidati. Il punto è che, per un verso, gli schemi non sempre appaiono così consolidati e, per l'altro, l'idea di trattare i *social media* come il resto della rete assume talvolta (ed in specie proprio per quel che concerne il trattamento dei dati) i contorni di una forzatura».

[34] Per Passaglia (2016), cit., p. 341, il fatto che la *household exemption* possa essere rivendicata, se non dai gestori delle piattaforme di *social networking*, almeno dalle persone fisiche (utenti) che condividono contenuti *user-generated*, suggerisce che «la sensazione che sia agevole eludere le norme di protezione non può essere meramente epidermica: si pensi, ad esempio, al fatto che un contenuto ben può diventare "virale" semplicemente attraverso una catena di condivisioni fatte da soggetti che possono tutti appellarsi alla *household exemption*, con il che l'ipotetica violazione, anche grave, della *privacy* risulta essere il prodotto di una serie di azioni poste in essere di per sé in maniera legittima».

gli intermediari digitali, con specifico riferimento ai gestori di *social network*.

Poiché le piattaforme di *social networking* si basano sul fatto che gli utenti si identificano e si caratterizzano mediante la costruzione di una pagina personale, il fulcro della loro attività consiste nella raccolta di dati personali[35] e spesso anche di dati sensibili[36]. Le pratiche di condivisione messe in atto dagli utenti dei *social network* comportano inevitabilmente la circolazione di questi dati all'interno della rete dei contatti – una rete estremamente ampia, che comprende non solo le persone con cui ciascun utente ha un rapporto diretto, ma anche tutti coloro con cui i legami sono solo indiretti (gli "amici egli amici") – con modalità tali per cui è praticamente impossibile per l'interessato mantenerne il controllo. Le clausole normalmente contenute nelle "licenze d'uso", accettando le quali è possibile accedere al *social network*, si basano per lo più sul principio dell'autotutela, affidando all'utente la responsabilità di decidere in che modo gestire i propri dati e con quali o quanti utenti condividerli[37]. Non infrequentemente – ma occorrerebbe un'osservazione caso per caso – le licenze d'uso sono impostate in base al principio dell'*opt-out*, in base al quale le informazioni che ogni

[35] Ai sensi dell'art. 4, comma 1, lett. *b* del d. lgs. n. 196/2003, si considera dato personali «qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale». Qualora questi dati personali permettano l'identificazione dell'interessato, sono detti "dati identificativi" (dell'art. 4, comma 1, lett. *c*). Secondo il nuovo regolamento europeo (art. 4), è dato personale «qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo *online* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

[36] Ai sensi dell'art. 4, comma 1, lett. *d* del d. lgs. n. 196/2003, sono dati sensibili «i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale».

[37] Sui *Terms of Service* (condizioni di servizio) dei *social network* si vedano: S. Scalzini (2012), *I servizi di online social network tra privacy, regole di utilizzo e violazione dei diritti dei terzi*, in *Giurisprudenza di merito*, n. 12, partic. pp. 2572-2578; S. Sica e G. Giannone Codiglione (2012), *Social network sites e il "labirinto" delle responsabilità*, in *Giurisprudenza di merito*, n. 12, partic. pp. 2721-2722. Per riflessioni di carattere generale sulla questione della protezione dei dati personali in Internet, oltre a Rodotà (2014), cit., partic. pp. 27-45, si vedano anche: F. Di Ciommo (2003), *Diritti della personalità, tra media tradizionali e avvento di Internet*, in G. Comandè (a cura di), *Persona e tutele giuridiche*, Torino, Giappichelli, pp. 3-47; G. Pascuzzi e F. Giovannella (2016), *Dal diritto alla riservatezza alla computer privacy*, in G. Pascuzzi (a cura di), *Il diritto nell'era digitale*, Bologna, Il Mulino, pp. 43-75.

utente carica sulle pagine del proprio profilo personale sono accessibili a tutti gli altri utenti del *social network*, a meno che non sia lo stesso titolare del profilo a prescegliere impostazioni sulla *privacy* più rigide, selezionando in modo più o meno restrittivo coloro con i quali intendere condividere tali informazioni. In questo modo, i gestori dei *social network* declinano ogni responsabilità legata alla diffusione dei dati personali degli utenti nonché a qualsiasi altro contenuto che gli utenti immettono sulla piattaforma. Tutto ciò riversa sull'utente l'onere di una continua e attenta vigilanza sulle modalità con cui le informazioni che lo riguardano possono circolare in rete.

Il nuovo regolamento europeo rovescia questa impostazione, sostituendo al principio dell'*opt-out* quello dell'*opt-in*, che richiede che la protezione dei dati personali sia assicurata al massimo livello dal gestore della piattaforma informatica per impostazione predefinita (*privacy by default*), a meno che non sia l'utente stesso a scegliere una tutela meno rigida; inoltre, in ogni fase del trattamento dei dati i *provider* – in qualità di titolari del trattamento – devono adottare ogni misura tecnica e organizzativa atta a garantire il massimo livello di protezione dei dati, minimizzando i rischi inevitabilmente connessi al trattamento stesso (*privacy by design*). Infatti, il consenso dell'interessato deve essere prestato in modo inequivocabile (art. 7) e il trattamento dei dati "sensibili"[38] è vietato, a meno che l'interessato non vi abbia prestato consenso esplicito (art. 9). Il regolamento disciplina in modo molto dettagliato gli obblighi di informativa e comunicazioni all'interessato che gravano sul titolare del trattamento (artt. 12-14), i diritti dell'interessato di accesso, rettifica, cancellazione, limitazione di trattamento e portabilità dei dati (artt. 15-20), il diritto di opposizione ai trattamenti automatizzati (artt. 21-22). L'onere di dimostrare che il trattamento dei dati è avvenuto in modo corretto grava sul titolare del trattamento, secondo l'art. 24, rubricato «Responsabilità del titolare del trattamento»; precisamente, secondo il comma 1, «tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato con-

[38] Segnatamente, i «dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona» (art. 9, comma 1, del nuovo regolamento).

formemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario»[39].

1.6. La tutela dell'identità personale nel caso dei falsi account

Secondo la normativa dell'Unione europea[40], la definizione di "dato personale" corrisponde a «qualsiasi informazione riguardante una persona fisica, identificata o identificabile». Più precisamente, «si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo *online* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale». All'interno di questa categoria possono essere ricomprese anche le informazioni personali che vengono diffuse *online* all'insaputa della persona interessata, attraverso falsi profili *social* riferibili appunto a tale persona. L'interessato, dunque, dovrebbe essere protetto dalla circolazione non autorizzata di informazioni personali, vere o false che siano, anche nell'ipotesi in cui tale informazioni siano riferibili ad un'identità "virtuale" diversa da quella reale.

Non si tratta di un'ipotesi remota. Un caso concreto di questo tipo, riguardante un falso profilo *Facebook*, è stato portato recentemente all'attenzione del Garante per la protezione dei dati personali[41]. Il caso ri-

[39] A proposito della responsabilità del titolare del trattamento, va segnalato il *Considerando* n. 74: «È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche». Però, tenendo presente il fatto che il regolamento consente al titolare del trattamento di affidare la responsabilità ad uno o più responsabili del trattamento, il *Considerando* n. 79 precisa: «La protezione dei diritti e delle libertà degli interessati così come la responsabilità generale dei titolari del trattamento e dei responsabili del trattamento, anche in relazione al monitoraggio e alle misure delle autorità di controllo, esigono una chiara ripartizione delle responsabilità ai sensi del presente regolamento, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento o quando l'operazione di trattamento viene eseguita per conto del titolare del trattamento».

[40] Direttiva n. 95/46/Ce, art. 2 (a); regolamento (Ue) n. 679/2016, art. 4 (1).

[41] Provvedimento n. 56 dell'11 febbraio 2016, doc. web n. 4833448. Si veda in proposito il commento di C. Martani (2016), *Tra tutela dell'identità personale e tutela dell'account nella decisione n. 56 dell'11 febbraio 2016 del Garante per la protezione dei dati personali*, in *Ciberspazio e diritto*, n. 1-2, pp. 141-162.

guardava il titolare di un *account* su *Facebook*, divenuto vittima di tentativi di estorsione da parte di un individuo che, venuto fraudolentemente in possesso di dati personali, fotografie e elenco dei contatti *social* della persona da ricattare, aveva creato un falso profilo *Facebook* che simulava l'identità di quest'ultima, inviando a tutti i suoi contatti contenuti audiovisivi artefatti con tecniche di manipolazione dell'immagine, che risultavano gravemente lesivi della dignità personale e della reputazione dell'interessato.

Dal punto di vista pratico, l'operazione non è difficile da realizzare, a condizione di conoscere qualche informazione personale relativa al soggetto la cui identità si vuole simulare. Infatti, sebbene *Facebook* dichiari nella propria *policy* di non consentire la creazione di falsi *account*, in realtà nessun controllo viene effettuato circa la reale identità della persona che chiede l'iscrizione al *social network* e all'effettiva riconducibilità a quest'ultima dei dati personali forniti all'atto dell'iscrizione (nome, cognome, data di nascita, sesso, indirizzo e-mail, numero di telefono, *password*). *Facebook* richiede ai propri utenti l'esibizione di un documento di identità solo nel caso in cui la persona sia già titolare di un *account*, ma per qualche ragione non riesca più ad accedervi: solo *ex post*, dunque, viene verificata la corrispondenza fra la reale identità dell'utente e quella dichiarata al momento della registrazione. Per contrastare l'apertura di falsi *account* è stato allestito una procedura *online* di segnalazione dei *fakes* da parte degli utenti del *social network*, ma è unicamente il *provider* a valutare l'attendibilità di tali segnalazioni e a decidere se disattivare o meno l'*account*, senza prevedere alcuna informativa per il soggetto che ha operato la segnalazione.

Si tratta di un *vulnus* intollerabile nella tutela di cui dovrebbero godere gli utenti dei *social network*, considerando che, come si è visto nelle pagine precedenti, il diritto alla protezione dei dati personali deve essere inteso come diritto all'autodeterminazione informativa, cioè alla possibilità di determinare le modalità di diffusione e utilizzazione dei propri dati personali, anche se caratterizzati da un contenuto informativo minimo, affinché la rappresentazione dell'identità personale sia veritiera o comunque corrispondente alla volontà della persona fisica cui essa si riferisce.

Nel caso di specie, la persona danneggiata dalla diffusione dei contenuti attraverso il falso *account* aveva chiesto al *provider* la rimozione del falso profilo e la aveva ottenuta; tuttavia, non aveva ottenuto l'accesso ai dati personali (informazioni e fotografie) detenuti in relazione ai profili *Facebook* aperti a suo nome, né informazioni circa l'origine di tali dati, le finalità, le modalità e la logica del loro trattamento, gli estremi identificativi del titolare e del responsabile del trattamento, nonché i soggetti o le categorie di soggetti cui i dati erano stati comunicati o che potevano venirne a conoscenza. Inoltre, il ricorrente aveva constatato che, pur essendo stato can-

cellato il falso *account*, una serie di informazioni riguardanti le conversazioni avute la persona che lo aveva attivato non erano state del tutto cancellate, ma rimanevano archiviate nei *server* di *Facebook*, pur risultando indisponibili per gli utenti.

Tutto ciò considerato, il Garante ha ordinato a *Facebook*: «a) di comunicare in forma intelligibile al ricorrente tutti i dati che lo riguardano detenuti in relazione ai profili *Facebook* aperti a suo nome, nonché di fornire all'interessato informazioni circa l'origine dei dati, le finalità, le modalità e la logica del trattamento, gli estremi identificativi del titolare e del responsabile, nonché i soggetti o le categorie di soggetti cui i dati sono stati comunicati o che possono venirne a conoscenza, entro e non oltre trenta giorni dalla ricezione della presente decisione; b) di non effettuare, con effetto immediato dalla data di ricezione del presente provvedimento, alcun ulteriore trattamento dei dati riferiti all'interessato, inseriti nel *social network* dal falso *account*, con conservazione di quelli finora trattati ai fini della eventuale acquisizione da parte dell'autorità giudiziaria».

La decisione evidenza come, fra tutela dell'*account* inteso come sua inviolabilità e tutela dell'identità personale, il Garante abbia opportunamente privilegiato quest'ultima.

1.7. La profilazione degli utenti

Un altro aspetto relativo alla protezione dei dati personali degli utenti dei *social network* inerisce alle pratiche commerciali di profilazione[42], che sempre più spesso gli intermediari digitali attuano per varie finalità: offerta di servizi sempre più mirati e conformati sulle specifiche esigenze dell'utente; fornitura di pubblicità personalizzata, più efficace – ma anche più pervasiva – rispetto all'*advertising* generico; sfruttamento commerciale dei profili ottenuti, che possono avere un significativo valore di mercato in ragione della loro capacità di fornire indicazioni sulle propensioni al consumo di beni e servizi. Un esempio evidente di queste pratiche è costituito dai "mi piace" di *Facebook*, attraverso i quali il gestore della piattaforma, utilizzando apposito algoritmi, è in grado di profilare attitudini, gusti, preferenze, interessi di ciascun utente: inutile sottolineare come molto spesso queste pratiche comportino il trattamento non solo di dati personali, ma an-

[42] Per approfondimenti sulla profilazione degli utenti: R. De Meo (2013), *Autodeterminazione e consenso nella profilazione dei dati personali*, in *Diritto dell'informazione e dell'informatica*, n. 3, pp. 587-608; E. C. Pallone (2015), *La profilazione degli individui connessi a Internet: privacy online e valore economico dei dati personali*, in *Ciberspazio e diritto*, n. 2, pp. 295-327.

che sensibili, per il fatto che attraverso i *likes* è possibile ricostruire molti aspetti della personalità individuale.

Giustamente è stato notato che «la tendenza delle nuove tecnologie è proprio quella di essere accessibile per il più ampio numero di persone possibili a prescindere dalla loro cultura, e ciò è possibile da una parte con una estrema semplificazione dei dispositivi elettronici, e dall'altra con un offuscamento, dietro ad un'accattivante interfaccia grafica, di ciò che succede (a livello di processi delle attività) durante il loro utilizzo. Da qui possiamo dire che sia l'incoscienza circa la possibilità di registrare e immagazzinare i dati sia la superficialità riservata al valore dei dati personali portano l'utente del *web* a fornire direttamente, o attraverso i propri comportamenti, moltissimi dati di carattere personale. In contrapposizione a questa inconsapevolezza o superficialità dell'utente, c'è invece una lucidissima consapevolezza delle aziende, sia appartenenti al settore dell'*information technology* che a settori diversi, di quanto al giorno d'oggi le informazioni e i dati personali costituiscano preziose merci di scambio, e tanto più tali informazioni possano riguardare aspetti intimi della persona, tanto più appaiono remunerative per chi le utilizza e le fa circolare. […] In cambio dei contenuti a cui possiamo accedere, *click* dopo *click*, vengono conservati e messi in relazione tra loro dati riferibili ad un determinato soggetto che possono rivelare le più sottili sfumature della sua personalità ma soprattutto mirano a cercare di comprendere cosa spinge all'azione l'utente o ancor di più qual è stato il processo mentale che lo ha portato a compiere quell'azione»[43]. Quindi, «le informazioni che rilasciamo in rete consapevolmente o meno costituiscono delle vere e proprie merci di scambio: dati personali in cambio di servizi. E se seguiamo un orientamento per cui riteniamo che i dati personali altro non sono che una manifestazione dell'identità della persona e della sua immagine, allora sembra che in realtà è l'individuo stesso a divenire la merce in cambio dei servizi ai quali accede in rete»[44].

Il d. lgs. n. 196/2003 non fa esplicito riferimento alla profilazione ma, in relazione all'obbligo di notifica dei trattamenti al Garante, parla di «dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti» (all'art. 37, comma 1, lett. *d*). Questo tipo di trattamento non è vietato, ma l'art. 14 stabilisce che l'interessato deve avere la possibilità di opporvisi e che comunque «nessun atto o provvedimento giu-

[43] Pallone (2015), cit., p. 296.
[44] Ivi, p. 305.

diziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato».

Peraltro, anche l'art. 15, comma 1, della direttiva 95/46/Ce stabilisce che «gli Stati membri riconoscono a qualsiasi persona il diritto di non essere sottoposta ad una decisione che produca effetti giuridici o abbia effetti significativi nei suoi confronti fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità, quali il rendimento professionale, il credito, l'affidabilità, il comportamento, ecc.».

Visto che l'utente ha il diritto di essere informato sulle modalità e sulle finalità del trattamento dei propri dati (articoli 7, 23, 24 e 122 del *Codice in materia di protezione dei dati personali*), anche per la profilazione è necessario che l'utente esprima preventivamente, liberamente e inequivocabilmente il proprio consenso, dopo essere stato debitamente informato delle caratteristiche, modalità e finalità della profilazione[45]. Se la profilazione, come spesso accade, avviene mediante l'utilizzo di *cookies*[46], l'utente deve riceverne un'informativa (in forma semplificata) e deve poter esprimere il proprio consenso al trattamento, conformemente all'art. 122 del *Codice in materia di protezione dei dati personali* e dell'art. 5, comma 3, della direttiva n. 2002/58/Ce, modificato dalla direttiva n. 2009/136/Ce[47]. Il punto debole di questo impianto risiede nel fatto che spesso, qualora l'utente non presti il consenso all'utilizzo dei *cookie* di profilazione, può essere escluso dalla possibilità di accedere a talune funzionalità offerte dal sito Internet.

[45] Garante per la protezione dei dati personali, *Linee guida in materia di trattamento di dati personali per profilazione on line*, provv. n. 161 del 19 marzo 2015, pubbl. in Gazzetta Ufficiale n. 103 del 6 maggio 2015.

[46] I *cookie* sono stringhe di testo di piccole dimensioni che i siti visitati dall'utente inviano al suo terminale (solitamente al *browser*), dove vengono memorizzati per essere poi ritrasmessi agli stessi siti alla successiva visita del medesimo utente. In particolare, i *cookie* di profilazione sono volti a creare profili relativi all'utente e vengono utilizzati al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dallo stesso nell'ambito della navigazione in rete. Il *Codice in materia di protezione dei dati personali* (d. lgs. n. 196/2003) si riferisce ai *cookie* nell'art. 122, comma 1: «l'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato informato con le modalità semplificate di cui all'articolo 13, comma 3». La necessità che gli utenti esprimano il consenso all'utilizzo dei *coockie* è stata evidenziata dal *Data Protection Working Party*, istituito ai sensi dell'art. 29 della direttiva 95/46/Ce, nel *Working Document 02/2013 providing guidance on obtaining consent for cookies*, 2 ottobre 2013 (1676/13/EN - WP 208).

[47] Si veda Garante per la protezione dei dati personali, *Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie*, provv. n. 229 dell'8 maggio 2014.

Il nuovo regolamento europeo dedica molta attenzione alle problematiche relative alla profilazione degli utenti. L'art. 4 definisce la profilazione come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica». Il trattamento, per essere considerato profilazione, deve riguardare, dunque, dati personali relativi a persone fisiche, e deve avvenire in modo automatizzato. Il titolare del trattamento dei dati deve fornire all'interessato l'informativa relativa alla profilazione, che deve comprendere anche notizie sulla logica utilizzata, sull'importanza e sulle conseguenze di tale trattamento (art. 13, comma 2, lett. *f;* art. 14, comma 2, lett. *g*). L'interessato ha diritto di accedere a queste informazioni (art. 15, comma 1, lett. *h*), di opporsi al trattamento in qualsiasi momento, soprattutto se la profilazione ha finalità di *marketing* diretto (art. 21), a non essere soggetto a decisioni che si basano automaticamente sul trattamento automatizzato dei suoi dati (art. 22). Inoltre il titolare del trattamento dei dati è tenuto ad effettuare una valutazione di impatto delle pratiche di profilazione degli utenti (art 35, comma 2).

In questo modo, il regolamento mira a promuovere la consapevolezza dell'utente circa le modalità e le finalità delle pratiche di profilazione. Tuttavia, se il consenso alla profilazione continuerà ad essere una condizione necessaria imposta dall'intermediario digitale per poter usufruire di alcuni servizi via Internet, l'espressione del consenso alla profilazione continuerà ad essere una pratica routinaria di scarso significato. Una scelta più decisa, che però il regolamento non ha compiuto, sarebbe stata quella di imporre ai gestori delle piattaforme la prestazione dei medesimi servizi tanto agli utenti che acconsento alla profilazione quanto a quelli che non vi acconsentono. Inoltre, il regolamento non risolve il problema dell'aggregazione delle informazioni derivante da diverse attività di profilazione condotte da diverse piattaforme: l'utente, infatti, acconsente alla profilazione in relazione a singoli servizi e singoli siti Internet, ma non ha la possibilità di controllare quale rappresentazione "immateriale" della propria identità emerge nel momento in cui i dati che lo riguardano vengono trattati in forma aggregata da soggetti terzi (es. motori di ricerca).

1.8. Il diritto all'oblio

Il nuovo regolamento europeo fa anche esplicito riferimento al cosiddetto "diritto all'oblio" o, più precisamente, al diritto di chiedere e ottenere la

cancellazione dei propri dati personali. In realtà, in senso più ampio l'espressione "diritto all'oblio" si riferisce al diritto individuale a non vedere continuamente riproposte dai mezzi di comunicazione notizie riferite alla propria persona che, per via del trascorrere del tempo, hanno perso i caratteri dell'interesse pubblico e dell'utilità sociale[48]. In questo senso – e cioè nella logica di bilanciare il diritto individuale a fornire un'immagine di sé il più possibile compatibile con la propria auto-percezione e il diritto della collettività di conoscere fatti di interesse pubblico – si è espressa anche la Corte di Cassazione nel 2015[49], con una sentenza che qualcuno ha definito "potenzialmente esplosiva" perché presuppone che chiunque gestisca un

[48] Sul diritto all'oblio si vedano: M. C. D'Arienzo (2015), *I nuovi scenari della tutela della privacy nell'era della digitalizzazione alla luce delle recenti pronunce sul diritto all'oblio*, in *Federalismi.it,* n. 2, pp. 1-31; F. Di Ciommo (2014), *Quello che il diritto non dice. Internet e oblio*, in *Danno e responsabilità*, n. 12, pp. 1101-1113; G. Finocchiaro (2015), *Il diritto all'oblio nel quadro dei diritti della personalità*, in G. Resta e V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE Press, pp. 29-42; T. E. Frosini (2014a), *Google e il diritto all'oblio preso sul serio*, in *Il diritto dell'informazione e dell'informatica*, n. 4-5, p. 563-567; T. E. Frosini (2014b), *Internet come ordinamento giuridico*, in M. Nisticò e P. Passaglia (a cura di), *Internet e Costituzione*, Torino, Giappichelli, pp. 57-69; M. Iaselli (2017a), *Come esercitare il diritto all'oblio in Internet*, Roma, Dike; G. Marchetti (2013), *Diritto di cronaca* on-line *e tutela del diritto all'oblio*, in Aa. Vv., *Da Internet ai Social Network. Il diritto di ricevere e comunicare informazioni e idee*, Rimini, Maggioli, pp. 71-90; M. Mezzanotte (2009), *Il diritto all'oblio*, Napoli, Esi; S. Pietropaoli (2017), *La rete non dimentica. Una riflessione sul diritto all'oblio*, in *Ars intrepretandi*, n. 1, pp. 67-80; F. Pizzetti (2013) (a cura di), *Il caso del diritto all'oblio*, Torino, Giappichelli; G. Resta e V. Zeno-Zencovich (2015) (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, TrE-Press; F. Sassano (2015), *Il diritto all'oblio tra Internet e mass media*, Vicalvi (FR), Key; G. Scotti (2015), *Dall'habeas corpus all'habeas data: il diritto all'oblio e il diritto all'anonimato nella loro dimensione costituzionale*, in *Diritto.it*, pp. 1-28; A. Sirotti Gaudenzi (2017), *Diritto all'oblio: responsabilità e risarcimento del danno*, Rimini, Maggioli; E. Stradella (2016), *Cancellazione e oblio: come la rimozione del passato, in bilico tra tutela dell'identità personale e protezione dei dati, si impone anche nella Rete, quali anticorpi si possono sviluppare e, infine,* cui prodest*?*, In *Rivista Aic*, n. 4, pp. 1-29.

[49] Corte di Cassazione, III sezione civile, sentenza 5 aprile 2012, n. 5525: «il diritto all'oblio salvaguarda in realtà la proiezione sociale dell'identità personale, l'esigenza del soggetto di essere tutelato dalla divulgazione di informazioni (potenzialmente) lesive in ragione della perdita (stante il lasso di tempo intercorso dall'accadimento del fatto che costituisce l'oggetto) di attualità delle stesse, sicché il relativo trattamento viene a risultare non più giustificato ed anzi suscettibile di ostacolare il soggetto nell'esplicazione e nel godimento della propria personalità. […] emerge allora la necessità, a salvaguardia dell'attuale identità sociale del soggetto cui la stessa afferisce, di garantire al medesimo la contestualizzazione e l'aggiornamento della notizia già di cronaca che lo riguarda, e cioè il collegamento della notizia ad altre informazioni successivamente pubblicate concernenti l'evoluzione della vicenda, che possano completare o financo radicalmente mutare il quadro evincentesi dalla notizia originaria, *a fortiori* se trattasi di fatti oggetto di vicenda giudiziaria, che costituisce anzi emblematico e paradigmatico esempio al riguardo».

archivio *online* sia tenuto ad implementare un sistema di aggiornamento costante di tutti i suoi contenuti per non incorrere in responsabilità civile (risarcimento del danno ingiusto) e talvolta anche penale (illecito trattamento dei dati personali)[50].

A differenza del diritto alla riservatezza, il diritto all'oblio non è rivolto a cancellare il passato, ma a proteggere il presente[51]. Va infatti precisato che il diritto all'oblio ha per oggetto avvenimenti che, nel momento del loro accadimento, non rientravano nella sfera della *privacy*, ma erano caratterizzati dall'interesse pubblico alla loro conoscenza. Dunque, in questa prospettiva il diritto all'oblio non è una mera espressione del diritto alla riservatezza, ma ne costituisce piuttosto un corollario, un riflesso[52]. Esso si pone comunque «in funzione protettiva della sfera intima dell'individuo, i cui dati memorizzati nei motori di ricerca e nelle reti sociali richiedono un affinamento ed un adeguamento delle garanzie, tale da assicurarne la protezione ed il monitoraggio e con la possibilità di ottenerne la rimozione decorso un certo lasso di tempo dalla pubblicazione ed essendo nel frattempo venuti meno i presupposti ed i requisiti di liceità del trattamento»[53].

Ma esiste davvero un diritto individuale soggettivo a che l'identità personale rappresentata *online* sia rappresentata nel suo dinamico divenire e risulti sempre aggiornata? Non tutti, in realtà, condividono questa idea dell'identità personale, «quasi che essa non si costruisca attraverso il passato, ma si cristallizzi in un presente che dalla memoria rifugge, nel timore che da questa giungano ricordi sgraditi di eventi che mai si vorrebbero vedere ripetuti»[54]. Anche perché, muovendo da un tale presupposto, il diritto all'oblio verrebbe a congiurarsi come un "diritto al pentimento", un diritto a rinnegare il proprio passato[55].

Secondo l'art. 17 del regolamento europeo, rubricato come "diritto all'oblio", «l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali», purché però sussistano alcune condizioni: dati divenuti non più necessari rispetto alle finalità per le quali erano stati raccolti o trattati; dati trattati illecitamente; revoca del consenso o opposizione al trattamento da parte dell'interessato; obbligo giuridico di cancellazione derivante dal diritto dell'Unione europea o di uno Stato membro; dati rela-

[50] Di Ciommo (2014), cit., pp. 1101 ss. Si veda anche Stradella (2016), cit., pp. 5 ss.
[51] Pizzetti (2013), cit., p. 30.
[52] Pietropaoli (2017), cit., p. 70.
[53] D'Arienzo (2015), cit., p. 17.
[54] Stradella (2016), cit., p. 7.
[55] Ivi, p. 22.

tivi a minori. Il comma 2 prevede inoltre che l'obbligo di cancellazione dei dati gravante sul titolare del trattamento tenga conto della tecnologia disponibile e dei costi di attuazione di tale misura[56].

L'obbligo di cancellazione dei dati personali, impropriamente definito "diritto all'oblio", è stato previsto anche in seguito alla notissima e molto commentata pronuncia pregiudiziale della Corte di Giustizia dell'Unione europea relativa al caso *Google Spain*, di cui si parlerà successivamente, che ha imposto al motore di ricerca di procedere, a richiesta dell'interessato, alla deindicizzazione dei *link* di accesso ad informazioni personali che l'interessato desidera vengano dimenticate[57]. In assenza di parametri oggettivi che possano guidare le valutazioni e le decisioni dei soggetti, pubblici e privati, titolari del trattamento, il nodo critico risiede nell'oggettiva difficoltà di stabilire fino a quando ricorrono le condizioni della permanenza *online* di informazioni riferite al passato, ovvero fino a quando e in base a quali presupposti queste ultime risultano avere ancora un apprezzabile interesse pubblico per la collettività. Così come pure risulta di non automatica individuazione il momento preciso in cui l'interessato può inoltrare la richiesta di cancellazione, e le modalità precise con cui la

[56] Così anche il *considerando* n. 54: «Per rafforzare il "diritto all'oblio" nell'ambiente *online*, è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a informare i titolari del trattamento che trattano tali dati personali di cancellare qualsiasi *link* verso tali dati personali o copia o riproduzione di detti dati personali. Nel fare ciò, è opportuno che il titolare del trattamento adotti misure ragionevoli tenendo conto della tecnologia disponibile e dei mezzi a disposizione del titolare del trattamento, comprese misure tecniche, per informare della richiesta dell'interessato i titolari del trattamento che trattano i dati personali». Da ciò sembra evincersi – secondo Stradella (2016), cit., p. 5 – che, a differenza da quanto statuito dalla Corte di Giustizia nella sentenza *Google Spain*, il regolamento europeo «consideri responsabile del trattamento soltanto il soggetto (ad esempio, l'editore di una pagina *web*) che ha immesso i dati personali nel *web*, soggetto su cui graverebbe quindi (in via esclusiva) l'obbligo di comunicare ai terzi che trattano tali dati della richiesta di cancellazione proveniente dall'interessato; tra i terzi spicca chiaramente il soggetto gestore del motore di ricerca che quindi pur catalogando, indicizzando e diffondendo verso i terzi i dati, non diverrebbe titolare del trattamento e non vedrebbe esercitato direttamente nei suoi confronti il diritto alla cancellazione».

[57] Corte di Giustizia dell'Unione europea, sentenza 13 maggio 2014, causa C-131/12, *Mario Costeja González c. Google Spain Sl, Google Inc., Agencia Española de Protección de Datos*. In tale occasione la Corte ha stabilito che il motore di ricerca, considerato alla stregua del responsabile del trattamento dei dati personali, è obbligato, in presenza di determinate condizioni, a sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei *link* verso pagine *web* pubblicate da terzi e contenenti informazioni relative a tale persona. Tale obbligo può esistere anche nell'ipotesi in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle suddette pagine web, e ciò eventualmente anche quando la loro pubblicazione sulle pagine in questione sia di per sé lecita.

cancellazione deve essere effettuata. Per non parlare del profilo della dubbia idoneità del titolare del trattamento dei dati – ad esempio un motore di ricerca, come nel caso *Google Spain* – a effettuare una valutazione equilibrata del rapporto fra tutela della *privacy* e interesse pubblico all'informazione[58].

Qualora il titolare del trattamento, ricorrendo le suddette condizioni, sia obbligato a procedere alla cancellazione, esso deve anche informare altri «titolari del trattamento che stanno trattando dati personali della richiesta dell'interessato di cancellare qualsiasi *link*, copia o riproduzione dei suoi dati personali» (art. 17, comma 2). Questo nuovo obbligo di informativa gravante sugli intermediari digitali nel loro ruolo di titolari del trattamento deve essere assolto mediante l'adozione di «misure ragionevoli, anche tecniche» e «tenendo conto della tecnologia disponibile e dei costi di attuazione». Si tratta quindi di un obbligo ad intensità variabile, basato sul principio di ragionevolezza, da valutare caso per caso, e sul livello di sviluppo tecnologico. La *ratio* sottesa a questa norma è quella di evitare di gravare l'interessato dell'onere di reperire i gestori di ogni singolo sito in cui l'informazione è pubblicata e di chiedere a ciascuno di essi la cancellazione, poiché questa attività spesso può essere più agevolmente svolta dal titolare del trattamento: si pensi al caso del motore di ricerca, cui l'interessato ha inoltrato richiesta di cancellazione dei dati, rispetto ai singoli siti Internet in cui la notizia è pubblicata; oppure al caso di richiesta di cancellazione inoltrata al gestore di un *social network* i cui utenti condividono informazioni pubblicate su altri siti.

Il diritto all'oblio, secondo il comma 3 dell'art. 17, non potrà essere invocato se le informazioni di cui si chiede la cancellazione sono state pubblicate: in esercizio del diritto alla libertà di espressione e di informazione; in adempimento di obblighi giuridici imposti al titolare del trattamento dalla legge nazionale o europea o nell'esercizio di pubblici poteri di cui il titolare del trattamento è investito a norma di legge; per motivi di interesse pubblico nel settore della sanità pubblica; a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici; per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Fra queste eccezioni, la più rilevante – ben evidenziata dalla Corte di Giustizia nel caso *Google Spain*[59] e da numerose pronunce recenti della nostra Corte di Cassazione[60] – è la prima, cioè il fatto che le informazioni di cui si chiede la cancellazione sia rilevanti al fine di assicurare l'esercizio della libertà

[58] D'Arienzo (2015), cit., p. 20 e 28.
[59] Alla sentenza *Google Spain* è dedicato il par. 5 di questo capitolo.
[60] Si veda il par. 6 di questo capitolo.

di cronaca, che implica che i cittadini siano informati di tutte le notizie di interesse pubblico.

Certo, data la circolazione ubiquitaria delle informazioni su Internet, una volta che vi sono state immesse, parlare di diritto all'oblio può semplicemente sembrare paradossale e anacronistico[61]. Si pensi al fatto che, tramite la funzione "copia *cache*", molti motori di ricerca mettono a disposizione degli utenti una copia dei dati testuali di ogni pagina *web* archiviata, anche quando la risorsa originale sia divenuta irraggiungibile. Oppure al fatto che gli utenti dei *social network* immettono ogni giorno in Rete volontariamente dati personali propri ed altrui, anche sensibili, non necessariamente consapevoli che la cancellazione di tali dati, condivisi da decine, centinaia o forse anche migliaia di altri utenti, non potrà mai essere realizzata del tutto. Bisogna dunque distinguere fra un'accezione ampia del concetto di diritto all'oblio come diritto ad essere dimenticati, che oggi rappresenta più un'aspirazione che una reale possibilità, e un'accezione più ristretta concernete solo il profilo del trattamento dei dati personali, in base alla quale si richiede all'intermediario digitale – motore di ricerca, *host provider* o *content provider* – di cancellare quelli scorretti, distorti o non più rilevanti, cosa che non necessariamente garantisce l'assoluta irreperibilità del dato. È in quest'accezione che il diritto all'oblio è considerato nella sentenza *Google Spain* così come nel regolamento Ue n. 2016/679. Il fatto incontestabile è che, come è stato giustamente notato[62], «abbiamo voluto, e per certi versi lasciato, che Internet invadesse la nostra vita individuale e comunitaria (fino al punto che oggi larga parte della nostra vita si svolge in Internet) perché abbiamo ritenuto, più o meno consapevolmente, che i benefici derivanti dalla grande Rete fossero, per tutti e per ognuno, infinitamente maggiori rispetto alle inevitabili (piccole?) controindicazioni».

2. Licenze d'uso e *privacy policies* dei *social network*

2.1. Le licenze d'uso come contratti sinallagmatici

Il rapporto fra utenti e gestore della piattaforma di *social networking* è regolato norme contrattuali[63].Caratteristiche di questi contratti (*terms of*

[61] Di Ciommo (2014), cit.

[62] Di Ciommo (2014), cit., p. 1111.

[63] A titolo esemplificativo: condizioni d'uso di *Facebook*: https://it-it.facebook.com/terms.php e https://www.facebook.com/legal/terms/update; termini di servizio di *Twitter*: https://twitter.com/it/tos; condizioni d'uso di *Instagram*: https://it.facebook.-

service) – che più propriamente devono essere considerati licenze d'uso di un bene immateriale, quindi contratti atipici[64] – sono: la transnazionalità, in quanto i servizi offerti dagli intermediari digitali si rivolgono a utenti di tutto il mondo; la gratuità, poiché il *provider* mette a disposizione dell'utente i propri servizi gratuitamente, senza richiedere alcuna controprestazione; il difetto di sinallagmaticità, poiché *prima facie* non sussisterebbe alcuno scambio di prestazioni. In realtà, la presunta gratuità del rapporto contrattuale nasconde una componente suscettibile di valutazione patrimoniale, considerando che i gestori dei *social network sites* traggono profitto proprio attraverso la raccolta dei dati personali e sensibili degli utenti (il c. d. *user data profiting*), di cui gli inserzionisti pubblicitari si servono al fine di individuare i profili degli utenti cui destinare pubblicità mirata in base ai loro gusti, alle loro preferenze, alle loro attitudini (*behavioural advertising*)[65]. Dunque, qualcuno ritiene che questo tipo di contratti andrebbero più correttamente inquadrati nella categoria civilistica dei contratti a prestazioni corrispettive o addirittura, vista la massiccia presenza di clausole che "alleggeriscono" la posizione contrattuale del *provider* – in quella dei contratti di appalto o di somministrazione di servizi[66].

I *terms of service* sono normalmente corredati da informative sulla *privacy*[67], nonché da ulteriori informazioni rivolte agli utenti, spesso redatte in

com/help/instagram/478745558852511; termini di servizio di *WhatsApp*: https://www.-whatsapp.com/legal/?l=it#key-updates.

[64] F. Agnino (2012), *Fino a che punto è possibile disporre contrattualmente dei propri diritti? (Vedi contratto FB)*, in *Giurisprudenza di merito*, n. 12, pp. 2555-2568; R. Ducato (2016), *I social network*, in G. Pascuzzi (a cura di), *Il diritto nell'era digitale*, Bologna, Il Mulino, pp. 269-288; P. Galdieri (2012), *Il trattamento illecito del dato nei social network*, in *Giurisprudenza di merito*, n. 12, pp. 2697-2713; S. Scalzini (2012), *I servizi di online social network tra privacy, regole di utilizzo e violazione dei diritti dei terzi*, in *Giurisprudenza di merito*, n. 12, pp. 2569-2590; S. Sica e G. Giannone Codiglione (2012), *Social network sites e il "labirinto" delle responsabilità*, in *Giurisprudenza di merito*, n. 12, pp. 2714-2733.

[65] Sulle informazioni personali degli utenti come beni di natura economica si vedano anche A. R. Popoli (2014), *Social network e concreta protezione dei dati sensibili: luci ed ombre di una difficile convivenza*, in *Il diritto dell'informazione e dell'informatica*, n. 6, pp. 981-1017, che mette bene in luce anche l'aspetto delle clausole vessatorie contenute in tali contratti. Si veda inoltre G. Giannone Codiglione (2017), *I dati personali come corrispettivo della fruizione di un servizio di comunicazione elettronica e la "consumerizzazione" della privacy*, in *Il diritto dell'informazione e dell'informatica*, n. 2, pp. 419-425.

[66] Sica e Giannone Codiglione (2012), cit., partic. pp. 2718-2719. Inoltre S. A. Cerrato (2011), *I rapporti contrattuali (anche associativi) tra i soggetti del social network*, in *Aida. Annali del diritto d'autore, della cultura e dello spettacolo*, p. 183.

[67] Per *Facebook*: https://it-it.facebook.com/about/privacy/; per *Twitter*: https://twitter.com/it/privacy; per *Instagram*: https://help.instagram.com/155833707900388; per *WhatsApp*: https://www.whatsapp.com/legal/?l=it#privacy-policy. Sulle *privacy policies* si veda Popoli (2014), cit.

forma di linee-guida o di lista di *Faq*[68], che hanno la funzione di spiegare agli utenti il significato delle clausole contrattuali con maggiore chiarezza e semplicità. Inoltre, talvolta sono presenti pagine informative dedicate a taluni specifici aspetti, come ad esempio l'utilizzo dei *cookie*[69] o la protezione dei diritti di proprietà intellettuale[70]. Infine, possono essere offerti agli utenti alcuni servizi, fra cui quello relativo alla segnalazione di contenuti illeciti[71] o alla personalizzazione dell'*advertising*[72].

Tanto le condizioni generali di contratto quanto le *privacy policies* subiscono continue modifiche ed esprimono una tendenza al progressivo aumento della complessità[73]. Il *New York Times* nel 2010 ha evidenziato come la *privacy policy* di *Facebook* sia passata dalle 1004 parole del 2005 alle quasi 6.000 del 2010, divenendo più lunga della Costituzione americana; aggiungendo le Faq, inoltre, si raggiungono le 45.000 parole, ovvero la metà di un romanzo. In aggiunta a ciò, è stato notato come per cambiare le impostazione della *privacy* sia necessario cliccare almeno cinquanta pulsanti e scegliere tra più di 170 opzioni[74]. Ciò non favorisce certamente l'utente, che si trova a dover cambiare frequentemente le impostazioni prescelte per adeguarle a requisiti sempre nuovi.

2.2. La dichiarata (ma insostenibile) estraneità dei social network provider *rispetto alle condotte degli utenti*

La principale finalità delle clausole contrattuali – che peraltro si riferiscono solo ai rapporti fra utenti e gestori del servizio, lasciando impregiudi-

[68] Per *Facebook*: https://it-it.facebook.com/help/?helpref=hc_global_nav; per *Twitter*: https://support.twitter.com/articles/93870; per *Instagram*: https://help.instagram.com/4774-34105621119/?helpref=hc_fnav&bc[0]=Centro%20assistenza%20di%20Instagram&bc[1]=Privacy%20e%20Centro%20per%20la%20sicurezza.

[69] Per *Twitter*: https://support.twitter.com/articles/20170519; per *WhatsApp*: https://-www.whatsapp.com/legal/?l=it#cookies.

[70] Per *Facebook*: https://it-it.facebook.com/help/399224883474207?helpref=hc_global_nav; per *WhatsApp*: https://www.whatsapp.com/legal/?l=it#ip-policy; per *Instagram*: https://help.instagram.com/535503073130320/?helref=hc_fnav&bc[0]=Centro%20assistenza%20di%20Instagram&bc[1]=Privacy%20e%20Centro%20per%20la%20sicurezza&bc[2]=Segnalazione%20di%20un%20contenuto.

[71] Per *Facebook*: https://it-it.facebook.com/help/1753719584844061/?helpref=hc_fnav; per *Instagram*: https://help.instagram.com/155833707900388.

[72] Per *Facebook*: https://it-it.facebook.com/help/109378269482053/?helpref=hc_fnav; per *Twitter*: https://business.twitter.com/it/help/troubleshooting/how-twitter-ads-work.html; per *Instagram*: https://it-it.facebook.com/help/instagram/1415228085373580.

[73] Popoli (2014), cit., par. 3.1.

[74] N. Bilton (2010), *Price of Facebook Privacy? Start Clicking*, in *The New York Times*, www.nytimes.com.

cati i rapporti orizzontali fra utenti – al di là della diversità di formulazioni che caratterizzano ciascun servizio, è quella di sottolineare la completa estraneità del *provider* rispetto alle condotte eventualmente illecite degli utenti. È l'utente a dover decidere in che modo intende gestire i propri dati, spesso in base al presupposto per cui le informazioni caricate *online* sono in linea di principio pubbliche, a meno che l'utente stesso non abbia deciso di impostare più restrittivamente i requisiti di *privacy*. I gestori dei *social network*, dunque, aspirano a configurarsi come Isp neutrali, cui possono essere applicate le norme sulla limitazione di responsabilità, e non come *hosting provider* attivi o *content provider*.

Per illustrare meglio questo atteggiamento, a titolo esemplificativo si può fare riferimento ad alcune clausole contenute nei *Terms of Service* di *Instagram* o di *Twitter*. Nel caso di *Instagram*, è esplicitato al punto n. 8 che «l'utente è il solo responsabile del proprio comportamento e di tutti i dati, testi, file, informazioni, nomi utente, immagini, grafici, foto, profili, audio e videoclip, suoni, composizioni musicali, opere di proprietà intellettuale, *app,link* e altri contenuti o materiali (collettivamente, i "Contenuti") inviati, pubblicati o mostrati sui Servizi o tramite essi». Per quanto riguarda *Twitter*, le clausole contrattuali si rivolgono all'utente in questi termini: «Sei responsabile dell'utilizzo dei Servizi e dei Contenuti che fornisci, compreso il rispetto delle leggi applicabili, delle norme e dei regolamenti. Devi fornire solo Contenuti che ritieni di poter condividere con altri. Qualsiasi utilizzo o affidamento relativo ai Contenuti o documenti pubblicati tramite i Servizi o ottenuti attraverso i Servizi avviene a tuo rischio. Noi non approviamo, sosteniamo, affermiamo o garantiamo la completezza, la veridicità, l'accuratezza o l'affidabilità dei Contenuti o comunicazioni pubblicate tramite i Servizi né le opinioni espresse attraverso i Servizi. Sei consapevole che utilizzando i Servizi puoi essere esposto a Contenuti che potrebbero essere offensivi, dannosi, imprecisi o inappropriati oppure, in alcuni casi, a messaggi che sono stati interpretati erroneamente o in modo ingannevole. La responsabilità relativa ai Contenuti ricade esclusivamente sulla persona che li ha creati. Noi non possiamo monitorare o controllare i Contenuti pubblicati tramite i Servizi e non ne siamo responsabili».

Tuttavia, al di là di quanto dichiarato dai *social network provider*, va evidenziato il fatto che nella realtà l'attività dei Snp spesso non è affatto neutrale rispetto ai contenuti diffusi dagli utenti. Si, pensi, ad esempio, all'utilizzo che *Facebook* fa dell'algoritmo *Edgerank*, che valorizza taluni contenuti in base al numero e alla frequenza delle interazioni fra gli utenti[75]. Così, le notizie

[75] Per comprendere meglio il funzionamento dell'algoritmo di *Facebook* si veda: K. Newman, *The ultimate guide to the Facebook Edgerank algorithm*, 17 agosto 2011, https://-

più popolari vengono mostrate ai vari utenti, in base ai loro gusti personali, nella lista personalizzata dei *trending* ("popolari"), che appare in una apposita colonna nella sezione *News Feed*, senza che gli utenti normalmente abbiano alcuna consapevolezza di tale procedimento di filtraggio[76]. In questo modo, *Facebook* incoraggia la lettura e la condivisione delle notizie più richieste, individuate attraverso un monitoraggio dei comportamenti *online* degli utenti stessi, che vengono corredata di pubblicità mirata in relazione ai profili degli interessati. Tra l'altro, non è escluso che, attraverso questa attività, venga amplificata la diffusione notizie false, ma eclatanti, diffuse da siti inaffidabili[77]. Del resto, più un'informazione – vera o falsa che sia – diventa "virale", maggiori saranno i guadagni per gli inserzionisti pubblicitari che traggono vantaggio dal gran numero dei fruitori di tale informazione. Non si può quindi sostenere che *Facebook* sia in una posizione del tutto neutra sia rispetto alla circolazione di talune notizie sia rispetto all'utilizzo di informazioni personali degli utenti[78].

Simili processi stanno avvenendo anche su *Instagram*, piattaforma che è stata recentemente acquisita da *Facebook*: l'algoritmo di *Instagram*[79] da alcuni mesi si sta strutturando in modo simile a quello di *Facebook*, per cui viene offerta maggiore visibilità a taluni contenuti (per lo più immagini) in base al numero e alla qualità delle interazioni fra utenti; in questo modo, agli utenti vengono offerti contenuti specifici selezionati in base ai loro gusti, venendo incontro alle esigenze delle aziende che utilizzano *Instagram* nella loro strategia di *social media marketing*. Qualcosa di analogo sta avvenendo anche in *Twitter*, che dal 2016 utilizza un algoritmo[80] che mette in

econsultancy.com/blog/7885-the-ultimate-guide-to-the-facebook-edgerank-algorithm; inoltre A. Puliafito, *Algoritmo Facebook: il News Feed, come funziona e come cambia*, 13 ottobre 2017, www.albertopuliafito.it/algoritmo-facebook/.

[76] G. Pitruzzella (2017), *La libertà di informazione nell'era di Internet*, in G. Pitruzzella, O. Pollicino e S. Quintarelli, *Parole e potere. Libertà d'espressione, hate speech e fake news*, Milano, Egea, partic. pp. 64-67.

[77] Sulla responsabilità degli intermediari digitali nella diffusione di *fake news* si veda l'ultimo capitolo di questo libro.

[78] Recentemente la policy di *Facebook* circa le *fake news* è diventata più restrittiva: si sta implementando un meccanismo che consente agli utenti di segnalare le notizie false, che vengono poi controllate da un gruppo di *fact-checkers* professionisti esterni; le pagine scoperte a diffondere ripetutamente notizie false non potranno più acquistare campagne per portare traffico a pagamento sui siti corrispettivi.

[79] Per comprendere meglio il funzionamento dell'algoritmo di *Instagram* si vedano: *Come funziona l'algoritmo di Instagram: i 7 fattori chiave*, 10 maggio 2017, https://daocontent.com/come-funziona-algoritmo-instagram/; E. Pasqualetto, *Come funziona il nuovo algoritmo di Instagram: i fattori chiave*, 9 maggio 2017, https://elisapasqualetto.it/come-funziona-il-nuovo-algoritmo-di-instagram/.

[80] Per comprendere meglio il funzionamento dell'algoritmo di *Twitter* si vedano: *Come funziona l'algoritmo della timeline di Twitter?*, 1° giugno 2017, www.commu-

evidenza taluni contenuti non in base all'ordine cronologico, ma in base a ciò che si presume possa risultare più interessante per il singolo utente, i cui comportamenti *online* vengono profilati. In *Twitter*, inoltre, i *tweet* più rilevanti sono organizzati per sezioni tematiche[81] e agli utenti vengono suggerite le modalità per migliorare le proprie *performances* in termini di visibilità, fornendo anche le relative statistiche[82].

Ciò considerato, ben difficilmente i *social network provider* possono in realtà ricusare le responsabilità relative al trattamento dei dati personali, a dispetto di quanto dichiarato nelle clausole contrattuali rivolte all'utente. Ai sensi della normativa al momento vigente (direttiva 94/46/Ce e d. lgs. 196/2003) essi possono essere considerati a tutti gli effetti responsabili del trattamento dei dati, ai sensi della normativa vigente, anche perché la loro attività ha natura professionale e finalità di lucro e, come si è visto nel paragrafo precedente, non può beneficiare della *household exemption*. Ammesso che, in linea con quanto dichiarato dagli stessi Snp nelle clausole contrattuali, il responsabile del trattamento dei propri dati sia l'utente, essi non possono sfuggire a tale qualifica almeno per quanto riguarda l'attività di profilazione degli utenti con finalità di *marketing* diretto, poiché in questo caso sono proprio i gestori delle piattaforme a determinare le finalità (il *behavioural advertising*) e i mezzi (gli algoritmi di profilazione) del trattamento. Per giunta, poiché il trattamento dei dati degli utenti avviene a fini di profitto, non si può escludere in via teorica l'applicabilità ai Snp del reato di cui all'art. 167 del *Codice della privacy* (trattamento illecito dei dati), di cui il profitto per sé o per altri è elemento costitutivo. Quando – ormai è questione di poche settimane – diverrà applicabile la distinzione fra "titolare" e "responsabile" del trattamento prefigurata dal regolamento (Ue) 216/679, i Snp saranno da considerarsi "titolari" dei trattamenti di dati di cui determinano finalità e mezzi (quindi, quando effettuano attività di profilazione degli utenti) e "responsabili" dei trattamenti di dati effettuati per conto degli utenti (cioè ogni qual volta i dati personali vengono memorizzati e trasmessi per consentire le interazioni fra gli utenti). In entrambi i casi, i gestori delle piattaforme non potranno sottrarsi alle connesse responsabilità.

nicationvillage.com/blogs/2017/06/01/come-funziona-algoritmo-della-timeline-di-twitter/; *Twitter, come funziona il suo algoritmo misterioso*, 10 marzo 2017, www.linkiesta.it-/it/article/2017/03/10/twitter-come-funziona-il-suo-algoritmo-misterioso/33505/.

[81] https://twitter.com/?lang=it.

[82] https://analytics.twitter.com/about.

2.3. Bring Your Own Identity

In conclusione, va segnalato che questione del trattamento dei dati personali degli utenti da parte dei gestori dei *social network* negli ultimi tempi si sta arricchendo di ulteriori profili problematici per via della diffusione del fenomeno conosciuto come Byoid (*Bring Your Own Identity*)[83]. Si tratta, in altre parole, di un meccanismo che consente di semplificare l'accesso ai vari siti Internet per i quali è richiesta una registrazione: senza dover acquisire e ricordare sempre nuove credenziali d'accesso ad ogni nuova registrazione a diversi siti, l'utente può utilizzare sempre le stesse credenziali di accesso a un *social network*. Gli utenti tendono a considerare questo sistema comodo e pratico; le imprese che operano su Internet lo apprezzano perché in tal modo possono acquisire sempre maggiori e più accurate informazioni sull'identità dei loro clienti. Il fatto è che le informazioni personali che ciascuno condivide con altri all'interno del *social network* raggiungono, spesso con il consenso inconsapevole del titolare dei dati, soggetti posti al di fuori della cornice pure estremamente ampia degli altri utenti del medesimo *social network.* Inutile sottolineare come divenga essenziale che gli utenti delle piattaforme *social* ricevano una adeguata informazione sul trattamento dei loro dati personali anche relativamente a questo specifico aspetto. Inutile anche evidenziare la difficoltà, in caso di trattamento illegittimo di tali dati, di distinguere le responsabilità fra il gestore del *social network* e quello del sito esterno cui si è acceduto utilizzando le credenziali del *social network*.

3. Profili giurisprudenziali sul trattamento dei dati personali da parte dei *provider*: il caso *Google c. ViviDown*

Sulla controversia che ha contrapposto, con alterne vicende, la filiale italiana di *Google* all'associazione *ViviDown* si è scritto molto[84]. In questa

[83] Si veda A. Salerno (2014), *Byoid: l'identità digitale la gestisce il social network*, in *www.corrierecomunicazioni.it*.

[84] *Ex pluribus*: S. Alvanini (2010), *La responsabilità dei services providers*, in *Il diritto industriale*, n. 4, pp. 239-337; E. Bassoli (2013), *Esclusa la responsabilità penale di Google per violazione di dati personali da parte di materiale multimediale immesso da terzi*, in *Rivista penale*, n. 5, pp. 558-563; E. Bassoli (2014), *L'approdo finale della vicenda Google-ViviDown*, in *Rivista penale*, n. 5, pp. 501-503; M. Bianca (2016), *Il caso Google-ViviDown: un caso di cyberbulismo*, in M. Bianca, A. Gambino, R. Messinetti (a cura di), *Libertà di manifestazione del pensiero e diritti fondamentali*, Milano, Giuffrè, pp. 92-95; G. Cassano (2010), *Google v. Vividown. Responsabilità "assolute" e fine di internet*, in *Vita notarile*, n. 2, pp. 579-594; P. Galdieri (2012), *Il trattamento illecito del dato nei social net-*

sede, il caso rileva soprattutto per i profili attinenti alla questione del trattamento dei dati personali da parte di un intermediario digitale e non tanto per quelli relativi al reato di diffamazione.

Il caso trae origine da un video girato da alcuni studenti di un istituto tecnico torinese, in cui un minore affetto dalla sindrome di Down veniva deriso, offeso, umiliato, minacciato e sottoposto a violenza fisica attraverso spintoni e lancio di oggetti. Nel settembre 2006 il video, caricato sulla piattaforma di *video-sharing* gestita da Google (*GoogleVideo*), otteneva moltissime visualizzazioni e saliva ai primi posti nella classifica dei video più divertenti e più scaricati. Un paio di mesi dopo, su segnalazione di un utente, il video veniva rimosso dalla Polizia postale. Comunque, il padre della vittima e l'associazione *ViviDown*, portatrice degli interessi dei soggetti afflitti dalla sindrome di Down, hanno querelato i *manager* di Google *Italia* (beneficiaria degli introiti pubblicitari derivanti dai video caricati su *Google Video*) e di *Google Inc.* per concorso omissivo nel delitto di diffamazione nei confronti del minore ripreso nel video e dell'associazione *ViviDown* (art. 40, comma 2, e art. 595 del codice penale), nonché per aver effettuato un illecito trattamento dei dati personali e sensibili (art. 167 del d. lgs. n. 196/2003).

La sentenza di primo grado[85] ha assolto gli imputati per l'imputazione relativa al concorso omissivo nel reato di diffamazione, non ritenendo sussistente in capo agli imputati l'obbligo giuridico di impedire il compimento di reati da parte dei propri utenti. La curia milanese, tuttavia, ha ritenuto

work, in *Giurisprudenza di merito*, n. 12, pp. 2697-2713; T. Giovannetti (2014), Governance *della Rete e il ricorso alla sanzione penale: il caso della responsabilità dell'*Internet Service Provider *tra tentazioni punitive e rispetto dei principi costituzionali*, in M. Nisticò e P. Passaglia (a cura di), *Internet e Costituzione*, Torino, Giappichelli, pp. 315-335.; M. Iaselli (2014), *Caso Vividown: la decisione della Cassazione nel solco della legalità*, in *Vita notarile*, n. 2, pp. 663-673; A. Ingrassia (2012), *Il ruolo dell'Isp nel ciberspazio: cittadino, controllore o tutore dell'ordine*?, in *www.penalecontemporaneo.it*; A. Ingrassia (2013), *La Corte d'Appello assolve i manager di Google anche dall'accusa di illecito trattamento dei dati personali*, in *www.penalecontemporaneo.it*; A. Ingrassia (2014), *La sentenza della Cassazione sul caso Google*, in *www.penalecontemporaneo.it*; F. Resta (2013a), *Diritti individuali e libertà della rete nel caso Vivi Down*, in *Giurisprudenza di merito*, n. 7-8, pp. 1589-1600; F. Resta (2013b), *Libertà della rete e protezione dei dati personali: ancora sul caso Google - Vivi Down*, in *Il diritto dell'informazione e dell'informatica*, n. 3, pp. 502-514; F. Resta (2014), *La rete e le utopie regressive (sulla conclusione del caso Google/Vividown*), in *Il diritto dell'informazione e dell'informatica*, n. 2, pp. 237-241; G. M. Riccio (2013), *Google/Vividown: "leading case" o abbaglio giurisprudenziale?*, in *Vita notarile*, n. 2, pp. 606-624; C. Rossello (2010), *Riflessioni de jure condendo sulla responsabilità del provider*, in *Il diritto dell'informazione e dell'informatica*, n. 4-5, pp. 617-629; R. Salvi (2014), *La Corte di Cassazione sul caso Google vs. Vivi Down: l'host provider non governa il mare magnum della rete*, in *www.diritto.it*.

[85] Tribunale di Milano, 4° sezione penale, sentenza 24 febbraio 2010, n. 1972.

sussistente il reato di trattamento illecito di dati personali e sensibili, in quanto questi ultimi (l'immagine del ragazzo deriso e le informazioni circa il suo stato di salute) erano stati raccolti senza il consenso dell'interessato e utilizzati illecitamente a fini di profitto, considerando che la piattaforma *Google Video* raccoglieva e organizzava i contenuti caricati dagli utenti al fine di abbinare ad essi inserzioni pubblicitarie "mirate" mediante il sistema *AdWords*. Ora, pur essendo fuor di dubbio che l'obbligo di richiedere all'interessato il consenso al trattamento dei dati gravasse in primo luogo su coloro che hanno effettuato le riprese video, così come la responsabilità penale per diffamazione, il tribunale ha ritenuto che l'Isp – soprattutto in veste di *host* attivo – fosse tenuto per legge (*ex.* art. 13 del *Codice della Privacy* relativo agli obblighi di informativa nei confronti di coloro cui i dati personali si riferiscono) non certo a controllare preventivamente i contenuti diffusi dagli utenti, ma a fornire agli utenti della piattaforma una corretta informazione sugli obblighi ad essi imposti dalla legge. Per la curia, pur non esistendo un obbligo di legge che impone agli Isp il controllo preventivo dell'enorme mole di dati che passano attraverso i servizi da essi offerti, e pur non potendo ricavare tale obbligo semplicemente aggirando il divieto dell'interpretazione analogica delle norme penali *in malam partem*, tuttavia «non esiste nemmeno la "sconfinata prateria" di Internet dove tutto è permesso e niente può essere vietato, pena la scomunica mondiale del popolo del web»[86]. In altre parole, il *provider* è stato ritenuto «responsabile per una insufficiente e colpevole comunicazione degli obblighi di legge in tema di trattamento illecito di dati personali, non essendo all'uopo idoneo un generico richiamo all'interno delle condizioni generali di sevizio, e con la prospettiva di ricavare da tale servizio benefici economici derivanti dal collegamento con un sistema di annunci pubblicitari»[87].

In sede di gravame, però, la sentenza è stata ribaltata. La Corte d'Appello di Milano[88] ha infatti annullato la condanna per il presunto illecito trattamento di dati personali poiché, dal combinato disposto degli artt. 13 e 167 del *Codice della privacy* (d. lgs. n. 196/2003), non si evincerebbe alcun dovere per il *provider* di informare gli utenti in merito alla disciplina sul trattamento dei dati personali. Infatti, pur confermando il ruolo "attivo" (non neutrale) di *Google Video* nell'organizzazione dei contenuti, da tale

[86] Citazione tratta da p. 95 della sentenza.

[87] P. Galdieri (2012), *Il trattamento illecito del dato nei social network*, in *Giurisprudenza di merito*, n. 12, p. 2705.

[88] Corte d'Appello di Milano, prima sezione penale, sentenza 12 dicembre 2012, n. 8611. Si veda soprattutto l'ottimo commento di A. Ingrassia (2013), *La Corte d'Appello assolve i manager di Google anche dall'accusa di illecito trattamento dei dati personali*, in *www.penalecontemporaneo.it*.

qualifica non si può far discendere un obbligo di predisporre un controllo preventivo in capo al *provider*: ciò sarebbe impossibile sia sotto il profilo quantitativo, per la mole di materiale caricata in rete, sia sotto quello qualitativo, non esistendo un filtro che verifichi semanticamente i dati sensibili eventualmente trattati nelle riprese e la corrispondente presenza di un consenso per tali dati. Inoltre, il reato di illecito trattamento dei dati personali (art. 167 del *Codice della privacy*) è un reato di mera condotta e non di evento, per cui non è possibile configurarne la fattispecie omissiva. In aggiunta a ciò, l'eventuale violazione degli obblighi di informativa di cui all'art. 13 del *Codice della privacy* non costituirebbe reato penale, ma semplice illecito amministrativo. Infine, considerando che – secondo la Corte d'Appello – il rapporto tra i soggetti ripresi e il *provider* è disciplinato dalla normativa sul commercio elettronico (d. lgs. n. 70/2003), secondo gli artt. 16 e 17 l'*host provider* non ha alcun obbligo di vigilare sul materiale che si limita a trasmettere e memorizzare né alcun onere di ricercare fatti o circostanze sintomatici di attività illecite, ma ha solo il dovere di rimuovere il materiale illecito su richiesta dell'autorità o qualora abbia diretta conoscenza dell'illiceità dei contenuti memorizzati.

La decisione del giudice di secondo grado è stata sostanzialmente confermata dalla Corte di Cassazione[89]. In via preliminare, la Suprema Corte ha confermato l'assenza di una posizione di garanzia in capo agli Isp: «Dall'esame delle disposizioni riportate, emerge che nessuna di esse prevede che vi sia in capo al *provider*, sia esso anche un *hosting provider*, un obbligo generale di sorveglianza sui dati immessi da terzi sul sito da lui gestito. Né sussiste in capo al *provider* alcun obbligo sanzionato penalmente di informare il soggetto che ha immesso i dati dell'esistenza e della necessità di fare applicazione della normativa relativa al trattamento dei dati stessi»[90]. Il reato di cui all'art. 167 del *Codice della privacy*, sempre secondo la Corte, si applica specificamente solo al titolare del trattamento dei dati, e non a qualunque altro soggetto che si trovi ad avere a che fare con i dati. Nella fattispecie, l'Isp – sia pure in veste di *host* attivo – non può essere equiparato al titolare del trattamento, in quanto tale qualifica si riferisce solo al soggetto che può determinare scopi, modi e mezzi del trattamento, mentre l'Isp non ha alcun controllo sui dati memorizzati, né contribuisce allo loro scelta, ricerca e formazione del *file* in cui i dati sono contenuti. Questa impostazione sarebbe confermata – a giudizio della Corte – anche dagli artt. 16 e 17 del d. lgs. 70/2003, che limitano la responsabilità civile dell'*hosting provider* a condizione che non sia a conoscenza del comporta-

[89] Corte di Cassazione, terza sezione penale, sentenza 17 dicembre 2013, n. 5107.
[90] Citazione tratta dal punto n. 7 della sentenza.

mento illecito degli utenti e che esclude la presenza di un obbligo generale di sorveglianza sulle informazioni trasmesse o memorizzate, nonché di un obbligo generale di ricercare attivamente eventuali illeciti. Occorre allora interpretare in modo armonico le norme della disciplina del commercio elettronico con quelle riguardanti la protezione dei dati personali e, proprio in base a tale interpretazione armonizzata, il *provider* non può essere ritenuto responsabile dei dati che ha contribuito a trasmettere o memorizzare a meno che, essendo venuto a conoscenza della loro illiceità, non abbia provveduto prontamente a rimuoverli. Nel caso di specie, i soli titolari del trattamento dei dati sarebbero i soggetti che hanno effettuato il video, mentre ai *manager* di *Google* non può essere imputato il reato di trattamento illecito di tali dati: essi infatti non erano a conoscenza del contenuto illecito del video e, appena acquisita tale conoscenza, avevano provveduto immediatamente alla rimozione.

Questi stessi principi potrebbero essere applicabili oggi ai *social network provider*? Se lo fossero, bisognerebbe partire dal presupposto che, quali che siano le condotte di coloro che condividono informazioni attraverso le piattaforme di *social networking* e quali che siano le attività svolte dai loro gestori in termini di organizzazione, aggregazione e indicizzazione dei contenuti, nonché di profilazione degli utenti stessi a fini commerciali, i Snp non potrebbero essere considerati responsabili del trattamento dei dati personali e quindi soggetti alle connesse responsabilità. In realtà, poiché oltre un decennio di progresso tecnologico è trascorso dal 2006 – anno dell'*upload* del video relativo al ragazzo con sindrome di Down – ad oggi, il ruolo degli intermediari digitali si è molto evoluto. Quindi, se allora verosimilmente i manager di *Google* potevano invocare la limitazione di responsabilità poiché, per ragioni semplicemente quantitative e tecniche, non potevano essere a conoscenza di eventuali contenuti illeciti prodotti dagli utenti, simili affermazioni da parte dei moderni intermediari digitali apparirebbero oggi inverosimili e irragionevoli. Questo è il motivo per cui i gestori dei principali *social network* si stanno via via dotando di sistemi sempre più sofisticati che consentono agli utenti di segnalare contenuti potenzialmente illeciti e al Snp, previa verifica dell'attendibilità della segnalazione, di rimuovere il contenuto.

Queste dinamiche, a dispetto delle clausole contenute nei *Terms of Service*, che attribuiscono al solo utente la piena ed esclusiva responsabilità di ogni suo comportamento, possono prestarsi ad essere interpretate come un'implicita assunzione di responsabilità, anche alla luce del nuovo regolamento europeo sul trattamento dei dati personali. Appare davvero improbabile, infatti, che con l'entrata in vigore del nuovo regolamento i Snp possano invocare, a sostegno della loro irresponsabilità rispetto al trattamento

dei dati personali, il fatto di non essere nella posizione di determinare le finalità e i mezzi del trattamento. Le loro condotte oggi, nell'era della dittatura dell'algoritmo[91], sembrano piuttosto suggerire il contrario.

4. Spunti dalla giurisprudenza italiana: la responsabilità di *Facebook* per la mancata rimozione di contenuti lesivi della *privacy* e della dignità personale

La vicenda di Tiziana Cantone, giovane donna napoletana che si è tolta la vita, non riuscendo a sopportare le ripercussioni sul piano sociale della diffusione "virale", per mezzo dei *social network*, di alcuni video *hard* di cui era protagonista, che lei stessa aveva inizialmente prodotto, ha appassionato le cronache di qualche tempo fa. Al di là dei dettagli scabrosi e del triste epilogo, in questa sede rilevano soprattutto i risvolti giudiziari della vicenda, che ha a che fare non solo con il trattamento illecito dei dati personali da parte degli intermediari digitali, ma anche – come già nel caso *Google c. Vividown* – con le conseguenti lesioni della dignità personale e della reputazione della protagonista. È interessante il fatto che il caso non riguardi genericamente un *provider*, ma specificamente un *social network provider*, e che i contenuti lesivi siano effettivamente *user-generated*.

Per tentare di ostacolare la diffusione incontrollata dei video, che pure in un momento iniziale lei stessa aveva condiviso tramite *WhatsApp* con un ristrettissimo gruppo di conoscenti, nell'estate del 2015 Tiziana Cantone si è rivolta al giudice civile per ottenere un provvedimento d'urgenza che intimasse a una decina di *social media* (fra cui *Facebook*, *Yahoo!*, *Google*, *YouTube* e alcuni altri meno noti) di cancellare i video in questione dalle rispettive piattaforme, di inibire ogni accesso ad essi da parte degli utenti e di impedire, in via preventiva, nuovi caricamenti degli stessi video o di altri contenuti analoghi che la ritraessero in atteggiamenti sessualmente espliciti. La ricorrente ammetteva che i video erano stati girati con il suo consenso e che era stata lei stessa, inizialmente, ad inviarli a cinque persone di cui si fidava, ma eccepiva di non aver prestato alcun consenso alla loro ulteriore circolazione; invece, proprio a causa della enorme ed incontrollata diffusione di tali contenuti, la sua reputazione e la sua stabilità psicologica erano state gravemente pregiudicate.

[91] Per ulteriori riflessioni sul funzionamento degli algoritmi di ricerca, sulle loro presunte (o asupicate) neutralità, accuratezza, affidabilità e correttezza, e soprattutto sul loro ruolo di controllori/censori della società dell'informazione si veda G. Fioriglio (2015), *La "dittatura" dell'algoritmo: motori di ricerca web e neutralità della indicizzazione. Profili informatico-giuridici*, in *Bocconi Legal Papers*, n. 5.

Il tribunale di Napoli Nord in composizione monocratica, con ordinanza del 10 agosto 2016 (depositata il 5 settembre) ha accolto il ricorso solo parzialmente. In primo luogo, il giudice ha escluso che la ricorrente potesse vantare un generale diritto all'oblio: «non si ritiene che rispetto al fatto pubblicato sia decorso quel notevole lasso di tempo che fa venir meno l'interesse della collettività alla conoscenza della vicenda». Presupposto fondamentale per opporsi al trattamento dei dati personali adducendo il diritto all'oblio, ha spiegato il giudice, è che tali dati si riferiscano a fatti lontani nel tempo, dai quali l'interessato abbia cercato di allontanarsi intraprendendo nuovi percorsi di vita personale e sociale. Al contrario, la vicinanza temporale dei fatti oggetto del ricorso e la stessa diffusione telematica dei video, per via della quale i fatti risultavano sempre attuali, avrebbero reso inapplicabile tale presupposto al caso di specie. Il giudice, dunque, ha posto in relazione il diritto all'oblio essenzialmente con l'elemento temporale, trascurando altre valutazioni, come ad esempio quella del protrarsi della lesione dei diritti della personalità della ricorrente, con conseguente aggravamento del danno non patrimoniale.

Anche la richiesta di risarcimento dei danni inoltrata dalla ricorrente è stata respinta, in quanto inammissibile in sede cautelare, rimandando la questione ad un eventuale successivo giudizio di merito. Nel caso di cinque dei dieci intermediari digitali indicati nel ricorso – segnatamente *Google*, *YouTube*, *Yahoo*, *Citinews* e *Appideas* – il giudice ha rilevato talune inesattezze nell'individuazione dei soggetti legalmente responsabili[92] o ha eccepito che i video erano stati effettivamente già rimossi in precedenza oppure ha ritenuto inapplicabile l'ordine di cancellazione dei contenuti lesivi, in quanto la ricorrente non aveva indicato con precisione i *link* da rimuovere. In particolare nel caso di motori di ricerca come *Google* e *Yahoo!*, l'indicazione precisa di tali *link* sarebbe stata una condizione necessaria per procedere alla loro rimozione poiché il motore di ricerca, la cui funzione consiste solo nell'aggregazione e nell'indicizzazione delle informazioni, non avrebbe potuto essere a conoscenza dei contenuti dei *link* indicizzati. In favore di questi cinque soggetti alla ricorrente è stato anche imposto il rimborso delle spese legali, per una cifra pari a circa ventimila euro.

Solo nei confronti di *Facebook* e di altri quattro siti, fra cui alcune testate giornalistiche *online*[93], il giudice ha ordinato, oltre al pagamento delle spese in favore della ricorrente, «l'immediata cessazione e rimozione dalla

[92] Per esempio, il ricorso era stato presentato conto *Yahoo! Italia* e non contro *Yahoo! Inc*.

[93] Oltre a *Facebook Ireland*, le altre quattro parti soccombenti sono state Sem srl, Ernesto Alaimo, Pasquale Ambrosino e Rg Produzioni. A loro carico è stato disposto il pagamento, in favore della ricorrente, di «320 euro, per esborsi, e 3.645 euro per compenso professionale, oltre al rimborso delle spese generali nella misura del 15 per cento sul compenso».

piattaforma del *social network* di ogni post o pubblicazione contenente immagini (foto e/o video) o apprezzamenti riferiti specificamente alla persona della ricorrente».

Il 20 settembre 2016, alcuni giorni dopo il suicidio di Tiziana Cantone, *Facebook Ireland Ltd* ha presentato reclamo contro l'ordinanza con le seguenti motivazioni: in primo luogo, al momento della decisione del primo giudice, i quattro *link* indicati dalla ricorrente non erano più accessibili tramite *Facebook*; inoltre, l'ordine di rimozione di "qualsiasi" *link* o post riferito alla ricorrente era inattuabile per via della sua eccessiva genericità e avrebbe implicato oneri di sorveglianza preventiva per il *provider*; infine, il d. lgs. n. 70/2003 non imporrebbe ai *provider*, in assenza di un ordine emesso dalle competenti autorità, alcun obbligo di rimozione dei contenuti. Il giudice del reclamo[94] ha in effetti dato ragione a *Facebook* circa l'assenza, in capo ai *provider*, di obblighi di sorveglianza preventiva o di ricerca attiva di fatti e circostanze illeciti, ma ha ritenuto «sussistente una responsabilità per le informazioni oggetto di memorizzazione durevole o *hosting* laddove, come avvenuto nel caso di specie, il *provider* sia effettivamente venuto a conoscenza del fatto che l'informazione è illecita e non si sia attivato per impedire l'ulteriore diffusione della stessa».

Più precisamente, il giudice ha ritenuto non indispensabile un ordine dell'autorità competente per procedere alla rimozione dei contenuti illeciti[95]: l'obbligo sussiste semplicemente «per effetto di una conoscenza acquisita *aliunde*, magari in modo specifico e qualificato, come nel caso di denuncia del soggetto cui l'attività o l'informazione si riferisce». Quindi, «pur non essendovi un obbligo di controllo preventivo dei contenuti presenti né una posizione di garanzia, sussiste tuttavia un obbligo successivo di attivazione di modo che la responsabilità a posteriori dell'*hosting provider* sorge per non aver ottemperato – come per l'appunto verificatosi nella fattispecie in esame – a una richiesta (diffida) di rimozione dei contenuti illeciti proveniente dalla parte che assume essere titolare dei diritti, ovvero per non aver ottemperato a un ordine dell'autorità, sia essa giurisdizionale o ammi-

[94] Tribunale di Napoli Nord, seconda sezione civile, ordinanza 3 novembre 2016, relativo al procedimento n. 9799/2016 promosso da *Facebook Ireland ltd c. Teresa Giglio* (madre della defunta Tiziana Cantone). Si vedano i commenti di: R. Bocchini (2017), *La responsabilità di Facebook per la mancata rimozione di contenuti illeciti*, in *Giurisprudenza italiana*, n. 3, pp. 632-643; L. Bugiolacchi (2017), *I presupposti dell'obbligo di rimozione dei contenuti da parte dell'*hosting provider *tra interpretazione giurisprudenziale e dettato normativo*, in *Responsabilità civile e previdenza*, n. 2, pp. 536-561; M. Montanari (2017), *La responsabilità delle piattaforme on-line (il caso Rosanna Cantone)*, in *Il diritto dell'informazione e dell'informatica*, n. 2, pp. 254-283.

[95] Il tribunale campano ha ritenuto «non condivisibile l'opinione secondo cui sussisterebbe un obbligo di rimozione solo laddove intervenga un ordine dell'autorità …».

nistrativa, cui si sia rivolto il titolare del diritto per ottenere il medesimo effetto». Spetta al danneggiato provare in giudizio – come avvenuto nel caso di specie – che «il *provider* era, comunque, stato messo a conoscenza del contenuto illecito di un'attività o di un'informazione alla quale dava accesso e che, nonostante ciò, non si sia attivato per darne tempestiva comunicazione all'autorità, né abbia provveduto ad impedire prontamente l'accesso a quel determinato contenuto, avvalendosi del potere di autotutela negoziale di cui avrebbe potuto avvalersi in base al contratto concluso con il destinatario del servizio».

Di conseguenza, non solo *Facebook* avrebbe dovuto attivarsi per impedire l'ulteriore diffusione dei *link* dettagliatamente indicati dalla ricorrente, ma avrebbe dovuto anche «denunciare prontamente il fatto alle autorità competenti, stante il contenuto palesemente diffamatorio e denigratorio anche solo dei commenti e delle immagini presenti nei *links* oggetto di segnalazione». Però, non sussistendo alcun obbligo da parte dei *provider* di verificare in via anticipata il contenuto dei post e dei commenti immessi dagli utenti, non appare di conseguenza configurabile a carico di *Facebook* il dovere di inibire, in via generale, il caricamento sulla sua piattaforma «di ogni video, immagini, notizie o articoli riferiti alla persona della ricorrente», ma solo dei *link* espressamente da lei indicati, in ottemperanza al dovere di controllo "successivo". L'obbligo per il gestore del *social network* di rimuovere i contenuti illeciti, una volta acquisitane la conoscenza in seguito alla diffida presentata dal titolare dei diritti lesi, deriverebbe non solo dall'interpretazione delle norme della direttiva 2000/31/Ce e del d. lgs. n. 70/2003[96], ma anche dalla considerazione che, trattandosi di una lesione dei diritti della personalità, questi ultimi potrebbero risultare irrimediabilmente pregiudicati e non più suscettibili di reintegrazione se si attendesse l'ordine proveniente dalle competenti autorità. Infatti, la lesione di un diritto personalissimo è cosa diversa dalla lesione di un diritto patrimoniale – ad esempio il diritto di utilizzazione economica di un'opera dell'ingegno – per la quale, data la possibilità di reintegrazione economica del diritto leso, il *provider* potrebbe rimanere inerte, per non rischiare le conseguenze, sul piano

[96] In primo luogo, se l'obbligo successivo di rimozione dei contenuti nascesse solo in seguito a un ordine della pubblica autorità, sarebbe stata inutile la previsione di un'autonoma ipotesi di "irresponsabilità" connessa alla non effettiva conoscenza dell'illiceità del contenuto; in secondo luogo, se l'obbligo di attivazione sorgesse solo a seguito di un ordine dell'autorità competente, non si comprenderebbe l'esonero *ex lege* dei *provider* dall'onere di ricercare "attivamente'' fatti o circostanze; infine, l'esclusione normativa della conoscenza acquisita attivamente rende logicamente possibile, *a contrario*, che la consapevolezza dell'illecito possa avvenire "passivamente" da parte del *provider*. Cfr. Bocchini (2017), cit., p. 637.

della responsabilità civile, della rimozione di alcuni contenuti sulla base di una segnalazione che dovesse rivelarsi infondata[97].

È interessante il fatto che, in questa decisione, il giudice non si sia basato sulla scivolosa distinzione – tutta di matrice giurisprudenziale – fra *hosting* passivo e attivo e non abbia quindi fatto discendere la responsabilità di *Facebook* dalla sua presunta appartenenza alla categoria degli *hosting* attivi, la cui attività incide sulla gestione e sull'organizzazione degli contenuti prodotti dagli utenti. Il giudice ha piuttosto messo in evidenza il profilo dell'effettiva conoscenza dell'illecito da parte del *provider*, in qualsiasi modo acquisita, come fonte dell'obbligo di attivazione *ex post* per la rimozione degli Ugc, considerando soprattutto l'elemento della lesione dei diritti della personalità[98].

5. La responsabilità dei motori di ricerca per il trattamento dei dati personali: il caso *Google Spain*

Anche la sentenza con cui nel 2014 la Corte di Giustizia dell'Unione europea ha risposto alla domanda di pronuncia pregiudiziale proposta dal giudice spagnolo rappresenta un caso molto studiato[99]. La dottrina se ne è occupata soprattutto in relazione al cosiddetto "diritto all'oblio", cioè al diritto individuale di richiedere al motore di ricerca la deindicizzazione dei link a siti *web* in cui comparivano notizie a lui riferite, ormai risalenti nel tempo

[97] *Ibid.* Si veda anche M. Gambini (2011), *Gli hosting providers tra doveri di diligenza professionale e assenza di un obbligo generale di sorveglianza sulle informazioni memorizzate*, in *Costituzionalismo.it*, n. 2, p. 12, che sostiene la tesi che sia invece imprescindibile la comunicazione formale da parte dell'autorità pubblica competente. Così anche Bugiolacchi (2017), cit., p. 542: «… ci sembra, al contrario, che proprio la "delicatezza" degli interessi, rispetto ai quali operare il bilanciamento, renda estremamente rischioso lasciare all'*hosting provider* la scelta di esercitare un vero e proprio ruolo censorio nei confronti dei propri utenti, rimuovendo autonomamente contenuti che dovessero essere poi contestati dai terzi che li hanno "caricati", « con buona pace dei diritti costituzionali di libera manifestazione del pensiero … ».

[98] Bocchini (2017), cit., p. 639. Interessante è anche la ricostruzione, offerta dall'Autore alle pp. 640-643, della posizione del *provider* come concorrente con l'utente del servizio in un illecito plurisoggettivo *ex* art. 2055 c. c., poiché le condotte di tutti i concorrenti – sia degli utenti che hanno caricato i contenuti illeciti sia del *provider* che ha reso possibile il caricamento – contribuiscono al verificarsi del danno. Tuttavia, la responsabilità dell'intermediario digitale insorge in un momento successivo rispetto a quella dell'utente che ha caricato i contenuti, e cioè nel momento in cui l'intermediario acquisisce conoscenza dell'illecito; il *provider*, dunque, non potrà rispondere dei danni verificatisi antecedentemente a tale momento.

[99] Corte di Giustizia dell'Unione europea, sentenza 13 maggio 2014, causa C-131/12, *Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (Aepd) e Mario Costeja González*.

e non più attuali[100]. Si è molto dibattuto, dunque, sull'estensione e sui limiti del diritto all'oblio, posto in relazione con il diritto di tutti ad essere informati sui fatti di interesse pubblico, nonché sull'idoneità dei motori di ricerca a effettuare la valutazione delle richieste di deindicizzazione, contemperando correttamente e efficacemente le esigenze individuali ad essere dimenticati e il diritto di cronaca. In questa sede, però, questa sentenza verrà presa in considerazione soprattutto sotto lo specifico profilo del trattamento dei dati personali: un motore di ricerca, che reperisce, organizza e indicizza automaticamente le informazioni diffuse da terzi via Internet, qualora tali informazioni contengano dati personali può essere considerato responsabile del trattamento di tali dati, in quanto ne determina le finalità e gli strumenti? La risposta a questo interrogativo può contribuire, *mutatis mutandis*, a chiarire meglio anche la posizione dei *social network provider* rispetto al trattamento dei dati personali, poiché l'uso massiccio di algoritmi di ricerca

[100] *Ex multis*: D'Arienzo (2015), cit.; Di Ciommo (2014), cit.; Frosini (2014a) e (2014b), cit.; Pietropaoli (2017), cit., partic. pp. 74 ss.; Piroddi (2015), cit.; Riccio (2013), cit.; Sirotti Gaudenzi (2017), cit., partic. pp. 147-157; Stradella (2016), cit., partic. pp. 8-13. Si vedano inoltre: L. Bugiolacchi (2016), *Quale responsabilità per il motore di ricerca in caso di mancata deindicizzazione su legittima richiesta dell'interessato?*, in *Responsabilità civile e previdenza*, n. 2, pp. 571-582; L. De Grazia (2013), *La libertà di stampa e il diritto all'oblio nei casi di diffusione di articoli attraverso Internet: argomenti comparativi*, in *Rivista Aic*, n. 4, pp. 1-9; R. Flor (2015), *Dalla "data retention" al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di Giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive "de jure condendo"*, in G. Resta e V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE Press, pp. 223-253; S. Leucci (2017), *Diritto all'oblio, verità, design tecnologico: una prospettiva di ricerca*, in *MediaLaws. Rivista di diritto dei media*, n. 1, pp. 116-125; A. Mantelero (2015), *Il futuro regolamento* EU *sui dati personali e la valenza "politica" del caso Google: ricordare e dimenticare nella* digital economy, in G. Resta e V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE Press, pp. 125-146; R. Pastena (2014), *Internet e privacy: una relazione complicata (A margine della sentenza della Corte di Giustizia del 13 maggio 2014)*, in *Osservatorio Aic*, n. 2, pp. 1-13; O. Pollicino (2015), *Un* digital right to privacy *preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel* reasoning *di Google Spain*, in G. Resta e V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE Press, pp. 7-28; S. Ricci (2015), *Le ricadute penali della sentenza della Corte di giustizia europea sul diritto all'oblio*, in *Cassazione penale*, n. 3, pp. 1247-1254; G. M. Riccio (2015), *Diritto all'oblio e responsabilità dei motori di ricerca*, in G. Resta e V. Zeno Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, TrE-Press, pp. 199-221; G. Scotti (2015), *Dall'habeas corpus all'habeas data: il diritto all'oblio e il diritto all'anonimato nella loro dimensione costituzionale*, in *Diritto.it*, pp. 1-28. Si veda infine: 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, 26 November 2014.

e profilazione che negli ultimi anni i Snp stanno ponendo in essere li rende in qualche modo assimilabili ai motori di ricerca da questo punto di vista.

I fatti sono i seguenti. Nel 2010 il sig. Mario Costeja González, cittadino spagnolo, presentava reclamo all'*Agencia Española de Protección de Datos*(Aepd) contro l'editore del quotidiano *La Vanguardia*, nonché contro *Google Spain* e *Google Inc*. Il reclamante lamentava il fatto che, digitando il suo nome nel motore di ricerca del gruppo Google (*Google Search*), l'elenco di risultati mostrava alcuni link verso pagine del quotidiano *La Vanguardia* del 1998, che facevano riferimento a un pignoramento effettuato nei suoi confronti. A causa di ciò, il sig. Costeja González riteneva di aver subito un pregiudizio della sua reputazione, soprattutto considerando che, anche per via del trascorrere del tempo, la vicenda che lo aveva riguardato nel 1998 era divenuta ormai priva di qualsiasi rilevanza. Egli chiedeva, pertanto, non solo che il quotidiano *La Vanguardia* sopprimesse tali pagine, o almeno ponesse in essere accorgimenti per la protezione dei dati personali che ivi comparivano, ma anche che interrogando il motore di ricerca *Google Search* i link a tali pagine non comparissero più fra i risultati della ricerca (deindicizzazione). L'Aepd ha respinto il reclamo diretto contro *La Vanguardia*, ritenendo che l'editore avesse legittimamente pubblicato le informazioni in questione. Tuttavia, l'Aepd ha accolto il reclamo nei confronti di *Google Spain* e *Google Inc*., chiedendo alle due società di adottare le misure necessarie per rimuovere i dati dai loro indici e per rendere impossibile in futuro l'accesso ai dati stessi. Contro questa decisione *Google Spain* e *Google Inc*. hanno presentato ricorso al giudice (*Audiencia nacional*), che a sua volta ha sottoposto una serie di questioni alla Corte di Giustizia dell'Unione europea.

Dunque, in relazione alla questione della responsabilità per il trattamento dei dati personali, la Corte di Giustizia con molta chiarezza ha statuito che[101], ai sensi della Direttiva 95/46/Ce, «l'attività di un motore di ricerca consistente nel trovare informazioni pubblicate o inserite da terzi su Internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza, deve essere qualificata come "trattamento di dati personali"» qualora tali informazioni contengano dati personali, e che «il gestore di detto motore di ricerca deve essere considerato come il "responsabile" del trattamento», in quanto senz'altro ne determina le finalità e gli strumenti. Ciò è evidente per il fatto che l'attività dei motori di ricerca svolge un ruolo decisivo nella diffusione dei dati personali, in quanto li rende accessibili a qualsiasi utente di Internet che effettui una ri-

[101] Punti da n. 21 a n. 41 della sentenza.

cerca a partire dal nome di una persona, anche a coloro che non avrebbero altrimenti trovato la pagina *web* contenente tali dati. In aggiunta a ciò, grazie ai motori di ricerca gli utenti ottengono un elenco di risultati da cui emerge una visione complessiva e strutturata delle informazioni relative a una persona fisica a partire dal cui nome la ricerca è stata effettuata, definendo un profilo più o meno dettagliato di tale persona. L'effetto dell'ingerenza nei suddetti diritti della persona interessata risulta moltiplicato in ragione del ruolo importante che svolgono Internet e i motori di ricerca nella società moderna, i quali conferiscono carattere ubiquitario alle informazioni contenute in un siffatto elenco di risultati. Il trattamento di dati personali effettuato nell'ambito dell'attività di un motore di ricerca si distingue da e si aggiunge a quello effettuato dagli editori dei singoli siti *web* in cui le informazioni sono pubblicate. Ciò considerato, «nella misura in cui l'attività di un motore di ricerca può incidere, in modo significativo e in aggiunta all'attività degli editori di siti *web*, sui diritti fondamentali alla vita privata e alla protezione dei dati personali, il gestore di tale motore di ricerca quale soggetto che determina le finalità e gli strumenti di questa attività deve assicurare, nell'ambito delle sue responsabilità, delle sue competenze e delle sue possibilità, che detta attività soddisfi le prescrizioni della direttiva 95/46, affinché le garanzie previste da quest'ultima possano sviluppare pienamente i loro effetti e possa essere effettivamente realizzata una tutela efficace e completa delle persone interessate, in particolare del loro diritto al rispetto della loro vita privata».

A proposito dell'equiparazione fra motore di ricerca e titolare del trattamento dei dati risultano assai significative – e parzialmente in contrasto con la decisione finale della Corte – le conclusioni dell'Avvocato generale Niilo Jääskinen presentate il 23 giugno 2013[102]. L'Avvocato ha sottolineato che «le ampie definizioni delle nozioni di dati personali, trattamento dei dati personali e responsabile del trattamento sono atte a coprire una serie mai così ampia di nuove situazioni di fatto legate all'evoluzione tecnologica. Ciò è dovuto alla circostanza che la maggior parte, se non la totalità, dei siti Internet e dei file accessibili loro tramite contengono dati personali, come i nomi di persone fisiche viventi. Questo impone alla Corte di applicare una regola di ragionevolezza, ossia il principio di proporzionalità, nell'interpretare l'ambito della direttiva, al fine di evitare conseguenze giuridiche irrazionali ed eccessive»[103]. Dunque, l'Avvocato ha contestato l'assunto in base al quale il motore di ricerca possa essere considerato alla stregua del titolare del trattamento dei dati. Infatti, a suo giudizio,

[102] De Grazia (2013), cit.
[103] Punto n. 30 della sentenza.

«l'economia generale della direttiva, la maggior parte delle sue versioni linguistiche e gli obblighi individuali da essa imposti al responsabile del trattamento si basano sull'idea della *responsabilità del responsabile del trattamento* riguardo ai dati *personali* trattati, nel senso che il *responsabile del trattamento* è consapevole dell'esistenza di una categoria definita di informazioni che corrispondono a dati personali e intende trattare tali informazioni proprio *in quanto* dati personali»[104]. Invece, «il fornitore di servizi di motore di ricerca su Internet che offre semplicemente uno strumento di localizzazione delle informazioni non esercita alcun controllo sui dati personali contenuti in pagine *web* di terzi. Il fornitore di servizi è "consapevole" dell'esistenza di dati personali unicamente nel senso che, sotto un profilo statistico, è probabile che le pagine web contengano dati personali»[105]. Tra l'altro, la tesi dell'equiparazione fra motore di ricerca e responsabile del trattamento cozzerebbe con il fatto che, qualora il trattamento riguardasse dati sensibili, il motore di ricerca – ammesso e non concesso che possa esserne a conoscenza – dovrebbe chiedere il consenso scritto della persona cui i dati si riferiscono[106]. Le uniche due eccezioni in base alle quali il motore di ricerca potrebbe essere considerato responsabile del trattamento dei dati personali, a giudizio dell'Avvocato, riguarderebbero la decisione di non rispettare i codici di esclusione relativamente ai contenuti della memoria *cache* oppure di non aggiornare una pagina web nella propria memoria cache nonostante il sito web gliene abbia fatto richiesta[107].

Queste riflessioni, sebbene non accolte dalla Corte di Giustizia nella decisione finale, potrebbero prestarsi, se applicate ai gestori dei *social network*, a convalidare la tesi della loro irresponsabilità: in base a questo ragionamento, infatti, non si potrebbe dare per scontato che i *social network provider* siano a conoscenza che i propri utenti stiano trattando dati personali o sensibili. Questa ricostruzione contrasta però con due considerazioni. La prima è che, a differenza dei motori di ricerca, i *social network provider* chiedono esplicitamente ai loro utenti di consentire il trattamento dei dati personali e, anzi, li invitano a regolare le impostazioni sulla *privacy* nel modo che preferiscono; quindi, sono gli stessi Snp a qualificarsi come titolari del trattamento dei dati personali. Il trattamento dei dati personali, infatti, costituisce la stessa *raison d'être* dei *social network* e non, come nel

[104] Punto n. 82.

[105] Punto n. 84.

[106] Punto n. 90.

[107] Punto n. 93. In altre parole, stante il fatto che i proprietari dei siti possono inserire dei codici di esclusione per evitare che alcuni contenuti siano oggetto di indicizzazione da parte del motore di ricerca, quest'ultimo potrebbe però ignorare l'applicazione di tali strumenti o non aggiornare il contenuto della memoria, incorrendo pertanto in responsabilità.

caso dei motori di ricerca, un accadimento che si verifica "per caso" nel momento in cui si aggregano e si rendono visibili dei *link* ad altri siti. I dati personali sono inoltre contenuti nelle pagine *web* a disposizione di ogni utente del *social network*, e non (o non solo) in siti esterni che il *social network* si limita a rendere visibili attraverso *link*; sono quindi dati personali trattati all'interno del *social network* stesso.

La seconda considerazione è che l'Avvocato Jääskinen non tiene presente che, per via dell'accurata attività di profilazione degli utenti che tanto i motori di ricerca quanto i *social network* effettuano, non è sostenibile la tesi che il *provider* non sia a conoscenza del trattamento dei dati personali. Certamente, la profilazione avviene in modo automatico, attraverso algoritmi, ma da tali algoritmi non si ricavano solo dati statistici, bensì informazioni relative alla personalità di singoli individui, ai quali viene destinata pubblicità mirata. Questa attività costituisce il *core business* di molti intermediari digitali – fra cui motori di ricerca e Snp – poiché consente di ricavare profitto. Risulta dunque evidente l'illogicità di una ricostruzione per cui un soggetto che fa del trattamento dei dati personali l'elemento portante della sua attività non sia poi considerato alla stregua del titolare (o almeno del responsabile) del trattamento dei dati. Il punto è che il ragionamento dell'Avvocato Jääskinen non poteva ovviamente tenere conto della distinzione fra "titolare" e "responsabile" del trattamento prefigurata dal regolamento (Ue) 2016/679: titolare è colui che effettua il trattamento determinandone finalità e mezzi (ad esempio, il Snp che svolge attività di profilazione degli utenti al fine di indirizzare loro pubblicità mirata), mentre responsabile è colui che effettua il trattamento per conto del titolare (cioè il Snp che memorizza e trasmette i dati degli utenti all'unico fine di consentire le interazioni fra gli utenti stessi): in entrambi i casi, con l'entrata in vigore del regolamento Ue il gestore della piattaforma di *social networking* non potrà sfuggire alle responsabilità connesse al suo ruolo.

Rispetto agli altri profili della sentenza, che appaiono meno rilevanti ai fini di questa trattazione, e per i quali si rimanda piuttosto alla copiosa letteratura[108], la Corte ha stabilito l'applicabilità della direttiva 95/46/Ce a *Google*, pur avendo la società sede negli Stati Uniti. Infatti, «qualora il gestore di un motore di ricerca apra in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti da tale motore di ricerca e l'attività della quale si dirige agli abitanti di detto Stato membro», il trattamento dei dati personali deve considerarsi effettuato all'interno di uno Stato membro dell'Unione. La Corte ha quindi accolto la tesi per cui il trattamento di dati personali realizzato da un

[108] Vedi nota n. 99.

motore di ricerca avente uno stabilimento in uno Stato membro (nella fattispecie, *Google Spain*) è effettuato «nel contesto delle attività dello stabilimento del responsabile del trattamento» in tale Stato membro, qualora esso sia destinato a garantire la promozione e la vendita di spazi pubblicitari che servono a rendere economicamente redditizio il servizio offerto dal motore di ricerca, e tale motore «è altresì lo strumento che consente lo svolgimento di dette attività»[109].

Ciò definito, la Corte ha esaminato la questione centrale, e cioè se «il gestore di un motore di ricerca sia obbligato a sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei *link* verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine sia di per sé lecita»[110]. *In primis*, la Corte ha ribadito alcuni punti fermi: che la persona interessata ha diritto di opporsi al trattamento dei dati; che la domanda va rivolta al responsabile del trattamento (nella fattispecie, al motore di ricerca); che quest'ultimo deve procedere ad un esame della fondatezza delle richieste e, se del caso, porre fine al trattamento dei dati; che, infine, qualora il responsabile del trattamento non dia seguito a tali domande, la persona interessata può adire l'autorità di controllo o l'autorità giudiziaria; che quest'ultime «possono ordinare al suddetto gestore di sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei *link* verso pagine *web* pubblicate da terzi e contenenti informazioni relative a tale persona, senza che un'ingiunzione in tal senso presupponga che tale nome e tali informazioni siano, con il pieno consenso dell'editore o su ingiunzione di una delle autorità sopra menzionate, previamente o simultaneamente cancellati

[109] Punti da n. 42 a n. 60 della sentenza. Questo aspetto è stato particolarmente considerato in dottrina da Piroddi (2015), cit. Ulteriori considerazioni, soprattutto in relazione all'applicazione territoriale delle norme nazionali di attuazione della direttiva 95/46 sulla tutela dei dati personali, in G. Caggiano (2015), *L'interpretazione del criterio di collegamento del "contesto delle attività di stabilimento" dei responsabili del trattamento dei dati personali*, in G. Resta e V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE Press, pp. 43-61. La questione è destinata ad essere in buona parte superata dal momento in cui entrerà in vigore il regolamento Ue n. 2016/679, che si applicherà anche i soggetti (titolari o responsabili del trattamento dei dati) stabiliti fuori dall'Unione europea, se il trattamento concerne i dati personali di coloro che si trovano nell'Unione europea oppure l'offerta di beni o servizi nel territorio dell'Unione oppure il monitoraggio di comportamenti di soggetti che si trovano all'interno dell'Unione (art. 3 del regolamento).

[110] Punti n. 62 e seguenti (fino a n. 88) della sentenza.

dalla pagina web sulla quale sono stati pubblicati»[111]. Dunque la deindicizzazione dei *link* non necessariamente deve andare di pari passo con la cancellazione delle informazioni dai siti che le contenevano, proprio perché il trattamento dei dati personali da parte del motore di ricerca è indipendente da quello effettuato da altri *content provider*; tanto più che il trattamento dei dati effettuato da un editore di una pagina *web* contenente informazioni personali potrebbe essere effettuato «esclusivamente a scopi giornalistici», beneficiando così, a norma dell'art. 9 della direttiva 95/46/Ce, di deroghe alle prescrizioni dettate da quest'ultima.

Ultima questione su cui la Corte si è pronunciata[112] è quella dell'estensione del cosiddetto "diritto all'oblio". In altre parole, se è legittimo che l'interessato inoltri al motore di ricerca la domanda di deindicizzazione a motivo del fatto che le informazioni personali rese visibili da motore di ricerca possono arrecarle pregiudizio o comunque hanno perso rilevanza per via del trascorrere del tempo. Con questa domanda si pongono in realtà due diversi quesiti: se l'interessato possa rivolgersi direttamente al motore di ricerca invece che al soggetto che ha pubblicato l'informazione *online* e se il presupposto della domanda possa essere costituito dalla considerazione che la divulgazione arrechi pregiudizio o dal desiderio che le informazioni siano dimenticate[113]. In realtà, l'espressone "diritto all'oblio" utilizzata dalla Corte stessa non è del tutto pertinente rispetto al *petitum*. Infatti, è stato giustamente osservato che la richiesta di deindicizzazione rivolta al motore di ricerca riguarda in realtà non «il diritto dell'interessato a "scomparire" dal *web*, bensì […] una posizione giuridica differente, collegata alla semplice riduzione di visibilità dell'informazione presente in rete»[114]. Peraltro, può apparire criticabile la scelta di aver onerato il motore di ricerca del compito di valutare le richieste di deindicizzazione senza che alcuna attività di rimozione dei contenuti venga richiesta, invece, al titolare del "sito sorgente"[115]. Senza contare che, in caso di affrettata e ingiustificata deindicizzazione da parte del motore di ricerca «il titolare del sito sorgente, o comunque l'*uploader* dell'informazione, potrebbe lamentare, una lesione della propria libertà di manifestazione del pensiero, nonché una

[111] Punto n. 82 della sentenza.

[112] Punti da n. 89 a n. 99 della sentenza.

[113] Finocchiaro (2015), cit., p. 36.

[114] S. Sica e V. D'Antonio (2015), *La procedura di de-indicizzazione*, in G. Resta e V. Zeno Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, TrE-Press, pp. 147-176.

[115] Bugiolacchi (2016), cit., p. 572.

"perdita di visibilità" della pagina *web* sorgente, conseguente proprio alla deindicizzazione[116].

Comunque, la Corte ha statuito che il semplice interesse economico del gestore del motore di ricerca al trattamento dei dati non può giustificare eventuali dinieghi alla deindicizzazione, considerando che per via di tale trattamento l'interessato può subire ingerenze potenzialmente molto gravi nella sua vita privata. Invece, la richiesta dell'interessato dovrà essere accolta ogni qual volta il trattamento dei dati risulti incompatibile con i presupposti della direttiva n. 95/46/Ce; tale incompatibilità può derivare «dal fatto che tali dati siano inesatti, ma anche segnatamente dal fatto che essi siano inadeguati, non pertinenti o eccessivi in rapporto alle finalità del trattamento, che non siano aggiornati, oppure che siano conservati per un arco di tempo superiore a quello necessario, a meno che la loro conservazione non si imponga per motivi storici, statistici o scientifici»[117]. Dunque, il diritto di ottenere la cancellazione va ponderato ed esercitato in ragione delle caratteristiche dei dati costituite dall'adeguatezza, dalla pertinenza o dalla non pertinenza del trattamento rispetto alle finalità[118]. Inoltre, la Corte ha affermato, come principio generale, che i diritti tutelati dagli artt. 7 e 8 della Carta europea dei diritti fondamentali (la protezione della vita privata e dei dati personali) prevalgano non soltanto sull'interesse economico del gestore del motore di ricerca – e su questo *nulla quaestio* – ma anche sull'interesse pubblico ad accedere a informazioni riguardanti una specifica persona, a meno che il ruolo ricoperto da tale persona nella vita pubblica non giustifichi l'ingerenza nei suoi diritti fondamentali. Ora, che il conflitto fra diritto alla riservatezza e diritto all'informazione debba essere risolto, *in linea di principio* e non in base a valutazioni caso per caso, automaticamente a favore del primo è opinione che a qualcuno appare non condivisibile[119].

A questo particolare aspetto viene data particolare rilevanza nelle conclusioni dell'Avvocato generale Niilo Jääskinen presentate il 25 giugno 2013[120]: la direttiva europea non prevedrebbe un diritto generale all'oblio che, in base a preferenze personali, possa permettere al soggetto interessato

[116] *Ibid.*

[117] Punto n. 92 della sentenza.

[118] Finocchiaro (2015), cit., p. 37. Però, se l'oggetto della cancellazione sono i *link* aggregati dal motore di ricerca, e se le finalità del trattamento sono quelle previste dal motore di ricerca (cioè facilitare l'accesso alle informazioni per gli utenti di Internet, migliorare l'efficacia della diffusione delle informazioni su Internet, consentire diversi servizi della società dell'informazione), allora è in rapporto ad esse che va effettuata la valutazione sull'adeguatezza, la pertinenza o la non pertinenza dei dati ed e assunta eventualmente la decisione di deindicizzare.

[119] Stradella (2016), cit., p. 10.

[120] In proposito: De Grazia (2013), cit., p. 6 ss.; Flor (2015), cit., p. 244.

di limitare o di impedire la diffusione di dati personali che egli non desidera rendere più accessibili; i criteri da applicare dovrebbero invece essere individuati nello scopo del trattamento e negli interessi da questo tutelati, bilanciati con quelli della persona interessata[121].

Per concludere il ragionamento della Corte, occorre tenere presente la prevalenza dei diritti fondamentali di cui agli artt. 7 e 8 della *Carta dei diritti fondamentali dell'Unione europea* non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse del pubblico a reperire le informazioni in occasione di una ricerca concernente il nome della persona interessata[122]. Tuttavia, tale prevalenza viene meno «qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, mediante l'inclusione summenzionata, all'informazione di cui trattasi»[123]. Se ne desume, dunque, che la rilevanza dell'informazione ai fini della libertà

[121] A proposito dei parametri che il motore di ricerca dovrebbe applicare per valutare se accogliere o rigettare le domande di deindicizzazione si veda Riccio (2015), cit., p. 213. Scrive l'Autore: «Il primo presupposto, per preservare la presenza del collegamento ipertestuale, è il tempo. Ma si tratta, evidentemente, di un parametro difficilmente determinabile e, soprattutto, che non può valere per tutte le fattispecie. Il verificarsi di un nuovo accadimento, connesso al precedente per cui si invoca l'oblio, comporta nuovamente attualità dell'informazione; determinati accadimenti cadono più facilmente nei silenzi della memoria, mentre altri colpiscono indefettibilmente l'immaginario collettivo, generando una loro persistenza tra i primi risultati delle ricerche. […] Il secondo parametro individuato dalla Corte fa riferimento al ruolo ricoperto dal soggetto nella vita pubblica. Si tratta, ancora una volta, di un'affermazione (forse necessariamente) generica, che però non tiene conto delle modifiche che internet ha realizzato sul piano sociale. Da decenni si discute dell'affievolimento della dimensione dicotomica pubblico/privato: con la diffusione dei nuovi media e la parcellizzazione dei canali di comunicazione (*social network*, televisioni satellitari, ecc.) quali sono le figure pubbliche? Una persona che non ha accesso ai canali televisivi o alla carta stampata, ma che ha diecimila *follower* su *Twitter*, acquista il rango di figura pubblica?».

[122] Secondo Pollicino (2015), cit., p. 18, l'accento posto dalla Corte sugli articoli 7 e 8 della Carta ha l'effetto di indebolire il suo ragionamento. Infatti, questo ragionamento trascura il fatto che gli obblighi posti in capo al responsabile del trattamento dei dati derivano dalla direttiva europea e, se applicati al gestore di un motore di ricerca, di snaturare profondamente il modello di *business* di questi operatori. Inoltre, se anche i motori di ricerca sono considerati responsabili della definizione degli strumenti e delle finalità del trattamento, può sorgere il dubbio che anch'essi debbano ottenere previamente il consenso dell'interessato. A p. 19 l'Autore chiarifica che «una cosa è un trattamento illecito di dati personali, rispetto al quale i rimedi sono contemplati dalla direttiva, altra è il trattamento senz'altro lecito di dati che l'interessato manifesti l'interesse a non vedere più diffusi in modo incondizionato, che corrisponde specificamente al diritto all'oblio. I due piani paiono confondersi nell'esame della Corte».

[123] Punto n. 97 della sentenza.

di cronaca, in quanto di interesse pubblico e di utilità sociale, possa essere addotta quale motivazione del rifiuto di deindicizzazione.

Certamente, «lascia perplessi la scelta di rimettere al gestore del motore di ricerca, quindi ad un soggetto privato che segue le logiche di mercato e, per sua stessa natura, difetta dei requisiti di neutralità ed imparzialità, il delicato compito di decidere in merito alle richieste di deindicizzazione dei dati»[124]. Infatti, è il responsabile del trattamento che, nel processare la richiesta, deve ponderare gli interessi in conflitto, considerando le inevitabili ripercussioni dell'esercizio del diritto alla cancellazione (o del diritto di opposizione) sul legittimo interesse degli utenti di Internet ad avere accesso alle informazioni, ricercando il giusto equilibrio tra tale interesse e i diritti fondamentali della persona[125].

Inoltre, non bisogna trascurare il fatto che l'assenza di confini geografici e nazionali in Internet rende facilmente aggirabili i principi affermati dal giudice europeo[126]. Ad esempio, i *link* che *Google* ha deindicizzato per gli utenti europei possono essere reperiti utilizzando le pagine americane del motore di ricerca, poiché al di fuori del territorio europeo *Google* non è obbligato a rispettare la sentenza della Corte di Giustizia (almeno fino all'entrata in vigore del nuovo regolamento europeo sulla protezione dei dati personali). Per lo stesso principio, subito dopo la sentenza *Google Spain* è stato attivato il servizio *Hidden From Google*[127] che, attraverso un *server* ubicato fuori dall'Unione europea, cataloga i risultati deindicizzati da *Google*, aggiornando la lista man mano che *Google* accoglie le richieste degli utenti desiderosi di esercitare il proprio diritto all'oblio.

Va rilevata una discrasia fra questa sentenza della Corte di Giustizia dell'Unione europea e quella della Corte di Cassazione italiana, di poche settimane precedente, che ha deciso definitivamente del caso *Google c. Vividown*: «comparando la posizione delineata per il motore di ricerca nelle

[124] D'Arienzo (2015), cit., p. 5.

[125] Sui nodi critici della procedura messa in atto da *Google* per vagliare e dare seguito alle richieste di deindicizzazione si veda Riccio (2015), cit., e Pietropaoli (2017), cit., pp. 76 ss., che rileva come l'accoglimento da parte di *Google* di una richiesta di deindicizzazione non preveda alcun contradditorio e non abbia alcuna evidenza pubblica, mentre la decisione di *Google* di respingere la richiesta investe le autorità pubbliche del compito di procedere a una sorta di "secondo grado" di giudizio. Sugli aspetti tecnici e procedurali della deindicizzazione si veda, oltre a Sica e D'Antonio (2015), cit., anche C. Comella (2015), *Indici, sommari, ricerche e aspetti tecnici della "de-indicizzazione"*, in G. Resta e V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE Press, pp. 177-198.

[126] Di Ciommo (2014), cit., pp. 1112-1113. Così anche Riccio (2015), cit., p. 212.

[127] La pagina http://hiddenfromgoogle.com, per la verità non risulta più accessibile. È invece tuttora accessibile il profilo *Twitter* associato a *Hidden From Google* (https://-twitter.com/hiddengoogle).

due sentenze, emerge piuttosto chiaramente una discrasia, sulla scorta della quale, in un caso, al motore di ricerca si è imposto un *facere*, mentre, nell'altro, si è giustificata la sua posizione di neutralità apparente rispetto a contenuti che erano stati comunque trattati»[128]. Se si considera che nel caso *Google Spain* i dati personali di cui si chiede la rimozione si presumono contenuti in siti *web* equiparabili a testate giornalistiche, mentre nel caso *Google c. ViviDown* si trattava di *user-generated content*, si potrebbe giungere alla paradossale conclusione che un *provider* (nella fattispecie, un motore di ricerca) debba essere considerato "titolare" del trattamento dei dati personali quando questi dati provengono da soggetti comunque tenuti, a loro volta, al rispetto della normativa sulla *privacy*, mentre il medesimo *provider* non possa essere considerato titolare del trattamento quando i dati personali diffusi attraverso i servizi da esso prestati siano presenti in *user-generated content*, quindi provenienti da soggetti che potrebbero godere della *household exemption*[129].

6. *Excursus*: il rapporto fra libertà di cronaca e diritto all'oblio nella giurisprudenza della Corte di Cassazione

Questo tema rappresenta una digressione rispetto al filo conduttore di questa ricerca, che è costituito dai diversi profili di responsabilità degli intermediari digitali. Tuttavia, poiché nel paragrafo precedente si è accennato al "diritto all'oblio", che è menzionato nel regolamento Ue n. 2016/679 e che costituisce il *thema decidendum* nella sentenza della Corte di Giustizia Ue su *Google Spain*, può risultare utile spendere qualche parola per delineare brevemente l'atteggiamento delle corti nazionali – in particolare del giudice di legittimità – a tale proposito.

Nella ricorrente giurisprudenza della Cassazione, l'espressione "diritto all'oblio" si riferisce essenzialmente al diritto individuale a non vedere continuamente riproposte dai mezzi di comunicazione notizie riferite alla propria persona relative a fatti di cronaca accaduti tempo addietro, dal momento che tali notizie non sono più di interesse pubblico e la loro ripubblicazione non è di utilità sociale. In altre parole, è il diritto ad essere dimenticati quando il trascorrere del tempo rende la notizia non più attuale, esaurendo l'interesse pubblico di conoscenza per quel fatto. Il diritto all'oblio sorge dunque a tutela della reputazione di un soggetto e può essere sacrificato soltanto nel caso in cui, per qualche ragione oggettiva, l'interesse pubblico

[128] Passaglia (2016), cit., p. 341.
[129] *Ibid.*

per quella notizia si risvegli. Oltre a questo profilo relativo al diritto all'oblio, connesso essenzialmente al trascorrere del tempo, la giurisprudenza italiana ha considerato anche un altro profilo, cioè il diritto alla contestualizzazione dell'informazione, in modo da non vedere travisata la propria immagine sociale.

In entrambe le accezioni, il bene giuridico tutelato è quello dell'identità personale, fondato sull'art. 2 Cost., che la Corte di Cassazione (sentenza 22 giugno 1985, n. 3769) ha definito in questi termini: «Ciascun soggetto ha interesse, ritenuto generalmente meritevole di tutela giuridica, di essere rappresentato, nella vita di relazione, con la sua vera identità, così come questa nella realtà sociale, generale e particolare, è conosciuta o poteva essere conosciuta con l'applicazione dei criteri della normale diligenza e della buona fede soggettiva; ha, cioè, interesse a non vedersi all'esterno alterato, travisato, offuscato, contestato il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale ecc. quale si era estrinsecato od appariva, in base a circostanze concrete ed univoche, destinato ad estrinsecarsi nell'ambiente sociale». Secondo la medesima pronuncia, l'identità personale rappresenta «una formula sintetica per contraddistinguere il soggetto da un punto di vista globale nella molteplicità delle sue specifiche caratteristiche e manifestazioni (morali, sociali, politiche, intellettuali, professionali, ecc.), cioè per esprimere la concreta ed effettiva personalità individuale del soggetto quale si è venuta solidificando od appariva destinata, in base a circostanze univoche, a solidificarsi nella vita di relazione»[130].

La terza sezione civile della Corte di Cassazione, nella sentenza n. 3679 del 1998, ha per la prima volta riconosciuto il diritto all'oblio come nuovo e specifico profilo del diritto alla riservatezza, e cioè come «giusto interesse di ogni persona a non restare indeterminatamente esposta ai danni ulteriori che arreca al suo onore e alla sua reputazione la reiterata pubblicazione di una notizia in passato legittimamente divulgata»; tuttavia «quando il fatto precedente per altri eventi sopravvenuti ritorna di attualità, rinasce un nuovo interesse pubblico all'informazione – non strettamente legato alla stretta contemporaneità fra divulgazione e fatto pubblico – che si deve contempe-

[130] Sull'identità personale si vedano: S. Niger (2008), *Il diritto all'identità personale*, in G. Finocchiaro (a cura di), *Diritto all'anonimato: anonimato, nome e identità personale*, Padova, Cedam, pp. 113-129; G. Pino (2006), *Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, Giuffrè, pp. 257-321; E. C. Raffiotta (2010), *Appunti in materia di diritto all'identità personale*, in *www.forumcostituzionale.it*; V. Zeno-Zencovich (1993), *Voce: identità personale*, in *Digesto delle discipline privatistiche*, vol. IX, Torino, Utet, pp. 294-315.

rare con quel principio, adeguatamente valutando la ricorrente correttezza delle fonti di informazione».

Da allora, per un lungo periodo le pronunce giurisprudenziali in tema di diritto all'oblio hanno riguardato perlopiù casi di persone che, essendo state protagoniste molto tempo addietro di fatti di cronaca (spesso giudiziaria) di cui si erano occupati i tradizionali mezzi di comunicazione, rivendicavano il diritto a che tali notizie non venissero più riproposte. In altre parole, l'insorgenza del diritto ad essere dimenticati veniva collegata essenzialmente al decorso del tempo, per via della quale l'interesse pubblico e l'utilità sociale di talune notizie era scemata.

Nella sentenza 25 giugno 2004, n. 11864, la Corte di Cassazione (prima sezione civile) ha ricondotto il diritto all'oblio nell'ambito dei diritti della personalità: il diritto all'oblio salvaguarda la proiezione sociale dell'identità personale, l'esigenza del soggetto di essere tutelato dalla divulgazione di informazioni (potenzialmente) lesive in ragione della perdita di attualità delle stesse, sicché il relativo trattamento viene a risultare non più giustificato ed anzi suscettibile di ostacolare il soggetto nell'esplicazione e nel godimento della propria personalità. Questa ricostruzione si fonda sul principio per cui la libera manifestazione del pensiero – e quindi il diritto di cronaca – riconosciuto e tutelato dall'art. 21 Cost. incontri comunque un limite nei diritti inviolabili dell'uomo (art. 2 Cost.) e, in particolare, nel diritto alla pari dignità sociale di ogni cittadino (art. 3 Cost.).

L'utilizzo di Internet per la diffusione di informazioni anche di tipo giornalistico impone di considerare il diritto all'oblio sotto un diverso profilo, poiché l'informazione presente *online* non è cancellata, ma permane disponibile o quanto meno astrattamente disponibile nella Rete. Non si può fare riferimento al tempo trascorso fra l'originaria pubblicazione della notizia e la sua ripubblicazione in un momento successivo, ma al tempo di permanenza dell'informazione in Rete. Si pone quindi l'esigenza di contestualizzare l'informazione, che è rimasta sempre disponibile *online*, adeguandola all'evoluzione storica dei fatti, in modo da non ledere l'integrità dell'identità personale.

Significativa a tale proposito è stata la sentenza della terza sezione civile della Corte di Cassazione 5 aprile 2012, n. 5525, che per la prima volta si è occupata del diritto all'oblio in connessione alla permanenza delle notizie in Internet, cioè nell'archivio *online* di un quotidiano: un personaggio politico, arrestato per corruzione nel 1993 e successivamente prosciolto, lamentava il fatto che gli articoli giornalistici relativi al suo arresto continuassero ad essere associata al suo nome per via dell'indicizzazione dei contenuti operata dai motori di ricerca. Secondo la Corte, anche riguardo a un fatto molto risalente nel tempo può persistere un interesse pubblico di conoscen-

za a distanza di anni, soprattutto nel caso in cui una vicenda passata sia da porre in relazione con nuovi fatti di interesse pubblico; tuttavia, a tutela della reputazione della persona protagonista della notizia, è importante che il titolare del trattamento dei dati provveda ad aggiornare la notizia attraverso «il collegamento della notizia ad altre informazioni successivamente pubblicate concernenti l'evoluzione della vicenda, che possano completare o financo radicalmente mutare il quadro evincentesi dalla notizia originaria»; occorre quindi «garantire la contestualizzazione e l'aggiornamento della notizia già di cronaca oggetto di informazione e di trattamento, a tutela del diritto del soggetto cui i dati pertengono alla propria identità personale o morale nella sua proiezione sociale, nonché a salvaguardia del diritto del cittadino utente di ricevere una completa e corretta informazione», altrimenti «la notizia, originariamente completa e vera, diviene non aggiornata, risultando quindi parziale e non esatta, e quindi sostanzialmente non vera». Dunque, il questo caso la Corte non ha riconosciuto alla persona protagonista delle notizie il diritto all'oblio, ma solo il diritto alla contestualizzazione di tali informazioni. Però, i giudici di legittimità non si sono soffermati su quali dovessero essere le modalità tecniche con cui realizzare in concreto questa contestualizzazione, né hanno chiarito se l'onere di provvedere a ciò spettasse unicamente al quotidiano cui apparteneva l'archivio storico *online* o per qualche verso anche ai motori di ricerca[131].

Poco tempo dopo, con sentenza 26 giugno 2013, n. 16111, la terza sezione civile della Corte di Cassazione si è occupata del caso di una persona che, arrestata nel 1979 per via dell'appartenenza a un gruppo terroristico, aveva scontato la relativa pena e desiderava non essere più accostato, dinanzi all'opinione pubblica, a fatti di terrorismo; tuttavia un quotidiano locale, in relazione alla notizia del ritrovamento di un arsenale di armi appartenute alle Brigate Rosse, aveva pubblicato una foto dell'uomo all'epoca dell'arresto, corredata da nome e cognome e da una sua presunta intervista. La Suprema Corte ha confermato la sentenza della Corte d'Appello, che aveva riconosciuto il diritto all'oblio dell'appellante in relazione a una parte tanto drammatica della sua vita personale, non sussistendo più un interesse attuale alla conoscenza della notizia, e aveva condannato il giornale al risarcimento del danno. Nel fare ciò, la Corte ha affermato il seguente principio di diritto: «In tema di diffamazione a mezzo stampa, il diritto del soggetto a pretendere che proprie, passate vicende personali siano pubblicamente dimenticate (nella specie, c.d. diritto all'oblio in relazione ad

[131] Si veda in proposito il commento di G. Marchetti (2013), *Diritto di cronaca* on-line *e tutela del diritto all'oblio*, in Aa. Vv., *Da Internet ai Social Network. Il diritto di ricevere e comunicare informazioni e idee*, Rimini, Maggioli, pp. 71-90.

un'antica militanza in bande terroristiche) trova il limite nel diritto di cronaca solo quando sussista un interesse effettivo ed attuale alla loro diffusione, nel senso che quanto recentemente accaduto (nella specie, il ritrovamento di un arsenale di armi nella zona di residenza dell'*ex* terrorista) trovi diretto collegamento con quelle vicende stesse e ne rinnovi l'attualità. Diversamente, il pubblico ed improprio collegamento tra le due informazioni si risolve in un'illecita lesione del diritto alla riservatezza, mancando la concreta proporzionalità tra la causa di giustificazione (il diritto di cronaca) e la lesione del diritto antagonista».

Qualche perplessità ha destato la recente sentenza della terza sezione civile della Corte di Cassazione, n. 13161 del 24 giugno 2016, con la quale è stata imposta la cancellazione dagli archivi di un quotidiano locale di una notizia relativa a un fatto risalente al 2008, con la motivazione che – nonostante fosse tuttora in corso un procedimento penale a carico dei protagonisti di tale vicenda e che essa fosse, almeno per la comunità locale, di interesse pubblico – la facile accessibilità e consultabilità di quell'articolo via Internet avesse determinato una lesione del diritto dei ricorrenti alla riservatezza ed alla reputazione. Il direttore del giornale *online*, che aveva mantenuto visibile l'articolo oltre il momento in cui il protagonista della vicenda ne aveva chiesto la rimozione, è stato dunque ritenuto responsabile sul piano civile. Con tale sentenza la Corte sembra aver sancito una "scadenza" del diritto di cronaca quantificabile in due anni e mezzo (tale era stato infatti il tempo intercorso fra la pubblicazione dell'articolo nel marzo 2008 e la richiesta al giornale di cancellare l'articolo, risalente al settembre 2010). Decorso tale lasso di tempo, il diritto alla riservatezza prevarrebbe sul diritto di cronaca e il trattamento dei dati personali, da un dato momento in poi, risulterebbe ingiustificato, essendo «trascorso sufficiente tempo perché le notizie divulgate potessero avere soddisfatto gli interessi pubblici sottesi al diritto di cronaca giornalistico».

È evidente che, qualora venga dato seguito a questa interpretazione basata sul decorso del tempo, vi sarebbero significative ripercussioni sulla libertà di cronaca e sul diritto di tutti ad essere informati. Tuttavia, è innegabile che ad essere censurata, in quanto lesiva del diritto alla riservatezza, non è la pubblicazione, di per sé lecita, bensì la permanenza a tempo indeterminato di notizie errate, non contestualizzate né aggiornate, riferite a vicende e ad episodi di vita trascorsa che non corrispondono all'identità attuale, memorizzate *online* e sempre reperibili tramite i motori di ricerca.

Anche il Garante per la protezione dei dati personali è più volte intervenuto con provvedimenti volti alla tutela del fondamentale diritto all'oblio, accogliendo i motivi per cui gli interessati si sono opposti al trattamento dei

dati. Il numero di questi provvedimenti[132] è cresciuto soprattutto dopo la sentenza della Corte di Giustizia dell'Unione europea nel caso *Google Spain*, perché coloro che non ottengono dal motore di ricerca la richiesta deindicizzazione dei *link* spesso ricorrono al Garante che, valutato il caso concreto in relazione all'attualità e all'interesse pubblico delle notizie, talvolta ordina al motore di ricerca di adempiere a quanto richiesto. In qualche caso, però, le richieste di deindicizzazione non sono state accolte. Per esempio, con provvedimento n. 152 del 31 marzo 2016, il Garante si è opposto alla richiesta di una persona di rimuovere alcuni contenuti digitali che associavano il suo nome a reati di matrice terroristica compiuti fra la fine degli anni Settanta e in primi anni Ottanta, che venivano visualizzati automaticamente attraverso la funzione "completamento automatico" di *Google*: sebbene, infatti, l'*ex* terrorista avesse finito di scontare la pena comminatagli per quei reati, avesse intrapreso un nuovo percorso di vita, non fosse un personaggio pubblico e fosse comunque trascorso tantissimo tempo da quei fatti, il Garante ha ritenuto che «l'attenzione del pubblico è tuttora molto alta su quel periodo e sui fatti avvenuti», che hanno ormai assunto una valenza storica e segnato la memoria collettiva, e che quindi «debba ritenersi prevalente l'interesse del pubblico ad accedere alle notizie in questione».

Fra i provvedimenti più interessanti, antecedenti alla sentenza *Google Spain*, possiamo ricordare quello dell'8 aprile 2009[133], con cui il Garante ha tenuto conto «delle peculiarità del funzionamento della rete Internet che possono comportare la diffusione di un gran numero di dati personali riferiti a un medesimo interessato e relativi a vicende anche risalenti nel tempo – e dalle quali gli interessati stessi hanno cercato di allontanarsi, intraprendendo nuovi percorsi di vita personale e sociale – che però, per mezzo della rappresentazione istantanea e cumulativa derivante dai risultati delle ricerche operate mediante i motori di ricerca, rischiano di riverberare comunque per un tempo indeterminato i propri effetti sugli interessati come se fossero sempre attuali»; di conseguenza il Garante ha ingiunto all'editore di un sito *web* di adottare «ogni misura tecnicamente idonea a evitare che da quel momento le generalità della ricorrente contenute nell'articolo pubblicato *online* oggetto del ricorso siano rinvenibili direttamente attraverso l'utilizzo dei comuni motori di ricerca esterni al proprio sito Internet». Oggi, alla luce della sentenza *Google Spain*, può apparire singolare – nonché tecnicamente di difficile realizzazione – che debba essere l'editore, e non il motore di ricerca, ad adottare le misure idonee alla deindicizzazione dei contenuti.

[132] Alcuni dei quali sono riportati in Sirotti Gaudenzi (2017), cit., pp. 247 ss.
[133] Doc. web n. 1617673.

LA RESPONSABILITÀ "EDITORIALE" DEGLI INTERMEDIARI DIGITALI PER I CONTENUTI DIFFAMATORI PRODOTTI DAGLI UTENTI

1. Analogie e sinergie fra *social network* ed editoria tradizionale

La questione che qui si intende esaminare, con l'ausilio della giurisprudenza delle corti europee e nazionali, è se i gestori delle piattaforme attraverso le quali gli *user-generated content* vengono diffusi possano essere considerati responsabili sul piano civile (responsabilità extracontrattuale) non solo nel caso di violazione dei diritti patrimoniali – ad esempio, i diritti di utilizzazione economica di taluni contenuti digitali – da parte degli utenti, ma anche dei diritti della personalità. In altre parole, se i *provider* possano avere qualche responsabilità per aver ospitato sulle proprie piattaforme, o per non aver rimosso con sufficiente prontezza, contenuti prodotti dagli utenti lesivi della reputazione altrui e considerati dal giudice diffamatori.

È evidente che il ragionamento ruota intorno a due assi: il ruolo effettivamente svolto dal *provider* nell'organizzazione e nella gestione dei contenuti prodotti dagli utenti – cioè, se l'intermediario digitale svolga un ruolo paragonabile a quello di un tradizionale editore, esercitando qualche forma di influenza o di controllo su di essi – e l'*an* e il *quomodo* dell'acquisizione di conoscenza dell'illiceità dei contenuti da parte dell'Isp.

Occorre inoltre valutare se le considerazioni che emergono dai casi giurisprudenziali qui di seguito esaminati possano in qualche modo adattarsi anche allo specifico tipo di intermediari digitali rappresentato dai gestori dei *social network*. Infatti, la commistione fra l'attività svolta dai *social network* e quella tipica degli editori di informazione giornalistica è sempre più evidente. Nel momento in cui i gestori delle piattaforme di *social networking*, profilando i gusti e le preferenze degli utenti, riescono a mettere in evidenza le *news* più interessanti per ciascuno di essi, opportunamente corredate da pubblicità mirata dalla quale il *provider* trae profitto, è difficile non paragonare questa attività a quella tipicamente editoriale. Se poi i *trending feeds* vengono individuati attraverso algoritmi che valorizzano il numero e la qualità delle interazioni fra gli utenti, non può sfuggire come il

gestore della piattaforma *social*, al pari del direttore di una testata giornalistica, contribuisca a distinguere e a mettere in risalto ciò che davvero "fa notizia" nel *mare magnum* dell'informazione. Non a caso, il rapporto presentato dal *Committee on Culture, Science, Education and Media* dell'Assemblea parlamentare del Consiglio d'Europa a gennaio 2017 fa riferimento al fatto che i *social media* che ospitano contenuti *user-generated* (particolarmente *Facebook, Twitter* e *YouTube*), attraverso l'utilizzo di strumenti di ricerca e aggregazione di notizie diffuse da altri media *online*, sono oggi diventati «the primary contact point for users seeking news»[1]. Eppure, «in relazione alla loro natura "informativa", ormai oggettivamente comprovata, i *social network* reagiscono in maniera schizofrenica: da una parte si augurano (economicamente) di divenire il principale luogo di reperimento di *news*, ma nello stesso tempo rifiutano di considerarsi come una *media corporation*»[2].

Sebbene i gestori dei *social media* siano piuttosto omertosi su questo punto, alcuni di essi (ad esempio *Facebook*, *Snapchat* e *Twitter*) possiedono una piccola redazione formata da giornalisti e professionisti del settore, che producono contenuti, curano e selezionano le notizie e colmano le lacune del materiale prodotto dagli utenti[3]. D'altro canto, già da tempo gli editori tradizionali, una volta approdati *online*, hanno iniziato a corredare l'informazione giornalistica di strumenti di interazione *social*, come ad esempio la possibilità per gli utenti di segnalare gli articoli più graditi e di arricchirli con propri commenti. Inoltre, oggi i tradizionali editori di notizie possono sviluppare sinergie con i *social media* – principalmente, ma non esclusivamente, con *Facebook* – in modo da produrre *instant articles* che possono essere fruiti con immediatezza attraverso le applicazioni mobili della piattaforma *social*, dietro pagamento di un abbonamento[4]. *Facebook*

[1] Assemblea Parlamentare del Consiglio d'Europa, Committee on Culture, Science, Education and Media, *Online media and journalism: challenges and accountability*, doc. 14428, 9 gennaio 2017, p. 5. Sul ruolo "editoriale" che i motori di ricerca come *Google*, ma anche dei *social network* come *Facebook*, svolgono attraverso l'utilizzo di algoritmi, come pure sulla necessità di rendere il funzionamento di tali algoritmi più trasparente, si veda M. Monti (2017c), *Regolazione, Internet e tecnica: le implicazioni di motori di ricerca e social networks sulla libertà di informazione*, in *Federalismi.it*, n. 24, p. 1-31. Sul ruolo pervasivo di *Facebook* nel sistema dell'informazione si veda E. Bell (2016b), *Facebook is eating the world*, in *Columbia Journalism Review* (www.cjr.org).

[2] Monti (2017c), cit., p. 23.

[3] J. Herrman, *Social Media Finds New Role as News and Entertainment Curator*, in *The New York Times*, edizione *online*, 15 maggio 2016.

[4] A proposito degli *instant articles*, va notato che gli editori tradizionali che scelgono di rendere visibili i loro articoli tramite tale servizio offerto da *Facebook*, in modo che gli articoli possano essere fruiti dagli utenti in modo più veloce e immediato, ottengono il vantaggio di incrementare il numero delle visualizzazioni, ma al prezzo di perdere il controllo del

sta anche iniziando a rendere ben visibili i loghi delle testate giornalistiche nelle sezioni *Trending* e *Search* della piattaforma[5], con l'obiettivo di estendere questa novità a tutti i luoghi in cui le persone possono leggere le notizie attraverso la piattaforma *social*. Inoltre, è in via di implementazione la nuova funzione *Article Context*, che fornisce agli utenti informazioni aggiuntive su un articolo (l'editore, l'autore, l'argomento di cui l'articolo tratta, gli altri articoli correlati o di tendenza e il livello di condivisione su *Facebook*).

In questo modo, attraverso la collaborazione con gli editori tradizionali, i *social media* stanno gradualmente sviluppando strategie per sfruttare a loro vantaggio l'affidabilità e la credibilità di cui gode la stampa, con l'effetto di occupare progressivamente lo spazio appartenuto finora all'editoria. D'altro canto gli editori tradizionali, per fronteggiare la posizione dominante detenuta dai *social media* in termini di volume di traffico e di raccolta pubblicitaria, ricercano con essi alleanze per sfruttare in modo proficuo le nuove opportunità offerte dalla digitalizzazione, nel tentativo di raggiungere un pubblico più ampio e meglio profilato, incrementando così gli introiti derivanti dalla raccolta pubblicitaria[6].

proprio traffico *web*, delegandolo al gestore della piattaforma *social*. Ecco perché *Facebook* – ma anche *Google* – non sono da considerarsi dei semplici aggregatori di notizie, ma dei veri e propri *competitor* nel settore dell'editoria. Si vedano: S. Hubbard (2017a), *Why Fake News Is An Antitrust Problem*, in *www.forbes.com*; S. Hubbard (2017b), *Fake News Is A Real Antitrust Problem*, in *CPI Antritrust Chronicle*, pp. 1-6 (www.competitionpolicyinternational.com). S veda anche G. Pitruzzella (2017), cit., partic. p. 84.

[5] Gli editori possono caricare il proprio logo attraverso la nuova *Brand Asset Library*, che si trova nella loro pagina sotto "strumenti di pubblicazione".

[6] Si veda in proposito S. Baraldi (2016), *Editori e social media: fare informazione nell'era digitale*, in *www.markpr.it*, di cui si riporta qui qualche passaggio: «I *social* diventano parte importante della nuova *collaborative economy* in cui le reti di produzione del valore, incluse le decisioni di *governance*, possono essere esterne all'impresa. È qui che emerge un altro mutamento strutturale che sposta l'attenzione verso i lettori-utenti, verso le interazioni. Verso la rete. Infatti, come sanno bene gli esperti di *marketing* digitale, la parola d'ordine è *share*, condividere. La focalizzazione dall'interno all'esterno (e poi di nuovo all'interno) delle imprese rimescola le nostre convinzioni su che cosa è e come si fa il business digitale. […] La strategia digitale porta a trascendere le singole funzioni aziendali e sembra in grado di ridefinire le modalità con cui soddisfare i bisogni e i desideri dei lettori, oltrepassando i classici confini dei settori preesistenti e collegandosi alle possibilità di cooperazione offerte dalle piattaforme *social*. […] Il digitale trasforma molte regole del gioco. Esso permette alle aziende di specializzarsi non su tutta la catena del valore ma in singole aree, perché consente di aggregare servizi in modo più economico e veloce e una più efficace segmentazione del mercato. Diventa possibile fare quello che fino a ieri era vietato: collaborare con i propri concorrenti anche attraverso uno scambio di dati. Gli editori hanno un sevizio informativo autorevole, credibile rispetto a quello che circola sulla rete e soprattutto sui *social*. In questa logica, che ridisegna la catena di valore, non può sorprendere che i *social media* e gli editori possano trovare un modo per cooperare. È la legge dello *sharing*,

Questi brevi cenni su come sta cambiando il mondo dell'informazione grazie anche ai *social media* evidenziano l'importanza di iniziare a considerare se per caso ai *social network provider* non si possa iniziare ad imputare responsabilità analoghe a quelle dei direttori delle testate giornalistiche o degli editori. In realtà non vi sono finora precedenti giurisprudenziali che abbiano avviato un percorso di questo tipo. Tuttavia, dall'esame di alcune sentenze relative alle responsabilità per diffamazione di alcuni *content provider* (editori di informazione giornalistica) possono essere estrapolate alcune linee di tendenza che, *mutatis mutandis*, possono riguardare anche i *social network*.

2. La Corte di Giustizia dell'Unione europea nel caso *Papasavvas c. O Fileleftheros*

In un unico caso finora la Corte di Lussemburgo si è trovata a dover decidere dell'applicazione delle disposizioni della direttiva 2000/31/Ce relative alla responsabilità dei *provider* a un caso diverso da quelli esaminati nel terzo capitolo di questo libro, che erano tutti relativi alla violazione dei diritti di utilizzazione economica dei contenuti digitali: la questione oggetto della decisione *Papasavvas c. O Fileleftheros*[7] del 2014 ha riguardato, infatti, la responsabilità civile di un *content provider* (un editore di un quotidiano) per diffamazione. Va precisato che la diffamazione non derivava, nel caso di specie, da contenuti *user-generated*, ma da articoli giornalistici scritti da giornalisti professionisti e pubblicati sul quotidiano.

Nel novembre 2010 il sig. Papassavvas, ritenendosi diffamato dal contenuto di alcuni articoli apparsi sia nell'edizione a stampa che in quella *online* del quotidiano nazionale *O Fileleftheros*, è ricorso al giudice per ottenere la rimozione degli articoli lesivi della sua reputazione e il risarcimento dei danni subiti. Il giudice cipriota si è rivolto in via pregiudiziale alla Corte di Giustizia per chiarire le seguenti questioni interpretative: 1) se la normativa nazionale in materia di diffamazione, che incide sulla capacità di fornire servizi d'informazione per via elettronica, possa essere considerata

della condivisione di informazioni, dati, contenuti e altre risorse che possono aumentare di valore se sono inserite in reti *social-mobile*». Sui rapporti sempre più stretti fra editoria e piattaforme di *social media* si veda anche la ricerca pubblicata dal *Columbia Journalism Review* nel 2016: E. Bell (2016a), *Who owns the news consumer: social media platforms or publishers?*, in *Columbia Journalism Review* (www.cjr.org).

[7] Corte di Giustizia dell'Unione europea, *Sotiris Papasavvas contro O Fileleftheros Dimosia Etaireia Ltd e a.,* domanda di pronuncia pregiudiziale, causa C-291/13, sentenza 11 settembre 2014.

una restrizione alla prestazione di servizi d'informazione ai fini dell'attuazione della direttiva 2000/31/Ce; 2) se le disposizioni di tale direttiva in materia di responsabilità degli intermediari digitali si applichino anche alle questioni relative alla responsabilità civile nell'ipotesi di diffamazione, ovvero se si limitino alla responsabilità civile nel caso di operazioni commerciali e contratti con i consumatori; 3) se l'intermediario digitale, nel contesto di un'azione civile per diffamazione, possa invocare a propria difesa le disposizioni della direttiva *e-commerce* relative alla limitazione di responsabilità; 4) se le nozioni di "servizi della società dell'informazione" e di "prestatore di servizi" si applichino anche a servizi di *informazione online* remunerati non direttamente dal destinatario dei servizi, bensì indirettamente grazie alle pubblicità commerciali che appaiono sulla pagina web; 5) se un giornale *online* (accessibile gratuitamente in quanto remunerato dalla pubblicità oppure accessibile a pagamento) debba essere considerato un *hosting provider* o se la sua attività non rientri piuttosto nella categoria del *provider* di *mere conduit* o di *caching*.

Rispetto alla prima questione, la Corte ha stabilito che la direttiva 2000/31/Ce non osta all'applicazione di un regime di responsabilità civile per diffamazione derivante dalla normativa nazionale. Per quanto riguarda la seconda questione, la Corte ha affermato che i limiti alla responsabilità civile previsti agli articoli da 12 a 14 della direttiva sul commercio elettronico sono applicabili anche nel contesto di una controversia tra privati vertente sulla responsabilità civile per diffamazione, qualora ricorrano le condizioni previste da detti articoli. Circa la terza questione, la Corte ha precisato che i suddetti articoli della direttiva *e-commerce* non consentono direttamente al prestatore di un servizio della società dell'informazione di opporsi alla proposizione di un'azione giudiziaria di responsabilità civile nei propri confronti e, conseguentemente, all'adozione di misure provvisorie da parte di un giudice nazionale, ma possono essere invocati dal prestatore conformemente alle disposizioni di diritto nazionale che ne garantiscono la trasposizione o, in mancanza di esse, ai fini dell'interpretazione conforme del diritto nazionale. Alla quarta questione la Corte ha risposto che la nozione di "servizi della società dell'informazione" e quella di "prestatore" di tali servizi si applicano ai servizi che forniscono informazioni *online*, indipendentemente dalla provenienza della remunerazione del servizio (se dal destinatario del servizio stesso oppure dalla pubblicità commerciale).

Il punto cruciale, a giudizio della Corte, ruota intorno alla quinta questione, la risposta alla quale rende in qualche modo irrilevanti tutti gli altri quesiti. La Corte, richiamando la sua precedente giurisprudenza, ha ribadito che le deroghe alla responsabilità previste dalla direttiva 2000/31/Ce riguardano esclusivamente i casi in cui l'attività di prestatore di servizi della

società dell'informazione sia di ordine meramente tecnico, automatico e passivo, e che, conseguentemente, il prestatore medesimo non conosca né controlli le informazioni trasmesse o memorizzate. Dunque, ai fini dell'applicabilità delle limitazioni di responsabilità non rileva tanto il fatto che l'accesso al sito del giornale *online* sia gratuito o a pagamento, e nemmeno il fatto che l'editore venga retribuito con i proventi della pubblicità commerciale; ciò che è importante, invece, è accertare nel caso concreto se il prestatore del servizio sia o non sia a conoscenza delle informazioni pubblicate ed eserciti un controllo sulle stesse.

Anche nel caso *Papasavvas c. Fileleftheros*, la Corte di Giustizia è rimasta in linea con la sua precedente giurisprudenza in materia di responsabilità dell'Isp nei casi di violazione dei diritti di proprietà intellettuale: qualunque prestatore di servizi della società dell'informazione soggiace al regime normativo (anche in tema di responsabilità) delineato dalle legislazioni nazionali, purché ciò avvenga nel rispetto delle norme comunitarie finalizzate al buon funzionamento del mercato interno; per quanto riguarda i prestatori di servizi che agiscono come intermediari – quindi solo i prestatori intermediari e non tutti i fornitori di "servizi della società dell'informazione" – si pone l'esigenza di introdurre delle limitazioni di responsabilità di carattere *eccezionale*, proprio in considerazione delle specifiche caratteristiche dei detti servizi; tali limitazioni possono applicarsi a condizione che sia esclusa *ab initio* ogni forma di interazione del prestatore con le informazioni trasmesse o memorizzate[8].

Se ne deduce, sebbene la Corte non lo abbia detto esplicitamente, che l'editore di un quotidiano in versione tanto cartacea quanto *online* sia da considerarsi, in linea di principio, a conoscenza del contenuto degli articoli pubblicati, e quindi non possa beneficiare delle limitazioni di responsabilità previsti per gli *hosting provider* passivi.

3. La giurisprudenza della Corte europea dei diritti dell'uomo sulla responsabilità dell'editore *online* per i contenuti *user-generated*

La giurisprudenza della Corte di Strasburgo in difesa della libertà di espressione, protetta dall'art. 10 della Cedu, è molto ampia[9] e non può esse-

[8] N. Lofranco (2015), *Corte di Appello Milano (Rti/Yahoo) versus Corte di Giustizia (Papasavvas/Fileleftheros). Sulla effettiva portata delle deroghe all'ordinario regime di responsabilità del provider*, in *www.diritto.it*.

[9] Si veda in argomento M. Orofino (2014), *La libertà di espressione tra Costituzione e carte europee dei diritti. Il dinamismo dei diritti in una società in continua trasformazione*, Torino, Giappichelli.

re esaminata nel dettaglio in questa sede. Ne emerge, comunque, una duplice concezione della libertà di espressione: da un lato, la sua valenza di diritto individuale a diffondere e a ricevere informazioni; dall'altro, la sua valenza funzionale al mantenimento di un sistema democratico, come *watchdog* della democrazia[10]. A differenza delle corti nazionali, la giurisprudenza della Corte europea dei diritti dell'uomo è volta ad individuare un minimo comune denominatore nella protezione dei diritti da parte dei diversi Stati aderenti alla Cedu, lasciando a questi ultimi il compito di operare il bilanciamento con altri diritti eventualmente configgenti con quello alla libera manifestazione del pensiero, in base al proprio ordinamento giuridico[11]. In particolare, il bilanciamento è stato sovente operato fra la libertà protetta dall'art. 10 Cedu, intesa non solo come diritto individuale ad esprimersi liberamente, ma anche come interesse collettivo alla circolazione delle informazioni di interesse pubblico, e il diritto individuale alla protezione della vita privata e della reputazione, sancito invece dall'art. 8 Cedu.

Occorre infatti ricordare che l'approccio europeo alla libertà di espressione non esclude in modo assoluto la possibilità che quest'ultima subisca delle limitazioni, purché previste dalla legge e considerate necessarie a garantire la convivenza civile in una società democratica. Così si esprime, infatti, l'art. 10, comma 2, della Cedu, che giustifica l'applicazione di quelle «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». Ogni qual volta, dunque, la Corte di Strasburgo si è trovata a giudicare della compatibilità con la Cedu di misure restrittive della libertà di espressione adottate a livello nazionale, il giudizio è stato incardinato intorno alla valutazione del rispetto del principio di legalità e dell'effettiva necessità (in termini anche di proporzionalità) di tali misure. Analizzando le pronunce della Corte sull'ammissibilità delle restrizioni alla libertà di espressione previste dagli ordinamenti giuridici nazionali, si osserva che «la legittimità delle medesime è valutata con riferimento al requisito della proporzionalità e della necessità, tenendo sempre presente il tipo di comunicazione e il grado di rilevanza che essa ha per lo sviluppo di un corretto processo democratico. Partendo da questa constatazione, è possibile ricostruire una tutela giurisprudenziale a cerchi concentrici, per cui più la comunicazione è vicina al nu-

[10] Ivi, pp. 42-43.
[11] Ivi, pp. 28 e 38.

cleo delle libertà, minori sono le restrizioni ammissibili; più ci si allontana, invece, da questo nucleo, maggiori sono le possibilità per gli Stati di apporre limitazioni»[12].

Nell'ambito della copiosa giurisprudenza in tema di libertà di espressione attraverso i media tradizionali e quelli *online*[13], si è scelto di prendere i considerazione in questa sede tre recenti pronunce accomunate dal fatto che i contenuti illeciti, in quanto lesivi della dignità personale e della reputazione individuale, erano di tipo *user-generated*, consistenti cioè in commenti offensivi prodotti e caricati autonomamente dagli utenti di alcuni siti *web* di informazione giornalistica. Infatti, pur mantenendo fermo il principio della responsabilità dell'editore per eventuali profili illeciti contenuti negli articoli pubblicati, non altrettanto scontata è l'estensione della medesima responsabilità anche ai contenuti dei *post* caricati autonomamente dagli utenti.

Dalla lettura delle tre sentenze considerate qui di seguono emergono quattro criteri che la Corte ha elaborato al fine di risolvere con una qualche coerenza e organicità il conflitto fra libertà di espressione in Rete e tutela della reputazione e della riservatezza individuali[14]: 1) il livello di "protagonismo" del gestore del sito, che può oscillare fra un atteggiamento del tutto neutrale e passivo e uno di coinvolgimento e intervento attivo; 2) le cautele eventualmente predisposte *ex ante* dall'intermediario digitale, come ad esempio strumenti di filtraggio preventivo e di rimozione automatica di contenuti illeciti; 3) l'eventualità che l'identità degli autori dei commenti illeciti sia coperta dall'anonimato, con conseguente eventuale ricaduta dell'a responsabilità sull'intermediario digitale; 4) l'impatto e la proporzionalità delle sanzioni irrogate all'intermediario digitale, in considerazione del suo ruolo e delle sue condizioni economiche, nonché dell'effetto dissuasivo delle sanzioni stesse rispetto alla libera circolazione delle idee attraverso Internet.

3.1. Il caso Delfi

A differenza del caso *Papassavvas*, il caso *Delfi As c. Estonia*[15], di cui si è occupata la Corte europea dei diritti dell'uomo, ha riguardato la respon-

[12] Ivi, p. 52:

[13] Fra cui si ricordano in particolare, con riferimento all'informazione diffusa attraverso Internet: *Times Newspapers Ltd v. The United Kingdom,* 10 marzo 2009, applications nn. 3002/03 e 23676/03; *Mosley v. The United Kingdom*, 10 maggio 2011, application n. 48009/08; *Ahmet Yıldırım v. Turkey*, 18 dicembre 2012, application n. 3111/10.

[14] P. Costanzo (2017), *Quando in internet la Corte di Strasburgo continua a navigare a vista*, in *DPCE On Line*, n. 3, partic. pp. 769-770.

[15] European Court of Human Rights, *Case of Delfi As c. Estonia*, application no. 64569/09: judgement of the First Section, 10 October 2013; judgement of the Grand Cham-

sabilità per diffamazione non di un editore, ma di un portale di informazione giornalistica, che dunque non produce direttamente gli articoli giornalisti che pubblica, ma ricerca e aggrega quelli pubblicati da altri. Per di più, il contenuto diffamatorio non derivava direttamente da un articolo giornalistico, ma da alcuni commenti ad un articolo, prodotti e caricati direttamente dagli utenti (*user-generated content*). Per queste ragioni, il caso di *Delfi* può presentare qualche analogia con l'attività dei *social network*, che segnalano ai propri utenti le notizie che possono risultare per essi più interessanti, in base al loro profilo, e favoriscono l'interazione fra gli utenti anche mediante i commenti apposti da ciascuno a tali notizie.

Delfi è un grande portale che ricerca e aggrega notizie di attualità pubblicate su organi di informazione *online* in lingue estone e russa. Il portale offre la possibilità agli utenti di rendere pubblici i propri commenti agli articoli, precisando nelle "clausole di utilizzo" che la responsabilità dei contenuti eventualmente illeciti di tali commenti ricade interamente sui loro autori e non sul gestore della piattaforma. Il portale prevede altresì un sistema di *notice-and-take-down*, che permette agli utenti di segnalare i commenti inappropriati, in modo che il gestore della piattaforma possa procedere alla loro rimozione. Coloro che si ritengono diffamati dal contenuto di un commento possono segnalarlo direttamente al gestore della piattaforma, chiedendone l'immediata rimozione. Infine, è in funzione un sistema di censura automatica dei commenti contenenti talune espressioni oscene.

Il caso, poi portato all'attenzione della Corte europea dei diritti dell'uomo, ha avuto origine da un articolo apparso nel 2006 sul portale di notizie *Delfi*, che aveva attratto una significativa quantità di commenti diffamatori postati dagli utenti. Il soggetto diffamato (una compagnia di navigazione) aveva chiesto a *Delfi* la rimozione dei commenti – richiesta che *Delfi* aveva in effetti prontamente soddisfatto – nonché il risarcimento del danno non patrimoniale subito per le circa sei settimane in cui i contenuti diffamatori erano rimasti *online* (nel periodo, cioè, intercorrente fra la prima pubblicazione del commento e la richiesta di rimozione da parte della compagnia di navigazione). *Delfi* aveva replicato che i commenti diffamatori erano stati rimossi immediatamente in applicazione della procedura di

ber, 15 June 2015. Si vedano: M. Bellezza (2013), *Delfi vs. Estonia: la libertà della Rete è davvero in pericolo?*, in *Newsletter Inform@ Digital*, www. portolano.it; F. Buffa (2017), *Responsabilità del gestore di sito Internet*, in *Questionegiustizia.it*; D. Mula (2016), *La responsabilità del portale*, in M. Bianca, A. Gambino e R. Messinetti (a cura di), *Libertà di manifestazione del pensiero e diritti fondamentali*, Milano, Giuffrè, pp. 73-87; R. Nigro (2015), *La responsabilità degli Internet service providers e la Convenzione europea dei diritti umani: il caso Delfi AS*, in *Diritti umani e diritto internazionale*, n. 3, pp. 681-689; G. E. Vigevani (2014), *La responsabilità civile dei siti per gli scritti anonimi: il caso Delfi c. Estonia*, in *www.forumcostituzionale.it*. Si veda inoltre Orofino (2014), cit., pp. 67-70.

notice-and-take-down e che, non avendo il gestore della piattaforma alcuna responsabilità per il contenuto dei commenti postati dagli utenti, non era tenuta a corrispondere il risarcimento. Di conseguenza, la compagnia di navigazione ha citato *Delfi* in giudizio: in primo grado, i giudici estoni avevano escluso la responsabilità di *Delfi*, ma in appello hanno invece stabilito che *Delfi* avesse una responsabilità editoriale anche in riferimento ai commenti postati dagli utenti; infine, nel terzo grado di giudizio, la Corte Suprema estone ha confermato la tesi della responsabilità del gestore della piattaforma, in considerazione sia del controllo che *Delfi* poteva effettivamente esercitare sui commenti degli utenti, sia dell'utilizzazione economica (raccolta pubblicitaria) che *Delfi* faceva dello spazio riservato ai commenti. *Delfi* si è allora rivolta alla Corte europea dei diritti dell'uomo, lamentando il fatto che averle attribuito una responsabilità per contenuti prodotti in realtà dagli utenti della piattaforma rappresentasse una violazione dell'art. 10 della Convezione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (Cedu), e non rientrasse fra le «formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica» di cui al secondo comma dell'articolo in questione[16].

Con decisione del 10 ottobre 2013, la prima sezione della Corte europea dei diritti dell'uomo ha respinto il ricorso di *Delfi*, negando che la decisione del giudice estone avesse rappresentato una violazione all'art. 10 della Cedu. Secondo i giudici di Strasburgo, il portale *Delfi* era in condizione di esercitare il controllo sul contenuto dei commenti postati dagli utenti e quindi avrebbe dovuto prontamente rimuovere i commenti dal contenuto offensivo in virtù del principio di precauzione inerente all'attività professionale di chi svolge attività editoriale[17]; inoltre, per il soggetto diffamato

[16] Art. 10 della Cedu, *Libertà di espressione*: «1. Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza considerazione di frontiera. Il presente articolo non impedisce agli Stati di sottoporre a un regime di autorizzazione le imprese di radiodiffusione, di cinema o di televisione. 2. 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, per la sicurezza nazionale, per l'integrità territoriale o per la pubblica sicurezza, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, per la 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». Sull'interpretazione dell'art. 10 Cedu e sul ruolo della Corte di Strasburgo nella tutela della libertà di espressione si veda Orofino (2014), cit., partic. pp. 35 ss.

[17] Dal punto n. 89 della sentenza: «the applicant company – and not a person whose reputation could be at stake – was in a position to know about an article to be published, to pre-

sarebbe stato eccessivamente oneroso individuare e citare in giudizio l'autore del commento diffamatorio, considerando anche la possibilità che l'autore della diffamazione fosse un utente anonimo (non registrato al sito); infine, l'entità del risarcimento non era assolutamente sproporzionata rispetto al danno subito. Di conseguenza, la Corte ha ritenuto che l'attribuzione al *provider* della responsabilità per diffamazione rappresentasse, nel caso concreto, una restrizione della libertà di espressione proporzionata e giustificata[18].

Successivamente, in seguito al ricorso presentato da *Delfi* alla *Grand Chamber* della Corte europea dei diritti dell'uomo, un'altra sentenza è stata emessa il 15 giugno 2015. La Corte di Strasburgo non ha ritenuto utile approfondire, come aveva fatto la Corte Suprema estone, la differenza fra il ruolo dell'editore di organi di informazione a stampa e quello di un *provider* che gestisce un portale di informazione giornalistica *online*, soffermandosi piuttosto sulla necessità, derivante dalla particolare natura di Internet, di differenziare le responsabilità attribuibili alle due figure[19]. Nel decidere, la Corte ha tenuto preliminarmente in considerazione il fatto che il caso riguardava un soggetto imprenditoriale che svolgeva l'attività di intermediario digitale professionalmente («a large professionally managed Internet news portal run on a commercial basis which published news articles of its own and invited its readers to comment on them»[20]) e non il gestore di qualsiasi sito che pubblica commenti di terze parti senza interferire nei contenuti prodotti dagli utenti, come per esempio un forum o un blog[21]. Così

dict the nature of the possible comments prompted by it and, above all, to take technical or manual measures to prevent defamatory statements from being made public».

[18] Dal punto n. 94 della sentenza: «Based on the above elements, in particular the insulting and threatening nature of the comments, the fact that the comments were posted in reaction to an article published by the applicant company in its professionally-managed news portal run on a commercial basis, the insufficiency of the measures taken by the applicant company to avoid damage being caused to other parties' reputations and to ensure a realistic possibility that the authors of the comments will be held liable, and the moderate sanction imposed on the applicant company, the Court considers that in the present case the domestic courts' finding that the applicant company was liable for the defamatory comments posted by readers on its Internet news portal was a justified and proportionate restriction on the applicant company's right to freedom of expression».

[19] A tale proposito, la Corte ha richiamato la Raccomandazione del Comitato dei Ministri del Consiglio d'Europa agli Stati membri (CM/Rec(2011)7 del 21 settembre 2011), che menzionava la necessità di un «differentiated and graduated approach» fra le diverse figure operanti nel settore dei media, tradizionali e *online*.

[20] Citazione tratta dal punto n. 115 della sentenza.

[21] Dal punto n. 116 della sentenza: « Accordingly, the case does not concern other fora on the Internet where third-party comments can be disseminated, for example an Internet discussion forum or a bulletin board where users can freely set out their ideas on any topics without the discussion being channelled by any input from the forum's manager; or a social

facendo, la Corte ha indirettamente affermato il principio per cui occorre tenere conto del ruolo e della natura dell'intermediario digitale per poterne valutare le effettive responsabilità. Infatti, il fondamento della restrizione della libertà di espressione derivava, nel caso di specie, da un'interpretazione estensiva della legge estone che *Delfi*, date le sue dimensioni e il suo ruolo, avrebbe potuto agevolmente prevedere[22]. Inoltre, sempre in relazione all'effettivo ruolo svolto da *Delfi*, la Corte ha ritenuto ragionevole che a un *provider* che trae profitto dalle inserzioni pubblicitarie collegate ai commenti degli utenti possano essere imposti obblighi più gravosi rispetto a quelli che sarebbe legittimo e proporzionato prevedere in capo a soggetti che non perseguono scopi di lucro[23].

Stabilito che l'attività di *Delfi* non era di natura puramente tecnica e automatica, ma comportava un ruolo attivo nella pubblicazione dei commenti degli utenti[24], e accertata anche l'impossibilità per il soggetto diffamato di individuare tutti gli autori dei commenti diffamatori, avendo alcuni di essi postato il commento in forma anonima, la Corte ha ritenuto compatibile con l'art. 10 della Cedu l'ordine del giudice estone impartito a *Delfi* affinché i commenti diffamatori fossero prontamente rimossi[25], ribadendo che in nessun caso questo potesse essere equiparato a una forma di "censura privata"[26]. Analogamente, il risarcimento richiesto a *Delfi* dal soggetto diffamato in compensazione del danno non patrimoniale non è stato considerato «disproportionate to the breach established by the domestic courts»[27]. Dunque, in conclusione la Corte ha ritenuto che l'art. 10 della Cedu non possa dirsi

media platform where the platform provider does not offer any content and where the content provider may be a private person running the website or a blog as a hobby».

[22] Orofino (2014), cit., p. 68.

[23] Ivi, p. 69.

[24] Dal punto n. 146 della sentenza: « In sum, the Court considers that it was sufficiently established by the Supreme Court that the applicant company's involvement in making public the comments on its news articles on the *Delfi* news portal went beyond that of a passive, purely technical service provider».

[25] Dal punto n. 153 della sentenza: « Consequently, and taking account of the above findings (see paragraph 145) to the effect that the applicant company must be considered to have exercised a substantial degree of control over the comments published on its portal, the Court does not consider that the imposition on the applicant company of an obligation to remove from its website, without delay after publication, comments that amounted to hate speech and incitements to violence, and were thus clearly unlawful on their face, amounted, in principle, to a disproportionate interference with its freedom of expression».

[26] Dal punto n. 157 della sentenza: «Having regard to the fact that there are ample possibilities for anyone to make his or her voice heard on the Internet, the Court considers that a large news portal's obligation to take effective measures to limit the dissemination of hate speech and speech inciting violence – the issue in the present case – can by no means be equated to "private censorship"».

[27] Dal punto n. 160 della sentenza.

violato dal fatto che gli Stati membri impongano ai *provider* obblighi di rimozione di contenuti illeciti che pregiudicano i diritti individuali[28].

La decisione è stata integrata dalla *concurring opinion* dei giudici Raimondi, Karakas, De Gaetano and Kjølbro, allegata alla sentenza. I quattro giudici, pur accogliendo la tesi che l'imposizione al *provider* di obblighi di rimozione dei contenuti illeciti non costituisse una violazione dell'art. 10 della Cedu, hanno voluto altresì precisare che l'eventuale attribuzione di responsabilità al gestore della piattaforma per non aver *prevenuto* l'inserimento di contenuti illeciti – in altre parole, l'attribuzione al *provider* di obblighi di sorveglianza preventiva – avrebbe invece rappresentato un'eccessiva restrizione della sua libertà di espressione. In effetti, suscitando qualche perplessità, la *Grand Chamber* della Corte europea ha mancato di soffermarsi su questo punto, cioè sul fatto che tanto la prassi giurisprudenziale a livello nazionale e di Corte di giustizia dell'Unione europea, quanto una serie di documenti prodotti dalle organizzazioni internazionali[29], escludono decisamente che i *provider* possano essere ritenuti responsabili del controllo *preventivo* dei contenuti prodotti dagli utenti e che gli Stati possano imporre ai *provider* un siffatto obbligo *ex lege*[30]. Questa timidezza della Corte può essere interpretata come segno di una qualche inquietudine per le potenzialità della Rete, da cui è ben difficile rimuovere le informazioni una volta rese pubbliche: dunque, i giudici europei potrebbero dimostrarsi inclini a tollerare imitazioni alla libertà di espressione che probabilmente in ambiente analogico avrebbero giudicato intollerabili[31].

[28] Dal punto n. 162 della sentenza: « Based on the concrete assessment of the above aspects, taking into account the reasoning of the Supreme Court in the present case, in particular the extreme nature of the comments in question, the fact that the comments were posted in reaction to an article published by the applicant company on its professionally managed news portal run on a commercial basis, the insufficiency of the measures taken by the applicant company to remove without delay after publication comments amounting to hate speech and speech inciting violence and to ensure a realistic prospect of the authors of such comments being held liable, and the moderate sanction imposed on the applicant company, the Court finds that the domestic courts' imposition of liability on the applicant company was based on relevant and sufficient grounds, having regard to the margin of appreciation afforded to the respondent State. Therefore, the measure did not constitute a disproportionate restriction on the applicant company's right to freedom of expression. Accordingly, there has been no violation of Article 10 of the Convention».

[29] Fra cui, ad esempio, la Dichiarazione del Comitato dei Ministri del Consiglio d'Europa sulla libertà di comunicazione in Internet (28 maggio 2003) e il Rapporto del Consiglio dei diritti umani delle Nazioni Unite sulla promozione e protezione del diritto alla libertà di opinione e di espressione (Rapporto *Frank La Rue* del 16 maggio 2011).

[30] Nigro (2015), cit.

[31] Vigevani (2014), cit.

I medesimi timori sono stati espressi ancora più chiaramente da un'altra *concurring opinion*, quella del giudice Zupančič, per il quale il modesto risarcimento richiesto a *Delfi* sarebbe assolutamente inadeguato rispetto alla gravità del danno subito dal soggetto diffamato; a suo giudizio, è *totally unacceptable* tanto l'idea che un Isp non sia direttamente responsabile dei contenuti prodotti dai suoi utenti, nei casi in cui tali contenuti siano gravemente diffamatori o ledano interessi commerciali, quanto il consentire a un portale di informazione di pubblicare commenti degli utenti coperti da anonimato.

Un altro punto che la Corte di Strasburgo sembra non aver chiarito del tutto, lasciandone la determinazione al legislatore e al giudice nazionale, è se il *provider* possa essere ritenuto responsabile per non aver rimosso i contenuti illeciti di propria iniziativa, anche a prescindere dalla richiesta del danneggiato. È vero che, soprattutto nel caso di contenuti gravemente lesivi dei diritti umani, una responsabilità di questo tipo in capo all'Isp può essere considerata compatibile con la Cedu. Tuttavia un simile approccio, se non giustificato da ragioni imperative di protezione dei diritti umani, rischierebbe di produrre ulteriori e ancora più gravi lesioni dei diritti. Inoltre, il riconoscimento della responsabilità dei *provider* per non avere rimosso *ex post*, di propria iniziativa, i contenuti lesivi equivale sostanzialmente ad attribuire agli Isp arbitrari poteri di censura[32]. Infine, non va trascurata la considerazione che, in assenza di una richiesta del danneggiato, manca l'elemento su cui fondare incontrovertibilmente l'acquisizione, da parte dell'intermediario digitale, della conoscenza del fatto illecito, nonché il termine *a quo* per l'insorgere della responsabilità.

Anche per questi motivi, secondo la *dissenting opinion* dei giudici Sajó and Tsotsoria, che hanno richiamato le considerazioni di Balkin sulla "censura collaterale"[33], l'imposizione di responsabilità agli intermediari digitali

[32] Nigro (2015), cit., partic. pp. 687-688.

[33] «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» (M. Balkin (2014), *Old School/New School Speech Regulation*, in *Harward Law Review*, n. 127, p. 2311). Secondo l'Autore, oggi come in passato gli stati hanno interesse a controllare – ed eventualmente censurare – il flusso di informazioni; a tal fine, non potendo intervenire direttamente sui mezzi di comunicazione per via del divieto di censura previsto dalle Costituzioni nazionali, ricercano la cooperazione degli intermediari digitali affinché siano questi ultimi a praticare forme di censura preventiva (*prior restraint*) attraverso l'applicazione di tecniche di filtraggio dei contenuti o altre metodologie di controllo consentite oggi dall'evoluzione tecnologica. Sempre a p. 2311 l'Autore scrive: «What looks like a problem from the standpoint of free expression, however, 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. Collateral censorship may be especially important for states that want to encourage filtering and blocking of con-

ha sempre rappresentato e continua a rappresentare un ostacolo alla libertà di espressione. La Suprema Corte estone, e conseguentemente anche la Corte europea dei diritti dell'uomo che ne ha convalidato la decisione, avrebbe sbagliato a richiedere a *Delfi* l'immediata rimozione dei contenuti illeciti a prescindere dall'accertamento del requisito della *actual knowledge* (effettiva conoscenza) della loro illiceità, poiché un'impostazione di questo tipo incoraggerebbe i legislatori e i giudici nazionali a richiedere ai *provider* l'applicazione di forme di censura privata preventiva[34]. I due giudici dissenzienti hanno inoltre sottolineato, nel caso di specie, l'estraneità dell'intermediario digitale rispetto al contenuto diffamatorio, essendo quest'ultimo *user-generated* e non avendo *Delfi* in alcun modo concorso alla sua formazione. Infine, il dissenso è stato espresso circa l'equiparazione operata dalla Corte Suprema estone fra un intermediario digitale che aggrega notizie di attualità come *Delfi* e un *publisher* (editore) in senso tradizionale, con conseguente applicazione della normativa nazionale sulla responsabilità editoriale, tanto più che questa equiparazione sarebbe stata fatta solo in virtù della natura commerciale dell'attività svolta da *Delfi*. Pur non contestando il fatto che *Delfi* potesse in concreto esercitare un qualche controllo sugli *user-generated content*, per i due giudici dissenzienti questo elemento non sarebbe sufficiente per avvalorare la tesi dell'equivalenza fra *Delfi* e un tradizionale editore, in base soprattutto a due considerazioni: «(a) in a newspaper the journalist is typically an employee (although there are good reasons to protect a journalist against his or her editor/employer); and (b) in principle, the editor is in a position to know in advance the content of an article to be published and has the decision-making power and the means to control the publication in advance. Contra-

tent from overseas, because governments cannot generally control foreign intermediaries and speakers. Intermediary liability is also a strategy for promoting public/private cooperation in speech regulation. For example, states might want intermediaries to flag and delete suspicious content, develop or finance effective filtering technologies (which the state can then use), shut down accounts, or hand over private user information. These tasks may be resource intensive and governments may be unable to perform them easily on their own. Threats of intermediary liability – coupled with promises of immunity for compliance – help states persuade owners of private infrastructure to work with them and for them».

[34] Sulla privatizzazione della censura ad opera degli intermediari digitali e sui rischi che ciò comporta si veda M. Bettoni (2011), *Profili giuridici della privatizzazione della censura*, in *Ciberspazio e diritto*, n. 4, pp. 363-383. A p. 371 l'Autore esprime preoccupazione per «lo spostamento del conflitto giuridico verso un piano di conflitto socio-tecnologico sul quale si confrontano, secondo l'antica legge della giungla, applicata però ai nuovi ambienti della tecnologia, le diverse aspirazioni variamente ispirate da motivi ideologici, politici, economici, sociali, culturali o personali, tra le quali la vincerà non quella più giusta, in senso ovviamente relativo, bensì quella più forte».

ry to the case of a publisher, these elements are only partially present in the case of active intermediaries who host their own content and actively monitor all data (that is to say, are in the position to read it and remove it after the data are made accessible), as in the case of Delfi»[35]. In altre parole, «Control *presupposes* knowledge. In this regard the difference between the editor/publisher and the active intermediary is obvious»[36].

La Corte di Strasburgo, in virtù del suo ruolo di garante del rispetto delle norme della Cedu da parte degli Stati membri e non certo della corretta applicazione della normativa nazionale o dell'Unione europea, ha valutato unicamente se la decisione del giudice estone rappresentasse o meno una violazione dell'art. 10 della Cedu, senza indagare se essa – o se la normativa nazionale che il giudice nazionale aveva interpretato e applicato – rispettasse il quadro normativo comunitario fondato sulla direttiva 2000/31/Ce sul commercio elettronico. Più precisamente, concordando con la Corte Suprema estone sul fatto che *Delfi* fosse da considerarsi un *content provider* e non un semplice *hosting provider*, la Corte europea sembra avere implicitamente affermato che il regime di limitazione di responsabilità previsto dalla direttiva 2000/31/Ce per i *provider* che svolgono attività meramente tecnica, automatica e passiva fosse inapplicabile al caso di specie. In realtà, il fatto di non aver riscontrato violazioni all'art. 10 della Cedu nulla dice sulla fondatezza dell'equiparazione fra *Delfi* e un *content provider* in virtù del tipo di attività economica svolta dall'intermediario digitale, né sulla natura civile o penale della sua eventuale responsabilità, né sull'applicabilità a *Delfi* del regime di limitazione di responsabilità previsto dalla normativa in vigore nell'Unione europea.

Tuttavia, nell'ipotesi in cui fosse stata la Corte di giustizia dell'Unione europea, e non la Corte europea dei diritti dell'uomo, a decidere del caso, è probabile il giudice di Lussemburgo avrebbe considerato l'intermediario digitale *Delfi* alla stregua di un *hosting provider*, la cui responsabilità può insorgere solo a partire dal momento dell'acquisizione della conoscenza del fatto illecito (richiesta di rimozione del contenuto da parte del soggetto diffamato) e non prima; di conseguenza, il risarcimento che *Delfi* è stata condannata a pagare, ancorché di modesta entità, probabilmente secondo la Corte di Lussemburgo sarebbe stato inesigibile, poiché riferito al danno subito nelle sei settimane precedenti alla richiesta di rimozione dei commenti presentata dalla compagnia di navigazione, quindi prima che il *provider* avesse acquisito la conoscenza del fatto illecito. Né a *Delfi*, secondo questa ricostruzione, avrebbe potuto essere attribuita alcuna responsabilità civile o

[35] Citazione tratta dal punto n. 31 della *dissenting opinion*.
[36] Punto n. 32 della *dissenting opinion*.

penale a titolo omissivo, per il fatto che la richiesta del soggetto diffamato di rimuovere i commenti offensivi era stata esaudita il giorno stesso, senza quindi alcun colpevole ritardo o inerzia.

3.2. Il caso Mte e Index c. Ungheria

Il caso ha avuto origine nel 2010 da un articolo pubblicato sul sito internet di Mte[37], in seguito al quale sono stati postati dagli utenti vari commenti dal contenuto diffamatorio, alcuni dei quali in forma anonima o pseudonima, nei confronti dei gestori di alcuni siti Internet. L'articolo è stato poi riprodotto da altre piattaforme, fra cui *Index*[38], provocando ulteriori commenti diffamatori. I soggetti diffamati si sono rivolti al giudice nazionale per ottenere l'immediata rimozione dei commenti offensivi, ma i *provider* hanno sostenuto in giudizio la tesi della loro totale estraneità rispetto ai commenti degli utenti e della mancanza di obblighi a loro carico, derivanti dalla normativa nazionale o dalla direttiva europea sul commercio elettronico, di controllarne il contenuto. In tutti e tre i gradi di giudizio, però, la responsabilità di *Mte* e *Index* per diffamazione è stata confermata, in quanto i giudici ungheresi hanno ritenuto che i *content provider* non potessero avvalersi del regime di limitazione della responsabilità previsto dalla direttiva *e-commerce* per gli intermediari digitali "passivi". Anche la Corte costituzionale ungherese, cui *Mte* e *Index* si sono infine rivolti adducendo una lesione della loro libertà di espressione, ha confermato la decisione dei precedenti giudici: poiché i commenti diffamatori erano anonimi e dunque la responsabilità non poteva essere ricondotta al loro autore, quest'ultima ricadeva inevitabilmente sui gestori delle pagine *web* che li ospitavano; questi ultimi, oltre a rimuovere prontamente i commenti, sono stati condannati al pagamento delle spese processuali.

La Corte europea dei diritti dell'uomo, adita nel 2013[39], ha ribadito *in primis* che il suo compito non era quello di valutare l'adeguatezza della

[37] L'associazione *Magyar Tartalomszolgáltatók Egyesülete* (Mte), con sede a Budapest, è un organismo di autoregolamentazione cui afferiscono i *content provider* ungheresi e dispone di un proprio portale web. Si occupa di sorvegliare che vengano rispettate le norme deontologiche ed etiche riconosciute dalla categoria dei fornitori di contenuti via Internet, anche attraverso le decisioni assunte da una commissione di arbitrato composta da undici membri.

[38] La società *Index.hu Zrt* (*Index*) è invece il più grande portale ungherese di informazione giornalistica.

[39] Corte europea dei diritti dell'uomo, *Case of Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, application n. 22947/2013, sentenza 2 maggio 2016. Si veda il commento di S. Vimercati (2016a), *Magyar c. Ungheria: la Corte europea ritorna sulla responsabilità dei portali web*, in *Quaderni costituzionali*, n. 2, pp. 393-400.

normativa nazionale e dell'Unione europea in materia di responsabilità dei prestatori dei servizi della società dell'informazione, né di accertarsi della corretta interpretazione di tali regole da parte dei giudici nazionali, ma semplicemente di valutare l'opportunità di alcune misure restrittive alla libertà di espressione a mezzo stampa rispetto al comma 2 dell'art. 10 della Cedu, in considerazione del fatto che la stessa Cedu tutela all'art. 8 la reputazione. In secondo luogo, in vari passaggi della sentenza la Corte ha sottolineato che i commenti offensivi, sebbene espressi talvolta in linguaggio volgare e suscettibili di ledere reputazione di un soggetto imprenditoriale dal punto di vista della sua affidabilità commerciale, non fossero tali da incitare all'odio e alla violenza, come invece era accaduto nel caso *Delfi*, e non fossero tali da ledere la dignità personale[40]. La Corte ha anche eccepito che i giudici nazionali non avessero adeguatamente valutato la diversità dei ruoli dei due ricorrenti, attribuendo ad entrambi la medesima responsabilità "editoriale" per gli *user-generated content*. Al contrario, maggiore attenzione andava prestata al fatto che almeno uno dei due (Mte) fosse solo un'associazione di *Internet content provider* senza finalità di lucro[41]. Inoltre, la Corte ha rilevato che, nella fattispecie, il soggetto diffamato non avesse mai richiesto direttamente ai *provider* di rimuovere i commenti, ma si fosse rivolto immediatamente al giudice; di conseguenza, i giudici nazionali avevano attribuito ai *provider* un sorta di responsabilità oggettiva, per il solo fatto di aver concesso spazio ai commenti diffamatori, senza alcuna valutazione circa la loro effettiva possibilità di conoscerne il contenuto[42].

[40] Dal punto n. 84 della sentenza: «However, the Court reiterates that there is a difference between the commercial reputational interests of a company and the reputation of an individual concerning his or her social status. Whereas the latter might have repercussions on one's dignity, for the Court interests of commercial reputation are primarily of business nature and devoid of the same moral dimension which the reputation of individuals encompasses. In the instant application, the reputational interest at stake is that of a private company; it is thus a commercial one without relevance to moral character».

[41] Dal punto n. 73 della sentenza: «The Court attaches importance to the fact that the second applicant is the owner of a large news portal, run on a commercial basis and obviously attracting a large number of comments. On the contrary, there is no appearance that the situation of the first applicant, the self-regulatory association of Internet content provider, was in any manner similar; indeed, the latter's publication of content of predominantly professional nature was unlikely to provoke heated discussions on the Internet. At any rate, the domestic courts appear to have paid no attention to the role, if any, which the applicants respectively played in generating the comments».

[42] Dai punti nn. 82-83 della sentenza: «The domestic courts held that, by allowing unfiltered comments, the applicants should have expected that some of those might be in breach of the law. For the Court, this amounts to requiring excessive and impracticable forethought capable of undermining freedom of the right to impart information on the Internet. The Court also observes that the injured company never requested the applicants to remove the comments but opted to seek justice directly in court – an element that did not

Infine, la Corte ha osservato che i giudici ungheresi avevano mancato di prestare sufficiente attenzione alle conseguenze che l'attribuzione di responsabilità al *provider* per i commenti degli utenti non sottoposti ad alcuna preventiva moderazione avrebbe potuto avere sulla tutela della libertà di espressione in Internet[43].

Per tutte queste ragioni, a differenza di quanto deciso nel caso *Delfi*, qui la Corte ha ritenuto che l'attribuzione di responsabilità per diffamazione ai *provider* che ospitano nei propri siti i commenti degli utenti rappresenti una violazione dell'art. 10 della Cedu. In via generale, però, la Corte ha affermato il principio – sulla scia del precedente caso *Delfi* – che gli Stati possono attribuire ai portali la responsabilità per i contributi pubblicati dagli utenti che costituiscano un incitamento all'odio o alla violenza, qualora non abbiano adottato misure idonee per eliminare senza ritardi i commenti illeciti, e ciò a prescindere da una specifica segnalazione della persona offesa o di terzi.

Sembra, in sintesi, che nell'ottica della Corte europea dei diritti dell'uomo la possibilità di attribuire agli intermediari digitali responsabilità di controllo ed eventuale rimozione dei contenuti *user-generated* dipenda non solo dal contenuto di questi ultimi, ma anche dalla natura più o meno lucrativa e più o meno "editoriale" del *provider*.

3.3. Il caso Pihl c. Svezia

A differenza dei due casi precedentemente trattati dalla Corte europea dei diritti dell'uomo, qui l'intermediario digitale non è un soggetto che svolge la propria attività professionalmente e con finalità di lucro, ma un piccolo *blog* gestito da un'associazione non-profit, che non ha alcuna possibilità, anche semplicemente dal punto di vista tecnico, di controllare il

attract any attention in the domestic evaluation of the circumstances. Indeed, the domestic courts imposed objective liability on the applicants for "having provided space for injurious and degrading comments" and did not perform any examination of the conduct of either the applicants or the plaintiff». Inoltre (dal punto n. 85), «the domestic courts do not appear to have evaluated whether the comments reached the requisite level of seriousness and whether they were made in a manner actually causing prejudice to a legal person's right to professional reputation».

[43] Dal punto n. 86 della sentenza: «In any event, the Court is of the view that the decisive question when assessing the consequence for the applicants is not the absence of damages payable, but the manner in which Internet portals such as theirs can be held liable for third-party comments. Such liability may have foreseeable negative consequences on the comment environment of an Internet portal, for example by impelling it to close the commenting space altogether. For the Court, these consequences may have, directly or indirectly, a chilling effect on the freedom of expression on the Internet. This effect could be particularly detrimental for a non-commercial website such as the first applicant».

contenuto dei *post* degli utenti. La natura del *provider*, che ha avuto un peso nella decisione tanto dei giudici nazionali quanto della Corte europea, rileva ai fini del tentativo di estrapolare dalla giurisprudenza alcuni principi che possano essere riferiti anche ai *social network*: in questo caso, il tentativo non andrebbe esente da qualche forzatura interpretativa.

Questo recente caso ha avuto origine da un commento diffamatorio anonimo nei confronti del sig. Pihl pubblicato in un *blog* gestito da una associazione non-profit, per il quale il danneggiato aveva chiesto un risarcimento di piccola entità. Sebbene, infatti, l'associazione che gestiva il *blog* avesse rimosso il commento e porto le sue scuse al sig. Pihl, il commento era rimasto visibile sul *blog* per nove giorni e poteva ancora essere rintracciato dopo la rimozione interrogando un motore di ricerca. L'associazione riteneva, al contrario, di non essere responsabile del contenuto di commenti sul cui contenuto non esercitava alcuna influenza. Nei tre gradi di giudizio esperiti dinanzi ai tribunali nazionali, le richieste del sig. Phil sono state sempre respinte, sulla base del fatto che, secondo la legge svedese, l'associazione non-profit non poteva essere considerata responsabile del reato di diffamazione in concorso con l'autore del commento, né gravavano su di essa obblighi di rimozione spontanea di contenuti diffamatori. Inoltre, conoscendo l'indirizzo Ip da cui il commento era stato generato, il danneggiato avrebbe potuto ricorrere in giudizio direttamente contro l'autore delle offese. Di qui l'iniziativa del sig. Pihl di ricorrere alla Corte europea dei diritti dell'uomo[44], lamentando che la legislazione svedese, escludendo la responsabilità dell'associazione che gestiva il *blog*, violava il suo diritto al rispetto della vita privata e familiare sancito dall'art. 8 della Cedu.

In primo luogo, la Corte ha precisato che il concetto di "vita privata" di cui all'art. 8 della Cedu si estende a vari aspetti dell'identità personale e dell'integrità fisica e psichica dell'individuo, ma ai fini del reato di diffamazione l'art. 8 può essere chiamato in causa solo nei limiti in cui il mancato rispetto della vita privata costituisca un grave attacco all'onore e alla reputazione. Accettato che, nel caso di specie, il contenuto del commento integrava tali presupposti, sebbene però non contenesse espressioni di incitazione all'odio o alla violenza, la Corte ha impostato la questione in questi termini: «The question is thus whether, in the present case, the State has achieved a fair balance between the applicant's right to respect for his pri-

[44] Corte europea dei diritti dell'uomo, terza sezione, *Rolf Anders Daniel Pihl against Sweden*, application n. 74742/2014, sentenza 7 febbraio 2017. Si vedano: P. Costanzo (2017), *Quando in internet la Corte di Strasburgo continua a navigare a vista*, in *DPCE On Line*, n. 3, pp. 767-771; S. Vimercati (2017), *La Corte di Strasburgo torna sulla responsabilità del gestore del sito: il caso Rolf Anders Daniel Pihl c. Svezia*, in *www.filodiritto.com*.

vate life under Article 8 and the association's right to freedom of expression guaranteed by Article 10 of the Convention»[45]. Per rispondere al quesito, la Corte ha valutato la limitata possibilità che il commento diffamatorio potesse incoraggiarne altri dello stesso genere, il ridotto numero dei potenziali lettori del commento, il fatto che l'associazione avesse chiaramente esplicitato di non effettuare alcun controllo sul contenuto dei commenti e che il commento in questione fosse stato comunque rimosso e seguito da scuse formali pubblicate *online*; ciò considerato, la Corte ha ritenuto che i giudici nazionali, nel respingere il ricorso del sig. Phil, avessero in realtà operato un equo bilanciamento dei diritti protetti dalla Cedu all'art. 8 e all'art. 10[46].

Il principio generale che si evince dalla sentenza, dunque è 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 il commento non contenga espressioni che trasmodino nell'incitamento all'odio e alla violenza e che il gestore abbia provveduto tempestivamente alla sua rimozione, a seguito della segnalazione della persona offesa. Quindi, 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, individuando un diverso bilanciamento fra i diritti, solo in caso di ragioni connesse con la particolare gravità dei contenuti offensivi[47].

Con questa sentenza e con la precedente, la Corte di Strasburgo sembra voler arginare la tendenza verso l'automatica responsabilizzazione degli intermediari digitali per gli *user-generated content*, riducendola ai soli casi in cui i contenuti prodotti dagli utenti incitino all'odio o alla violenza e i *provider* non abbiano prontamente provveduto alla loro rimozione su richiesta dell'interessato.

[45] Dal punto n. 29 della sentenza.

[46] Dal punto n. 37 della sentenza: «In view of the above, and especially the fact that the comment, although offensive, did not amount to hate speech or incitement to violence and was posted on a small blog run by a non-profit association which took it down the day after the applicant's request and nine days after it had been posted, the Court finds that the domestic courts acted within their margin of appreciation and struck a fair balance between the applicant's rights under Article 8 and the association's opposing right to freedom of expression under Article 10».

[47] Vimercati (2017), cit.

4. Orientamenti giurisprudenziali della Corte di Cassazione in tema di responsabilità editoriale nel caso delle pubblicazioni *online*

Nel contesto italiano, a proposito della possibile (o impossibile) equiparazione fra i siti (compresi i *social network sites*) attraverso cui gli utenti possono pubblicare contenuti informativi e le testate giornalistiche vere e proprie – con le connesse responsabilità derivanti, oltre che dal codice penale e dal codice civile, dalla legge sulla stampa del 1948[48] e dalla legge sulla professione giornalistica del 1963[49] – qualche spunto può provenire dalla giurisprudenza di legittimità. Quest'ultima può essere letta come il segno di una graduale evoluzione verso una concezione basata sul convincimento di una similitudine, anche se non propriamente di una analogia, fra l'editoria tradizionale e quella *online*, anche sotto il profilo delle responsabilità dei gestori delle piattaforme[50].

In una prima fase, la Suprema Corte ha affermato la «assoluta eterogeneità della telematica rispetto agli altri media sinora conosciuti e, per quel che qui interessa, rispetto alla stampa»[51], negando categoricamente che, in virtù del divieto di applicazione analogica della norma penale *in malam partem*, le responsabilità penali del direttore responsabile di una testata giornalistica tradizionale (art. 57 c. p.) fossero applicabili anche al direttore di un giornale *online* e che i coordinatori dei *blog* e dei *forum* telematici potessero essere equiparati, sotto il profilo penale, agli editori di "stampa clandestina" (art. 58 *bis* c. p.). Tale assunto sarebbe confermato, sul piano pratico, dal fatto che «la c.d. interattività (la possibilità di interferire sui testi che si leggono e si utilizzano) renderebbe, probabilmente, vano – o comunque estremamente gravoso – il compito di controllo del direttore di un giornale *on line*». Per la Cassazione, affinché possa parlarsi di "stampa" in senso giuridico «occorrono due condizioni che certamente il nuovo *medium* non realizza: a) che vi sia una riproduzione tipografica (*prius*); b) che il prodotto di tale attività (quella tipografica) sia destinato alla pubblicazione

[48] Legge 8 febbraio 1948, n. 47, *Disposizioni sulla stampa*.

[49] Legge 3 febbraio 1963, n. 69, *Ordinamento della professione di giornalista.*

[50] *Contra* S. Seminara (2014), *Internet (diritto penale*), in *Enciclopedia del diritto*, Annali VII, Milano, Giuffrè, pp. 567-606, per il quale gli illeciti realizzati attraverso *Internet* non sono riconducibili alla normativa sulla stampa.

[51] Corte di Cassazione, quinta sezione penale, sentenza 16 luglio 2010, n. 35511. Si vedano su questa sentenza i commenti di: S. Logroscino (2011), *Il direttore del periodico online non è responsabile di omesso controllo ai sensi dell'art. 57 c. p.*, in *www.penale.it*; V. Lubello (2011), *Commento alla sentenza della Corte di Cassazione n. 35511/2010*, in www.*medialaws.eu*; S. Turchetti (2010), *L'art. 57 c.p. non è applicabile al direttore del periodico online*, in *www.penalecontemporaneo.it*. Si veda inoltre P. Costanzo (2011), *La "stampa" telematica nell'ordinamento italiano*, in *Costituzionalismo.it*, n. 2, pp. 1-14.

e quindi debba essere effettivamente distribuito tra il pubblico (*posterius*). Il fatto che il messaggio internet (e dunque anche lo pagina del giornale telematico) si possa stampare non appare circostanza determinante, in ragione della mera eventualità, sia oggettiva, che soggettiva». Inoltre, la Corte ha sottolineato, evidentemente trascurando il processo di progressiva attuazione della cosiddetta "convergenza tecnologica", che alla pluralità di mezzi utilizzati corrisponde una pluralità di discipline: «non si può non sottolineare che differenti sono le modalità tecniche di trasmissione del messaggio a seconda del mezzo utilizzato: consegna materiale dello stampato e sua lettura da parte del destinatario, in un caso (stampa), irradiazione nell'etere e percezione da parte di chi si sintonizza, nell'altro (radio e Tv), infine, trasmissione telematica tramite un Isp (*Internet service provider*), con utilizzo di rete telefonica nel caso di *internet*».

Altre sentenze che la Corte di Cassazione ha emesso in tema di sequestro degli stampati sembrano confermare il medesimo orientamento. Nel 2008 la terza sezione penale, con sentenza 11 dicembre 2008 n. 10535, ha escluso che i mezzi di comunicazione del proprio pensiero consentiti dall'evoluzione tecnologica (*newsletter*, *blog*, *forum*, *newsgroup*, *mailing list*, *chat*, messaggi istantanei, e così via) possano essere inclusi nel concetto di stampa, senza considerare specificamente il loro ruolo, e dunque che ad essi siano applicabili le garanzie sul sequestro degli stampati di cui al terzo comma dell'art. 21 Cost. Al contrario, il fatto che i messaggi e gli interventi dei partecipanti a un *forum* di discussione telematico siano visionabili da chiunque non rende il *forum* stesso assimilabile a un prodotto editoriale, o a un giornale *online* o a una testata giornalistica informatica. Il *forum*, quindi, non è sottoposto alle regole ed agli obblighi cui è soggetta la stampa (quale quello di indicazione di un direttore responsabile o di registrazione) né può giovarsi delle guarentigie in tema di sequestro che l'art. 21, comma 3, Cost. riserva soltanto alla stampa, sia pure latamente intesa, ma non genericamente a qualsiasi mezzo e strumento con cui è possibile manifestare il proprio pensiero.

Sulla stessa linea, alcuni anni dopo la quinta sezione penale (sentenza 5 novembre 2013, n. 10594) ha ribadito che ai messaggi che appaiono sui *forum* di discussione telematici, che sono da considerarsi manifestazioni del pensiero assimilabili ai messaggi che possono esser lasciati in una bacheca, pubblica o privata, non possono applicarsi le disposizioni in tema di sequestro degli stampati di cui all'art. 21, comma 3, della Costituzione; inoltre, non possono essere equiparati alla stampa propriamente detta nemmeno gli articoli pubblicati *online* cui corrisponde anche una versione cartacea, quindi tali articoli non godono della tutela che la Costituzione ha riservato

alla stampa con riguardo al sequestro[52]. Tuttavia, in base a una pronuncia di poco successiva[53], sarebbe illegittimo il sequestro dell'intero *blog* nel caso in cui solo alcuni dei commenti inseriti dagli utenti abbiano carattere diffamatorio: «data la natura stessa del *blog* quale strumento di diffusione periodica di contenuti informativi e multimediali *on-line*, un'azione inibitoria generale nei confronti del sito contenente il *blog*, attuata mediante sequestro preventivo, impedisce al *blogger* di esprimersi liberamente».

Più recentemente, le Sezioni Unite hanno modificato la precedente impostazione (sentenza 29 gennaio 2015, n. 31022, dep. 17 luglio 2015)[54], evidenziando che al concetto di stampa deve attribuirsi un significato evolutivo, coerente tanto con il progresso tecnologico quanto con l'ordinamento giuridico considerato nel suo complesso, e giungendo alla conclusione che ai quotidiani e ai periodici *online* dotati di direttore responsabile e di una propria organizzazione redazionale debbano essere applicate – con esclusivo riferimento ai contenuti redazionali e non anche ai commenti postati dagli utenti[55] – le medesime disposizioni previste per la stampa tradizionale; continuano invece ad essere esclusi dall'ambito di applicazione delle disposizioni riferite alla stampa tutti quegli strumenti telematici caratterizzati dalla spontaneità della comunicazione (*forum*, *blog*, *newsletter*, *social network*, *newsletter*, *mailinglist*, ecc.)[56]. Ne consegue che «il giornale *online*, al pari di quello cartaceo, non può essere oggetto di sequestro preventivo, eccettuati i casi tassativamente previsti dalla legge, tra i quali non è compreso il reato di diffamazione a mezzo stampa». Nei casi diversi da quello della testata telematica registrata, il sequestro preventivo è

[52] Si veda il commento di C. Melzi d'Eril (2014), *La Cassazione esclude l'estensione ai siti internet delle garanzie costituzionali previste per il sequestro di stampati*, in *www.penalecontemporaneo.it*. Si veda inoltre V. Riglietti (2016), *Diffamazione a mezzo stampa e diffamazione online: problematiche giuridiche*, in *Ciberspazio e diritto*, n. 3, pp. 455 ss.

[53] Corte di Cassazione, quinta sezione, penale, sentenza 30 ottobre 2013, n. 11895, dep. 12 marzo 2014.

[54] Si veda il commento di C. Melzi d'Eril (2016), *Contrordine compagni: le Sezioni Unite estendono le garanzie costituzionali previste per il sequestro degli stampati alle testate on-line registrate*, in *www.penalecontemporaneo.it.* Si veda inoltre Riglietti (2016), cit., pp. 457 ss.

[55] Dal punto n. 22 della sentenza: «Ovviamente – è il caso di sottolinearlo – le garanzie e le responsabilità previste, per la stampa, dalle disposizioni sia di rango costituzionale, sia di livello ordinario, devono essere riferite ai soli contenuti redazionali e non anche ad eventuali commenti inseriti dagli utenti (soggetti estranei alla redazione), che attivano un *forum*, vale a dire una discussione su uno o più articoli pubblicati»,

[56] In particolare, in questa stessa sentenza è precisato (punto 18.3) che «il *social network* più diffuso, denominato *Facebook*, non è inquadrabile nel concetto di "stampa", ma è un servizio di rete sociale …».

invece ammissibile e inevitabilmente implica un intervento sul prestatore del servizio (*internet service provider*)» perché impedisca l'accesso al sito o alla singola pagina ovvero disponga il blocco o la cancellazione del *file* incriminato».

In altri termini, la Cassazione ha ritenuto che un sito *web* non debba essere qualificato con riferimento alla sua totalità, ma tenendo distinte le sue diverse funzioni, cosicché il *provider* può essere qualificato come *content provider* con riferimento alla parte redazione e come *host provider* per quanto attiene alle sezioni dedicate agli interventi degli utenti[57]. In questa sentenza, il ragionamento della Corte muove dalla considerazione dell'irragionevolezza, per violazione del principio di uguaglianza, del trattamento differenziato dell'informazione veicolata su carta stampata rispetto a quella diffusa via Internet. Tuttavia, la distinzione operata dalla Cassazione fra le testate *online* regolarmente registrate e le altre piattaforme sembra non tenere conto del fatto che l'attività giornalistica non è solo quella veicolata dalle testate registrate: molti giornalisti, invece, svolgono oggi la loro attività anche mediante altri mezzi di comunicazione più "informali"[58]. Per ridurre l'arbitrarietà, qualcuno ha suggerito di interpretare in chiave evolutiva l'art. 21 Cost., terzo comma, applicando le garanzie previste per la stampa anche a tutte le forme di comunicazione che abbiamo le caratteristiche dell'informazione giornalistica, quindi anche eventualmente «alle pagine *web* ove sia esplicito l'autore del contenuto e la data di immissione in rete»[59].

Questo orientamento, però, non è stato seguito dalla Corte di Cassazione nella successiva sentenza della quinta sezione penale, 25 febbraio 2016 (dep. 24 marzo 2016), n. 12536[60]. Sebbene, infatti, il caso riguardasse il sequestro operato nei confronti di un *blog* dedicato in parte anche all'informazione giornalistica, e perciò in astratto assimilabile a una testata giornalistica telematica, la Corte ha ribadito che le garanzie costituzionali in tema di sequestro non possono essere estese ai *blog* e agli altri mezzi di manifestazione del pensiero telematici diversi dalle testate giornalistiche *online*, perché non assimilabili ai giornali cartacei ed estranei alla nozione di stampa. Al contrario, sebbene il gestore di quel *blog* fosse iscritto all'Ordine dei giornalisti, il *blog* difettava della registrazione e dell'indicazione del direttore responsabile, oltre a non avere una regolare

[57] Mula (2016), cit., p.84.

[58] Melzi d'Eril (2016), cit., p. 10.

[59] Ivi, p. 14.

[60] Si veda il commento di S. Vimercati (2016b), *La Cassazione conferma l'inestensibilità ai blog delle garanzie costituzionali previste per gli stampati in tema di sequestro*, in *www.penalecontemporaneo.it*.

periodicità. Per la Corte, affinché l'informazione *online* possa essere equiparata alla stampa occorrerebbe invece constatare l'esistenza di attività consistenti«nella raccolta, nel commento e nell'analisi critica di notizie legate all'attualità (cronaca, economia, costume, politica) e dirette al pubblico, perché ne abbia conoscenza e ne assuma consapevolezza nella libera formazione della propria opinione». Il problema, però è che la distinzione tra le testate telematiche registrate e tutti gli altri mezzi di informazione *online* appare priva di qualsiasi riferimento normativo, poiché né nella Costituzione né nella legislazione ordinaria si rinviene una definizione di "informazione professionale" che consenta di applicare questo o altri *distinguo*[61]. Quindi, il confine fra giornali *online* e gli altri siti Internet non trova alcuna giustificazione, come è chiaramente dimostrato dal fenomeno dei cosiddetti *instant articles*, cioè quegli articoli pubblicati su *Facebook* direttamente e non tramite *link* di rimando alle testate giornalistiche. A ragionare diversamente, invece, si verrebbe a creare il paradosso per cui il sequestro non sarebbe applicabile nel caso di un articolo dal contenuto diffamatorio pubblicato su una testata giornalistica registrata (cartacea o telematica), mentre lo sarebbe nel caso dello stesso identico articolo pubblicato su *Facebook*[62].

Ulteriori spunti di riflessione possono provenire da due sentenze che hanno riguardato l'assimilazione fra la diffamazione che avviene attraverso *Facebook* e la fattispecie aggravata del reato di diffamazione (diffamazione a mezzo stampa o con altro mezzo di pubblicità). Nella prima sentenza[63], la suprema Corte ha stabilito che la fattispecie aggravata del reato di diffamazione, di cui al comma 3 dell'art. 595 c. p., «trova il suo fondamento nella potenzialità, nella idoneità e nella capacità del mezzo utilizzato per la consumazione del reato a coinvolgere e raggiungere una pluralità di persone, ancorché non individuate nello specifico ed apprezzabili soltanto in via potenziale, con ciò cagionando un maggiore e più diffuso danno alla persona offesa». Quindi, poiché la diffusione di un messaggio attraverso *Facebook* ha potenzialmente la capacità di raggiungere un numero indeterminato di persone, la relativa condotta rientra nella tipizzazione codicistica descritta dal terzo comma dell'art. 595 del codice penale. In una sentenza successiva[64], la Corte ha ribadito il medesimo principio, ma ha precisato che la no-

[61] Ivi, p. 11.

[62] *Ibid*.

[63] Corte di Cassazione, prima sezione penale, sentenza 8 giugno 2015, n. 24431.

[64] Corte di Cassazione, quinta sezione penale, sentenza 14 novembre 2016 (dep. 1 febbraio 2017), n. 4873. Si veda il commento di E. Birritteri (2017), *Diffamazione e Facebook: la Cassazione conferma il suo indirizzo ma apre a un'estensione analogica in malam partem delle norme sulla stampa*, in *Diritto penale contemporaneo*, n. 4, pp. 286-289.

zione di "stampa" non è applicabile a un *social network*, ma solo al settore dell'informazione professionale veicolata *online*; l'applicabilità della fattispecie aggravata del reato di diffamazione deriva, quindi, dall'essere *Facebook* «altro mezzo di pubblicità», non propriamente "stampa". Un'ulteriore sentenza[65], sempre in tema di diffamazione compiuta attraverso *Facebook*, ha aggiunto che «la circostanza che l'accesso al *social network* richieda all'utente una procedura di registrazione – peraltro gratuita, assai agevole e alla portata sostanzialmente di chiunque – non esclude la natura di "altro mezzo di pubblicità" richiesta dalla norma penale per l'integrazione dell'aggravante, che discende dalla potenzialità diffusiva dello strumento di comunicazione telematica utilizzato per veicolare il messaggio diffamatorio, e non dall'indiscriminata libertà di accesso al contenitore della notizia …». In questo modo, la Corte ha avvalorato la tesi della natura dei *social network* come spazi pubblici di comunicazione, e non come luoghi privati di interazione fra le persone.

Infine, va segnalato un caso in cui – con qualche analogia rispetto alle pronunce della Corte europea dei diritti dell'uomo – la quinta sezione penale della Corte di Cassazione (27 dicembre 2016, n. 54946) si è occupata della responsabilità di un gestore del sito internet per i commenti diffamatori postati in modo autonomo dagli utenti[66]. La vicenda ha riguardato un commento diffamatorio pubblicato da un utente della *community* del sito *agenziacalcio.it*. In tale occasione la Cassazione ha confermato la sentenza di condanna per concorso nel reato di diffamazione comminata dalla Corte d'Appello di Brescia al gestore del sito per non aver rimosso prontamente il commento in questione, pur essendo venuto a conoscenza della sua illiceità. Così la Corte ha confermato la tesi della sussistenza di un obbligo di rimozione, in capo ai gestori dei siti, di ogni contenuto potenzialmente offensivo pubblicato dagli utenti di cui il gestore sia venuto a conoscenza. Questa impostazione è parzialmente in contrasto con quella derivante dalla giurisprudenza della Corte europea dei diritti dell'uomo (in particolare *Phil c. Svezia*), che sembra invece propendere per la tesi dell'obbligo di rimozione solo nel caso in cui il contenuto offensivo sia suscettibile di incitare all'odio e alla violenza. Non va sottaciuto il fatto che, sebbene il gestore del sito avesse ec-

[65] Corte di Cassazione, prima sezione penale, sentenza 2 dicembre 2016 (dep. 2 gennaio 2017), n. 50. Si veda il commento di M. Iaselli (2017b), *Facebook: l'offesa in bacheca è diffamazione aggravata*, in *www.altalex.com*.

[66] Si vedano i commenti di: F. Buffa (2017), *Responsabilità del gestore di sito Internet*, in *Questionegiustizia.it*; G. De Gregorio (2017a), *Il regime di responsabilità degli Isp alla luce della sentenza della Corte di Cassazione n. 54946/2016*, in *www.medialaws.eu*; M. Miglio (2017), *I gestori di un sito internet rispondono penalmente per i commenti offensivi pubblicati dagli utenti*, in *Giurisprudenza penale web*, n. 1.

cepito di non poter essere a conoscenza dell'illecito per il fatto di trovarsi in quel momento all'estero, tale circostanza non è stata giudicata rilevante. Dunque, se questa lettura venisse applicata anche a casi analoghi, si potrebbe ottenere il risultato – per la verità assai rischioso – di ritenere automaticamente responsabile il gestore di qualsiasi sito dotato di un sistema di moderazione dei commenti[67]. Tuttavia, secondo un'interpretazione più rassicurante[68], «la sentenza della Cassazione non stabilisce il principio secondo il quale i gestori dei siti internet d'ora in avanti saranno ritenuti responsabili dei contenuti pubblicati dagli utenti sulle proprie pagine, né riconosce una generale responsabilità editoriale dei siti web. Inoltre, […] la mancanza di qualsiasi riferimento nella sentenza alla disciplina europea e nazionale relativa alla responsabilità degli Isp svuota la portata riformatrice di una simile decisione. Per tale ragione, la sentenza in questione non potrà essere annoverata tra le *landmark decision* in tema di responsabilità degli Isp né aspirare alla definizione di un nuovo regime di responsabilità degli Isp».

In sintesi, dalla giurisprudenza della Corte di Cassazione emerge una recente tendenza all'equiparazione fra i quotidiani e i periodici *online* dotati di direttore responsabile e di una propria organizzazione redazionale e la stampa tradizionalmente intesa, con la conseguente estensione della normativa sulla stampa alle testate telematiche. Tuttavia, le forme di comunicazione *online* più informali (*blog*, *forum*, commenti degli utenti in calce agli articoli pubblicati, comunicazione attraverso i *social network*) possono essere considerati "mezzi di pubblicità", ma non propriamente "stampa". Il ché, però, non ha impedito di ritenere responsabile del reato di diffamazione il gestore di un sito internet, in base alla presunzione della sua conoscenza dell'illiceità dei contenuti *user-generated* (commenti degli utenti) presenti sul sito.

[67] Buffa (2017), cit.
[68] De Gregorio (2017a), cit.

PROFILI DI RESPONSABILITÀ PENALE DEGLI INTERMEDIARI DIGITALI IN PROSPETTIVA *DE JURE CONDENDO*

1. Il concorso nel reato

I reati che possono essere commessi dagli utenti di Internet sono di vario tipo[1]. Alcuni di questi – quelli per cui l'utilizzo delle tecnologie informatiche è considerato dal legislatore fra gli elementi costitutivi del reato – sono definiti come reati informatici "in senso stretto"; si pensi, ad esempio, alle frodi informatiche o agli accessi abusivi ai sistemi informatici. Altri, invece, sono considerati reati informatici "in senso ampio": si tratta di quei reati che, pur essendo concepibili e attuabili anche a prescindere dall'uso di Internet, trovano negli strumenti informatici, e in particolare nel ciberspazio, una peculiare forma di realizzazione che solitamente li rende più temibili e dannosi[2]. Si pensi, ad esempio, al trattamento illecito dei dati personali, alla diffamazione, all'istigazione alla violenza, all'odio o alla discriminazione, all'apologia di reati, alla diffusione di materiale pedopornografico, allo sfruttamento della prostituzione, alla violazione del diritto d'autore. In molti casi, l'utilizzo dei *social network* per la commissione di tali reati, soprattutto di quelli che sono connessi alla manifestazione del pensiero, contribuisce ad amplificarne l'effetto, e quindi il danno.

Senza dilungarsi nell'analisi delle diverse fattispecie delittuose che possono verificarsi nel ciberspazio, e tralasciando di considerare il ruolo degli utenti di Internet (e dei *social network*) come autori o come vittime dei reati, il tema che si vuole qui esaminare è quello della responsabilità penale

[1] L. Picotti (2012), *I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali*, in *Giurisprudenza di merito*, n. 12, pp. 2522-2547.

[2] R. Flor (2012), *Social networks e violazioni penali dei diritti d'autore. Quali prospettive per la responsabilità del fornitore del servizio?*, in *Rivista trimestrale di diritto penale dell'economia*, n. 3, p. 657.

degli Isp, che può essere evocata con riferimento sia al concorso nel reato commesso dagli utenti (artt. 110 e ss. del codice penale) sia al reato omissivo improprio *ex* art. 140 del codice penale. In realtà, *de iure condito* risulta assai difficile, se non addirittura impossibile, affermare la responsabilità penale degli intermediari digitali per reati commessi da altri, perché l'attribuzione di responsabilità oggettive è in contrasto con il principio di personalità della responsabilità penale, mentre è fuor di dubbio che l'Isp risponde direttamente sul piano penale delle violazioni di legge commesse in prima persona nello svolgimento della propria attività[3].

Ciò deriva anche dalla perdurante incertezza sulla posizione dell'Isp, rispetto alla quale sussistono tre diverse concezioni[4]. Secondo un primo paradigma, l'Isp è posto sullo stesso piano di qualsiasi altro soggetto, senza doveri di controllo rispetto a condotte altrui, obblighi di denuncia dei reati da altri commessi di cui viene a conoscenza o oneri di collaborazione con le autorità nella repressione degli illeciti; l'Isp così considerato risponderebbe solo dei reati di cui è autore o cui ha offerto un contributo concorsuale attivo. In base a un secondo paradigma, l'Isp rivestirebbe il ruolo di "controllore" delle attività che gli utenti realizzato grazie ai servizi offerti dal *provider*; l'intermediario digitale avrebbe allora oneri di sorveglianza *ex ante* (nonché eventualmente di censura preventiva) e risponderebbe di eventuali reati non solo a titolo commissivo (per quelli da lui attivamente commessi), ma anche a titolo omissivo, per non avere impedito le condotte delittuose degli utenti. Un terzo paradigma vedrebbe invece l'Isp come "tutore dell'ordine" del ciberspazio, che non avrebbe obblighi di sorveglianza preventiva, ma solo di attivarsi per ridurre le conseguenze di reati già commessi e per agevolare la punizione degli autori; l'attivazione dell'intermediario digitale sarebbe richiesta nelle due ipotesi di acquisizione della conoscenza del fatto illecito (spontaneamente o su segnalazione da parte dei soggetti interessati) e di richiesta di attivazione proveniente dall'autorità giudiziaria o amministrativa; l'Isp sarebbe allora responsabile a titolo commissivo (per condotte criminose direttamente a lui imputabili), a titolo omissivo improprio (per non avere impedito le condotte criminose degli utenti, pur avendone acquisito conoscenza) e a titolo omissivo proprio (per non aver ottemperato agli ordini provenienti dalle competenti autorità). Questa terza rico-

[3] G. P. Accinti (2017), *Profili di responsabilità penale dell'hosting provider "attivo"*, in *Archivio penale*, n. 2, p. 3.

[4] T. Giovannetti (2014), *Governance della Rete e il ricorso alla sanzione penale: il caso della responsabilità dell'Internet Service Provider tra tentazioni punitive e rispetto dei principi costituzionali*, in M. Nisticò e P. Passaglia (a cura di), *Internet e Costituzione*, Torino, Giappichelli, partic. pp. 328 ss.; A. Ingrassia (2012), *Il ruolo dell'Isp nel ciberspazio: cittadino, controllore o tutore dell'ordine*?, in *www.penalecontemporaneo.it*.

struzione è quella che sembra più aderente al dettato normativo del d. lgs. n. 70/2003 che, sia pure riferito alla responsabilità civile, può essere utilizzato come ausilio interpretativo per definire anche quella penale. Per quanto riguarda la giurisprudenza, invece, va detto che finora la strada dell'attribuzione di responsabilità penali al *provider* è stata scarsamente battuta.

Con riferimento alla questione del concorso nel reato commesso da altri, in linea generale va premesso che il legislatore italiano ha rinunciato a distinguere analiticamente le varie forme di partecipazione al reato, graduando le connesse responsabilità; si è piuttosto prescelto un modello unitario nel quale, al di là dei diversi ruoli svolti dai concorrenti nella commissione del reato, la medesima pena è applicata a tutti[5]. In prospettiva finora solo teorica, il giudice potrebbe quindi distinguere – considerandole più lievi – le responsabilità di un *provider* eventualmente imputato di concorso nel reato *ex* artt. 110 e 113 c. p. solo qualora si dimostrasse che il suo apporto sia stato di minima importanza (art. 114 c. p.). Il nodo da sciogliere riguarda essenzialmente la valutazione del ruolo effettivamente svolto dall'Isp: se il gestore della piattaforma avesse mantenuto un atteggiamento davvero neutrale ed estraneo alle attività degli utenti, si dimostrerebbe infondata un'eventuale accusa di aver cooperato alla realizzazione del reato. Tuttavia oggi – come si è ampiamente evidenziato nelle pagine precedenti – la presunta neutralità dell'Isp può essere messa in discussione dal fatto che sempre più spesso gli intermediari digitali svolgono attività di selezione, organizzazione e indicizzazione dei contenuti. In questi casi, occorrerebbe probabilmente procedere a una valutazione caso per caso, per esempio verificando se l'attività dell'Isp sia di tipo esclusivamente automatizzato oppure se, sia pure in forma semi-automatica, il *provider* sia in qualche modo intervenuto nell'*editing* dei contenuti prodotti dall'utente[6], contribuendo così direttamente alla commissione del reato (concorso materiale).

Anche qualora si accertasse la posizione di non neutralità dell'intermediario digitale, attribuendo ad esso una qualche condotta attiva, non si potrebbe trascurare il fatto che, in base alla concezione causale del concorso criminoso, l'azione del compartecipe dovrebbe costituire la *condicio sine qua non* del fatto punibile[7]. In altre parole, l'apporto del *provider* dovrebbe essere stato elemento necessario e indispensabile, e non meramente accessorio, per la realizzazione dell'evento delittuoso. Quindi, in tale ottica, i servizi offerti dal *provider* agli

[5] G. Fiandaca e R. Musco (2001), *Diritto penale. Parte generale*, Bologna, Zanichelli, pp. 448-453.

[6] R. Bartoli (2013), *Brevi considerazioni sulla responsabilità penale dell'Internet Service Provider*, in *Diritto penale e processo*, n. 5, p. 605.

[7] Fiandaca e Musco (2001), cit., p. 460.

utenti dovrebbero essere considerati condizione *necessaria* per consentire la circolazione *online* dei contenuti illeciti prodotti o diffusi dagli utenti, quindi fattore *indispensabile* per la realizzazione del fatto criminoso. Però, secondo un diverso modello – quello della cosiddetta *causalità agevolatrice*, che consente di estendere l'incriminazione anche alle ipotesi di partecipazione non necessaria – può assumere rilevanza penale anche la condotta che, in base a un giudizio *ex post*, abbia semplicemente facilitato o agevolato la realizzazione del reato[8]. I servizi offerti agli utenti dal *provider*, allora, potrebbero essere considerati semplicemente fattori agevolativi. Per questo qualcuno sostiene che «allorquando il *provider* si inserisca in qualche modo nella divulgazione del contenuto illecito con un *quid pluris* rispetto alla mera attività di stoccaggio e messa a disposizione del materiale *online*, sarebbe infatti almeno astrattamente possibile ipotizzare un suo contributo causale alla realizzazione del fatto illecito rilevante *ex* art. 110 c. p.», qualora il suo comportamento abbia anche semplicemente facilitato la commissione del reato[9].

Comunque si voglia considerare la questione, un ostacolo interpretativo all'attribuzione al *provider* di responsabilità penali a titolo di concorso è determinato dal fatto che gran parte dei reati tradizionalmente commessi dagli utenti di Internet (diffamazione, apologia di reato, diffusione di materiale pedopornografico, diffusione di materiale coperto da *copyright*) sono reati di condotta caratterizzati da verbi modali quali "diffondere", divulgare" e simili; in tutti questi casi, poiché la condotta del *provider* che mantiene *online* tali contenuti o omette di cancellarli è successiva alla commissione del reato, non si può propriamente parlare di concorso nel reato stesso[10]. Allo stesso modo, è necessariamente successiva alla commissione del reato da parte dell'utente l'insorgenza nell'Isp della consapevolezza dell'illiceità dei contenuti, mentre «il dolo di partecipazione richiederebbe (ovviamente) una rappresentazione almeno coeva alla perpetrazione dell'illecito»[11].

Inoltre, per quanto riguarda l'elemento psicologico del reato, nel concorso di persone nel reato è necessario che il dolo abbracci tanto il fatto principale realizzato dall'autore quanto il contributo causale recato dalla condotta atipica del concorrente; non convince quindi l'attribuzione di responsabilità al *provider* con riferimento al dolo eventuale, in assenza di elementi che consentano di ricondurre alla sua "sfera di conoscibilità" una specifica attività illecita commessa per suo tramite[12]. Ciò si verificherebbe,

[8] Fiandaca e Musco (2001), cit., pp. 461-463.
[9] Accinti (2017), cit., p. 10.
[10] Ingrassia (2012), cit., p. 21.
[11] Accinti (2017), cit., p. 13.
[12] Accinti (2017), cit., p. 12.

in realtà, nel solo caso specifico in cui «il contenuto illecito sia stato in qualche modo trattato dal gestore del servizio per lo svolgimento di ciascuno dei servizi aggiuntivi che valgono ad identificarlo come *hoster* attivo»[13].

Un ausilio interpretativo per chiarire meglio queste questioni può provenire dalla recente giurisprudenza. Un caso interessante è rappresentato da una decisione del febbraio 2016[14], in cui il giudice ha affrontato la questione della responsabilità penale gravante in capo all'amministratore di un gruppo creato su *Facebook* per i commenti offensivi pubblicati dagli iscritti al gruppo. Il giudice ha condiviso l'orientamento giurisprudenziale dominante, secondo il quale i messaggi diffamatori pubblicati tramite *Facebook* integrano la fattispecie di diffamazione aggravata prevista al comma 3 dell'art. 595 c. p., in quanto sono potenzialmente in grado di raggiungere un numero indeterminato o comunque quantitativamente apprezzabile di persone[15]. A proposito dell'eventuale responsabilità dell'amministratore del gruppo in concorso con gli autori delle condotte illecite, però, il giudice ha precisato che «in sede penale non è possibile ritenere che le offese degli utenti debbano darsi per condivise dal *dominus* del gruppo solo in quanto da questi approvate, in modo specifico (nel caso in cui abbia predisposto un sistema di filtri) ovvero in modo generico e incondizionato (nel caso in cui non l'abbia predisposto)». Al contrario, in linea di principio l'amministratore di un gruppo *Facebook* non è in grado di operare un controllo preventivo sulle affermazioni che gli utenti immettono in Rete, ma, «tenuto conto dell'elevato numero di messaggi da gestire per la pubblicazione nel sito, a questi si può richiedere unicamente un controllo *prima facie* circa la presenza di espressioni immediatamente ed oggettivamente valutabili come diffamatorie». Ciò considerato, può essere attribuita una responsabilità per diffamazione all'amministratore del gruppo «solo allorché ricorra, sotto il profilo soggettivo, una responsabilità concorsuale, commissiva ovvero omissiva, di tipo morale, la cui prova deve essere rigorosamente fornita dall'ufficio di Procura». In conclusione, «affinché l'elemento soggettivo del reato ex art. 595 c. p. possa ritenersi sussistente, è necessario che il moderatore abbia scientemente omesso di cancellare, anche a posteriori, le frasi diffamatorie. Ove, invece, egli si sia prontamente

[13] Ivi, p. 17.

[14] Tribunale di Vallo Della Lucania, Uff. Gip, 24 febbraio 2016.

[15] *Ex multis*: Cass. pen., sez. V, 1 marzo 2016, n. 8328 (si veda il commento di C. Curreli (2017), *La diffamazione su Facebook, tra diritto sostanziale e profili probatori*, in *Responsabilità civile e previdenza*, n. 1, pp. 189-198); Cass. pen., sez. I, 8 giugno 2015, n. 24331; Cass. pen., sez. I, 22 gennaio 2014, n. 16712 (si veda il commento di F. Zani (2014), *Il difficile bilanciamento fra tutela della libertà di manifestazione del pensiero e diritto alla riservatezza nell'era dei social network*, in *Osservatorio costituzionale Aic*, n. 2, pp. 1-9).

attivato in senso emendativo, allora la sua condotta non assumerà connotati illeciti».

Il nodo critico di questa sentenza[16] risiede nel fatto che essa non ha statuito l'insussistenza di obblighi di controllo in capo all'amministratore del gruppo sui contenuti diffamatori pubblicati dagli utenti, ma ne ha soltanto posticipato l'insorgenza al momento immediatamente successivo alla loro pubblicazione. Infatti, nell'opinione del giudice la mancata rimozione dei commenti diffamatori equivale ad un'adesione agli stessi da parte dell'amministratore, tale quindi da configurare la sua responsabilità concorsuale, anche di tipo omissivo. Però, in realtà il *dominus* potrebbe non cogliere appieno la portata diffamatoria del commento, pur non condividendone il tenore o il tono, e nel dubbio potrebbe decidere di non rimuovere il commento. Deve allora desumersi che l'amministratore, a scopo cautelativo, dovrebbe eliminare tutti i commenti aventi contenuto e forma dubbie, così da evitare di incorrere in ipotesi di responsabilità penale nei suoi confronti? L'imposizione di un obbligo siffatto, di creazione tutta giurisprudenziale, andrebbe considerata piuttosto alla stregua di un'applicazione analogica *in malam partem* della norma penale.

Un altro caso interessante è rappresentato da una sentenza della Corte di Cassazione (V sez. pen., 27 dicembre 2016, n. 54946), che è stata la prima (e finora l'unica?) ad affermare, in sede di giudizio di legittimità, la responsabilità penale del *provider* per i contenuti prodotti dagli utenti del sito. La vicenda processuale è la seguente[17]. Il 24 giugno 2015 la Corte d'Appello di Brescia, riformando la sentenza assolutoria emessa in primo grado dal Tribunale di Bergamo il 10 novembre 2014, ha condannato per concorso nel reato di diffamazione il gestore di un sito internet (*agenziacalcio.it*) che non aveva rimosso un commento dal contenuto inserito da un utente. La decisione del giudice di primo grado si basava sul fatto che il gestore del sito fosse inconsapevole del contenuto diffamatorio del commento, mentre nuove prove emerse in sede di gravame avevano portato la Corte d'Appello a ritenere che il commento fosse stato mantenuto *online* pur nella consape-

[16] M. Miglio (2016), *La responsabilità dell'amministratore di un gruppo Facebook per i commenti offensivi pubblicati da altri utenti: un travagliato percorso giurisprudenziale*, in *Giurisprudenza penale web*, n. 9, p. 6.

[17] Si vedano i commenti di: F. Buffa (2017), *Responsabilità del gestore di sito Internet*, in *www.questionegiustizia.it*; R. Carbone (2017), *Responsabilità del* blogger*: parziale* revirement *della Cassazione?*, in *Cassazione penale*, n. 7-8, pp. 2782-2790; A. Ingrassia (2017), *Responsabilità penale degli* Internet service provider*: attualità e prospettive*, in *Diritto penale e processo*, n. 12, pp. 1621-1628; C. Melzi d'Eril e S. Vimercati (2017), *Diffamazione, il gestore del sito risponde dei commenti*, in *Il Sole24Ore*, edizione *online*; M. Miglio (2017), *I gestori di un sito internet rispondono penalmente per i commenti offensivi pubblicati dagli utenti*, in *Giurisprudenza penale web*, n. 1.

volezza della sua illiceità. Infine la Corte di Cassazione ha giudicato infondato il ricorso proposto dal gestore del sito avverso la sentenza della Corte d'Appello, non ravvisando in essa i vizi motivazionali che il ricorrente adduceva[18]. La condanna del gestore del sito per concorso nel reato di diffamazione è stata dunque confermata. Nel ragionamento della Cassazione, però, non può sfuggire una certa confusione concettuale[19]: dapprima si rimprovera all'imputato di aver consentito il perdurare dell'efficacia diffamatoria dello scritto e, poche righe dopo, di non aver impedito che la condotta diffamatoria si protraesse. Si tratta però di due diversi modelli di responsabilità perché, nel primo caso, il reato è già consumato e il disvalore si incentra sugli effetti che esso produce sul bene giuridico, mentre nel secondo caso ci si riferisce alla classica ipotesi di omesso impedimento del reato[20], caratterizzato da una condotta di durata.

Il nodo problematico consiste nel fatto che la sentenza sembra dare per scontato che il gestore di un sito Internet che ospiti commenti degli utenti – una categoria, questa, in cui potrebbero essere fatti rientrare anche i gestori dei *social network* – sia responsabile per il solo fatto della conoscenza del messaggio ospitato, a prescindere dall'esistenza di una richiesta di rimozione del dato da parte del presunto diffamato e dell'autorità giudiziaria[21]. Alla base di questo assunto vi è l'idea che l'illecito commesso attraverso Internet sia un illecito permanente, poiché il contenuto illecito viene permanentemente ritrasmesso senza che il danneggiato possa impedirlo. Se è così, occorre necessariamente un intervento diretto del *provider* per impedire la continuativa consumazione del reato; nel momento in cui il *provider* acquisisce la conoscenza che attraverso i suoi servizi si sta realizzando un comportamento lesivo permanente, egli concorre nel fatto altrui se non interrompe la visibilità del messaggio illecito, rimuovendo il dato informatico in questione o bloccando l'accesso allo stesso[22].

Però, la conclusione per cui il titolare di un sito *web* possa essere ritenuto direttamente responsabile di diffamazione se non si attiva per impedire la

[18] Si legge nella sentenza: «Il ricorso è infondato. La motivazione della sentenza impugnata, sull'affermazione di responsabilità dell'imputato, era coerente e rispettosa, contrariamente a quanto sostenuto dal ricorrente, dell'onere di adeguata critica dell'impostazione assolutoria della decisione di primo grado. […] La doglianza relativa alla mancata riassunzione delle prove nel giudizio di appello è infine manifestamente infondata, essendo l'affermazione di responsabilità, per quanto detto, giustificata non da una rivalutazione delle prove dichiarative, ma dalla valorizzazione di un dato documentale non considerato rilevante in primo grado.

[19] Ingrassia (2017), cit., pp. 1263-1264.

[20] Vedi il paragrafo successivo di questo capitolo.

[21] Buffa (2017), cit.

[22] *Ibid.*

permanenza *online* di un *post* diffamatorio *user-generated* non pare del tutto convincente: in primo luogo, il concorso di persone nel reato presuppone il contributo morale e materiale di tutti i concorrenti alla realizzazione del fatto criminoso, contributo che non pare realizzato nel caso di mera inerzia del *provider*; in secondo luogo, considerata la natura istantanea del reato, che appunto si consuma al momento della lettura del messaggio da parte di almeno due persone, la protrazione degli effetti diffamatori, derivante dal mantenimento *online* del contributo, non è da considerarsi penalmente rilevante; infine, poiché non si rinviene nell'ordinamento giuridico alcuna posizione di garanzia in capo al gestore di un sito[23], non pare configurabile l'ipotesi di responsabilità per diffamazione in forma omissiva[24].

Al di là di queste considerazioni, resta il fatto che, sulla scia di questa sentenza, i gestori dei *blog*, per porsi al riparo da addebiti penali per i contenuti inseriti dagli utenti, sarebbero incentivati a dotarsi del personale tecnico in grado di valutare l'illiceità di quanto introdotto, cosa che potrebbe condurre alla fine dell'esperienza dei *blog* non professionali, con grave nocumento al principio della libertà di espressione[25].

2. Il reato omissivo improprio

Problemi interpretativi anche maggiori sono posti dal profilo relativo alla commissione del reato mediante omissione. In base al secondo comma dell'art. 40 del Codice penale, «non impedire un evento, che si ha l'obbligo giuridico di impedire, equivale a cagionarlo». Dall'innesto dell'art. 40 c. p. sulle norme di parte speciale relative alle singole fattispecie delittuose, la dottrina ha ricostruito la categoria del *reato omissivo improprio*[26], commesso da chi contravviene all'obbligo di impedire il verificarsi di un evento lesivo. Qualche discordanza sussiste fra coloro che ritengono che il reato omissivo improprio non sia che una manifestazione della fattispecie commissiva, e quanti invece propendono per la tesi secondo cui si tratta di una fattispecie a carattere autonomo, ricostruzione che però solleva qualche dubbio sulla compatibilità di questo modello con i principi di legalità e di sufficiente determinazione della fattispecie.

Altre incertezze riguardano la sfera di operatività della "clausola di equivalenza" di cui all'art. 40 c. p.: la dottrina più accorta tende a considerarla applicabile ai soli reati di evento per i quali le modalità comportamen-

[23] Vedi su questo anche Miglio (2016), cit., pp. 6-9.
[24] Melzi d'Eril e Vimercati (2017), cit.
[25] Carbone (2017), cit., p. 2785.
[26] Fiandaca e Musco (2001), cit., pp. 546 ss.

tali che innescano il processo causale appaiono indifferenti (reati causali puri), escludendo invece i reati per i quali la norma incriminatrice prevede una condotta positiva tipizzata. A tale proposito, è stato anche osservato che l'inottemperanza ad un obbligo di intervento dell'intermediario digitale non avrebbe in ogni caso alcuna efficacia causale, poiché il reato sarebbe già consumato nel momento dell'insorgere, per il *provider*, dell'obbligo di attivarsi[27].

Ulteriori perplessità derivano dall'ipotesi del concorso mediante omissione a un reato materialmente commesso da altri; in particolare, ci si chiede – con soluzioni discordanti in dottrina – se il titolare dell'obbligo di impedire l'evento possa partecipare, mediante omissione, alla commissione di qualsiasi reato o solo dei reati causali puri. È pacifico che, per attribuire all'omittente la responsabilità dell'evento, occorre dimostrare la sussistenza di una connessione fra l'evento stesso e la condotta omissiva. Per determinare questo nesso, spetta al giudice formulare un giudizio ipotetico o prognostico, chiedendosi se, qualora l'azione doverosa omessa fosse stata invece posta in essere, l'evento lesivo si sarebbe realizzato ugualmente oppure no, con una probabilità vicina alla certezza. Quindi, fra omissione ed evento lesivo non sussiste un nesso di causalità vero e proprio, quanto piuttosto un rapporto di mera *causalità ipotetica*.

Si registra però una difficoltà a determinare i casi in cui l'obbligo giuridico di impedire la condotta dannosa effettivamente sussista. Infatti, «da un lato, la mancanza di un numero "chiuso" di obblighi di impedire l'evento legislativamente prefissati dovrebbe consentire alla giurisprudenza di far fronte alle nuove esigenze di tutela eventualmente emergenti dalla prassi; dall'altro lato, però, questo affidarsi alla prassi fa sì che il settore dei reati omissivi impropri oscilli inevitabilmente tra limiti incerti»[28]. Qualcuno esclude quindi decisamente che tale obbligo possa sussistere[29]. Altri, inve-

[27] Accinti (2017), cit., p. 6.

[28] Ivi, p. 560.

[29] Per Seminara (2014), cit., p. 602, non esiste ad oggi alcun obbligo di legge codificato che imponga all'Isp un controllo preventivo sui dati che circolano *online* grazie ai suoi servizi di intermediazione, né possibile ricavare interpretativamente un obbligo siffatto senza incorrere nel divieto di analogia *in malam partem* della legge penale. Non esiste quindi alcun obbligo giuridico di impedimento dei reati da parte dei *provider*. Così anche Miglio (2016), cit., pp. 7-8: «Orbene, appare dirimente segnalare sin da subito che non sembra potersi rinvenire, all'interno del nostro ordinamento, alcuna norma giuridica che impone, in capo al gestore (o amministratore di un gruppo), l'obbligo giuridico di impedire una diffamazione o, *rectius*, di impedire che taluno inserisca un commento diffamatorio o quanto meno di far sì che i commenti possano essere postati solo a valle di un vero e proprio controllo sul contenuto degli stessi». E a p. 9: «La mancata rimozione di un *post* consiste in una mera inerzia, totalmente neutra dal punto di vista soggettivo, che può essere dettata da una dimenticanza, da una mancata percezione del carattere dei contenuti pubblicati o da una me-

ce, propendono per la tesi dell'ammissibilità della responsabilità in capo all'Isp – particolarmente nel caso di un *social network provider* – per omesso impedimento dell'evento, almeno per quanto riguarda alcuni reati in materia di diritto d'autore, per i quali l'Isp sarebbe dotato di un effettivo potere-dovere di interferenza per impedire la prosecuzione delle violazioni dei diritti d'autore, se specificamente individuate e definite da provvedimenti cautelari o inibitori[30].

La giurisprudenza e la dottrina italiane hanno per lo più fatto riferimento alla concezione *formale* dell'obbligo di impedire l'evento, ritenendolo sussistente solo qualora una fonte formale lo riferisca a situazioni giuridiche tipizzate. Una di queste situazioni è quella rappresentata dalla *posizione di garanzia*, che può essere definita come «uno speciale vincolo di tutela tra un soggetto garante e un bene giuridico, determinato dall'incapacità (totale o parziale) del titolare a proteggerlo autonomamente»[31]. In realtà, non da tutte le posizioni di garanzia discendono obblighi giuridici di impedire gli eventi dannosi, ma solo da quelle per cui ciò è disposto da norme giuridiche. Quindi, fra posizione di garanzia e obbligo *ex* art. 40 c. p. un rapporto da *genus* a *species.* Le posizioni di garanzia possono essere originarie, cioè connesse allo specifico ruolo che il soggetto titolare riveste, oppure possono avere natura contrattuale, cioè derivare da un trasferimento negoziale. Inoltre, un'ulteriore distinzione va fatta fra le posizioni di garanzia intese come *protezione* (obbligo di preservare determinati beni giuridici a tutti i pericoli che possono minacciarne l'integrità) e quelle intese come *controllo* (obbligo di neutralizzare le fonti di pericolo da cui i beni giuridici protetti possono risultare minacciati).

Le principali posizioni di protezione si ritrovano nel diritto di famiglia e sono connesse allo speciale rapporto fra genitori e figli minori sancito dall'art. 30 della Costituzione e dall'art. 147 del codice civile. Si tratta in questo caso di posizioni originarie. Esse possono però anche derivare da un contratto (come nel caso del rapporto fra la *baby sitter* e i bambini cui essa deve badare per conto dei genitori). Fra le posizioni di controllo possiamo ricordare, a titolo esemplificativo, quella rivestita dal proprietario, possessore o custode di beni mobili e immobili, che è tenuto ad apprestare le misure di sicurezza idonee ad impedire il verificarsi di eventi dannosi, oppure quella di colui che è obbligato ad impedire l'agire illecito di un terzo (per esempio il tutore nei confronti dei soggetti sottoposti alla sua tutela).

ra noncuranza o disattenzione sullo sviluppo di una conversazione nel gruppo ma che, di per sé, nulla dice in merito alla consapevole adesione soggettiva del *webmaster* in merito ai contenuti non rimossi aventi carattere denigratorio».

[30] Flor (2012), cit., pp. 670-672 e 681-682.

[31] Ivi, p. 564.

Sempre come esempio, fra le posizioni di garanzia può essere annoverata quella del direttore responsabile di una testata giornalistica periodica (art. 57 c. p.) che ometta di esercitare il necessario controllo al fine di impedire la commissione di reati a mezzo stampa. In questo caso, però, la posizione di garanzia corrisponde a un reato omissivo *proprio*, cioè esplicitamente tipizzato dalla norma incriminatrice. Analoga posizione è rivestita, nel caso delle pubblicazioni non periodiche, dall'editore o dallo stampatore (art. 57 *bis* c. p.).

Tuttavia, la Corte di Cassazione nel 2010, con una sentenza molto discussa, ha precisato che, in virtù del divieto di applicazione analogica in *malam partem* delle norme penali, nonché per via della «assoluta eterogeneità della telematica rispetto agli altri media sinora conosciuti e, per quel che qui interessa, rispetto alla stampa», l'art. 57 c. p. non può applicarsi analogicamente al direttore di una testata periodica telematica, sia pure regolarmente registrata, così come la l'art. 58 c.p., riferito ad editori e stampatori di periodici "clandestini", non può applicarsi anche ai coordinatori di *blog* o *forum* telematici che, pur avendo carattere di periodicità, non sono ovviamente registrati. Questo orientamento, come si è già detto in precedenza, è stato parzialmente corretto da alcune sentenze successive. Nella medesima sentenza del 2010, la Corte, richiamando l'art. 14 del d. lgs. n. 70/2003, ha ribadito che «che non sono responsabili dei reati commessi in rete gli *access provider*, i *service provider* e – *a fortiori* – gli *hosting provider*, a meno che non fossero al corrente del contenuto criminoso del messaggio diramato (ma, in tal caso, come è ovvio, essi devono rispondere a titolo di concorso nel reato doloso e non certo *ex* art 57 c. p.)». Peraltro, è certamente corretto sostenere che, laddove il direttore responsabile di una testata giornalistica può effettivamente controllare il contenuto degli articoli pubblicati, siffatto controllo risulta impossibile per il *provider* in ragione della vastità e mutevolezza dei contenuti presenti *online*, con conseguente impossibilità di ricostruire l'omesso controllo in termini di responsabilità colposa *ex* art. 57 del codice penale[32].

Senza addentrarci nei meandri della dottrina penalistica, da quanto appena premesso appare chiaro che il punto fondamentale è stabilire se i *provider* – con particolare riferimento ai gestori delle piattaforme di *social networking* – siano titolari di posizioni di garanzia nei confronti degli eventi dannosi eventualmente cagionati dagli utenti e se, in ogni caso, siano soggetti all'obbligo giuridico di impedirli, onde evitare che possa essere loro imputato il reato omissivo improprio.

[32] Accinti (2017), cit., p. 4.

Per qualcuno[33], la fattispecie del reato omissivo improprio non è applicabile agli Isp per almeno quattro ragioni: in primo luogo, l'art. 17 comma 1 del d. lgs. n. 70/2003 ha escluso l'obbligo di sorveglianza dei *provider* sulle condotte degli utenti[34]; in secondo luogo, l'utente di per sé non può essere considerato un soggetto potenzialmente pericoloso per il quale sia necessario predisporre una posizione di controllo; in terzo luogo, non è configurabile un bene giuridico identificabile come "rete sana" rispetto al quale l'Isp possa essere posto in posizione di protezione; infine, per via dell'enorme mole di informazioni che transitano attraverso Internet, anche dal solo punto di vista tecnico il controllo da parte dell'Isp sarebbe impossibile o comunque troppo oneroso, pregiudicando la sua libertà di iniziativa economica. Peraltro, per il fatto che la posizione dell'Isp è sostanzialmente estranea all'attività degli utenti, il *provider* non può essere equiparato al coordinatore di un *blog* o di un *forum* telematico – per i quali potrebbe essere ipotizzata comunque una responsabilità penale a titolo di concorso nel reato – e men che meno al direttore di una testata giornalistica periodica[35]. Secondo questa ricostruzione, allora, la responsabilità dell'Isp verrebbe a configurarsi esclusivamente *ex post*, cioè solo per omesso impedimento della protrazione del reato, nel caso in cui l'Isp non ottemperi agli ordini di rimozione dei contenuti ricevuti dalle competenti autorità giudiziarie o amministrative[36].

Questa interpretazione è suffragata da una pronuncia del tribunale di Milano[37] relativa alla presunta responsabilità penale dell'intestatario di un sito che forniva *link* a un altro sito in cui era diffuso materiale pedopornografico. In tale occasione, il giudice collegiale ha stabilito che i *provider* appartenenti alle diverse categorie (*content provider*, *network provider*, *access provider*, *service provider*) non potessero essere ritenuti corresponsabili della distribuzione, divulgazione, pubblicizzazione e cessione a terzi del materiale pedopornografico. In capo ai *provider* non sarebbe infatti ravvisabile, nel diritto vigente, alcuna posizione di garanzia, sia perché l'attività da essi svolta non può essere considerata pericolosa, sia perché gli artt. 57 e 57-*bis* del codice penale non sono suscettibili di interpretazione analogica *in malam partem*. Parimenti, non graverebbe sui *provider* alcun

[33] Bartoli (2013), cit., pp. 602-603.

[34] Questo argomento è sostenuto anche da Accinti (2017), cit., p. 6, per il quale la richiamata disposizione comporta una vera e propria negazione di una posizione di garanzia in capo al *provider*, rendendo inapplicabile l'art. 40 c. p.

[35] Ivi, p. 604.

[36] Ivi, p. 606.

[37] Tribunale di Milano, quinta sezione, sentenza 25 febbraio 2004, n. 1993.

obbligo giuridico di impedimento, poiché non è ravvisabile la possibilità concreta di esercitare un efficace controllo sui contenuti.

Sulla stessa linea anche la sentenza di primo grado relativa al caso *Google c. Vividown*, che si è già ampiamente commentato nelle pagine precedenti[38]. L'impianto accusatorio nei confronti dei *manager* di *Google* era fondato proprio sull'assunto che essi avessero contravvenuto all'obbligo giuridico *ex* art. 40 c. p. in quanto avrebbero omesso di attuare le misure idonee ad impedire l'illecito trattamento dei dati personali da parte degli utenti. Tuttavia, il giudice non ha condiviso questa ricostruzione, escludendo la sussistenza di una posizione di garanzia dell'Isp rispetto alle condotte degli utenti. Infatti, «pur ammettendo per ipotesi che esista un potere giuridico derivante dalla normativa sulla *privacy* che costituisca l'obbligo giuridico fondante la posizione di garanzia, non vi è chi non veda che tale potere, anche se correttamente utilizzato, certamente non avrebbe potuto "impedire l'evento" diffamatorio. In altre parole, anche se l'informativa sulla *privacy* fosse stata data in modo chiaro e comprensibile all'utente, non può certamente escludersi che l'utente medesimo non avrebbe caricato il *file* video incriminato, commettendo il reato di diffamazione»[39]. La sentenza di appello[40] ha assolto gli imputati anche dall'accusa di aver commesso, in concorso fra loro, il reato di illecito trattamento dei dati personali al fine di trarne profitto. L'accusa aveva prospettato, fra l'altro, la tesi del concorso consistente in una condotta omissiva, ma il giudice di secondo grado ha osservato che trattamento illecito dei dati personali è un reato di pura condotta, mentre la sfera di applicabilità dell'art. 40, comma 2, del codice penale è limitata ai reati di evento[41].

Va anche ricordato che la sentenza della Corte di Cassazione (V sez. pen., 27 dicembre 2016, n. 54946), di cui si è parlato nel paragrafo precedente, sembra aver imputato al gestore del sito imputato una responsabilità per omesso impedimento degli effetti del reato altrui[42]. Si badi: non del reato altrui, ma solo dei suoi effetti. Non solo, infatti, il *leading case Google c. Vividown* ha escluso la possibilità di attribuire al *provider* l'obbligo di impedire un reato altrui, ma anche, essendo la diffamazione un reato istantaneo che si consuma nel momento della pubblicazione *online* del contenuto, non è possibile ascrivere ad alcuno la responsabilità per omesso impedimento di un reato già consumato. Non sembra quindi che, in questo caso, la Cassazione abbia inteso né modificare il suo precedente consolidato orien-

[38] Tribunale di Milano, quarta sezione penale, sentenza 24 febbraio 2010, n. 1972.
[39] Citazione tratta da p. 104 della sentenza.
[40] Corte d'Appello di Milano, sentenza 21 dicembre 2012, n. 8611.
[41] Si veda in proposito Giovannetti (2014), cit., p. 325.
[42] Ingrassia (2017), cit.

tamento in materia di momento consumativo del reato di diffamazione né attribuire ai *provider* una posizione di garanzia. L'imputato è stato infatti condannato per non aver interrotto gli effetti del delitto, cioè l'offesa alla reputazione altrui, arricchita e aggravata dalla possibilità per nuovi lettori di accedere alla pagina *web*.

Anche questa ricostruzione, però, non convince[43] poiché si tratta di un'imputazione penale atipica: nel vigente ordinamento giuridico, infatti, la responsabilità per omissione si rinviene solo nelle ipotesi tipiche relative alla tutela del diritto d'autore (art. 1, comma 6, d. l. n. 72/2004) e di prevenzione della diffusione di materiale pedopornografico (art. 14 *quater*, legge n. 269/1998), cui corrispondono elevate sanzioni pecuniarie in caso di trasgressione, mentre la disciplina del commercio elettronico (d. lgs. n. 70/2003) su cui si fonda in regime di responsabilità degli Isp non sanziona in alcun modo il *provider* che non si attivi per inibire l'accesso a contenuti illeciti. Inoltre, asserire che il gestore del sito, pur non essendo gravato di obblighi di sorveglianza *ex ante*, è tenuto a una autonoma valutazione *ex post* del carattere diffamatorio di taluni contenuti, decidendo discrezionalmente di rimuoverli, significa rendere i *provider* dei veri e propri censori della Rete.

Il problema è che la tesi della non sussistenza di responsabilità per omissione in capo agli intermediari digitali, se pur condivisibile sul piano giuridico per le motivazioni fin qui esaminate, alimenta «la preoccupazione per la lamentata esistenza di uno "statuto di impunità penale" per i "colossi" del *web*, che, allorquando non violino essi stessi una disposizione di legge, non potrebbero essere mai chiamati a rispondere del pur elevatissimo numero di illeciti commessi loro tramite»[44]. Alla luce dell'evoluzione del ruolo dei *provider*, e con particolare riferimento alla figura dell'*hosting provider* "attivo", di creazione giurisprudenziale[45], occorre piuttosto chiedersi se la più moderna natura dei servizi offerti sia ancora compatibile con il regime di irresponsabilità penale degli Isp[46].

Il modello che, in prospettiva *de jure condendo*, la dottrina maggioritaria sembra condividere è piuttosto quello di lasciare all'autorità giudiziaria la valutazione dell'illiceità dei contenuti, sancendo la responsabilità dell'Isp solo in caso di inerzia qualificata dal mancato adempimento di uno specifico provvedimento, sulla falsariga del meccanismo di *notice-and-take-down* prevista dalla disciplina del commercio elettronico e dalle disposizioni in

[43] Ingrassia (2017), cit., pp. 1265 ss.
[44] Accinti (2017), cit., p. 7.
[45] Si veda il terzo capitolo di questo libro.
[46] Accinti (2017), cit., p. 8.

materia di tutela delle opere dell'ingegno e di contrasto alla diffusione di materiale pedopornografico.

Secondo un'altra interpretazione[47], anch'essa suggerita solo in prospettiva *de jure condendo*, potrebbe essere introdotta dal legislatore una fattispecie di responsabilità oggettiva del *provider*, sulla falsariga della responsabilità amministrativa degli enti di cui al d. lgs. n. 231/2001, che corrisponderebbe sul piano penale alla responsabilità civile per danni causati da attività pericolose di cui all'art. 2050 c. c. Più precisamente, «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»[48].

[47] Miceli (2017), cit.
[48] Ivi, p. 115.

STRATEGIE DI CONTRASTO ALLA DIFFUSIONE DELLE MANIFESTAZIONI DI ODIO E DELLE NOTIZIE FALSE TRAMITE I *SOCIAL NETWORK*

1. Il contrasto allo *hate speech*: repressione penale e sistemi di autoregolamentazione

Che cosa si intenda esattamente con l'espressione *hate speech*, tradotta normalmente in Italiano come "discorsi d'odio" o "espressioni d'odio" o "linguaggio d'odio" non è del tutto chiaro, data l'assenza di una precisa norma definitoria[1]. Certamente, in via generale nel contesto europeo lo *hate speech* può essere ricondotto a una di quelle forme di discriminazione vietate dall'art. 14 della Cedu, in quanto consistente proprio in una violenza, realizzata attraverso modalità espressive verbali o audiovisive, atta a discriminare particolare categorie di individui[2]. Anche nel più ristretto ambito dell'Unione europea, il divieto di discriminazioni è un principio giuridicamente vincolante, sancito oggi dall'art. 21 della *Carta dei diritti fondamentali*[3] e ripreso dall'art. 19 del Trattato sul funzionamento dell'Unione europea[4]. Su queste basi, sono state adottate due importanti direttive: la direttiva

[1] A. G. Lana (2016), *Hate speech online: strategie di contrasto e prevenzione*, in *I diritti dell'uomo*, n. 3, p. 503.

[2] L'art. 14 della Cedu vieta ogni forma di discriminazione, in quanto incompatibile con il godimento dei diritti sanciti dalla Convenzione; in particolare, il divieto riguarda espressamente le discriminazioni «fondate sul sesso, la razza, il colore, la lingua, la religione, le opinioni politiche o quelle di altro genere, l'origine nazionale o sociale, l'appartenenza a una minoranza nazionale, la ricchezza, la nascita od ogni altra condizione».

[3] *Carta dei diritti fondamentali dell'Unione europea*, art. 21, comma 1: «È vietata qualsiasi forma di discriminazione fondata, in particolare, sul sesso, la razza, il colore della pelle o l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, il patrimonio, la nascita, la disabilità, l'età o l'orientamento sessuale».

[4] Art. 19 Tfue, comma 1: «Fatte salve le altre disposizioni dei trattati e nell'ambito delle competenze da essi conferite all'Unione, il Consiglio, deliberando all'unanimità secondo una procedura legislativa speciale e previa approvazione del Parlamento europeo, può pren-

2000/43/Ce del Consiglio, del 29 giugno 2000, che attua il principio della parità di trattamento fra le persone indipendentemente dalla razza e dall'origine etnica, e la direttiva 2000/78/Ce del Consiglio, del 27 novembre 2000, che stabilisce un quadro generale per la parità di trattamento in materia di occupazione e di condizioni di lavoro, indipendentemente dalla loro religione o convinzione personale, disabilità, età o orientamento sessuale. In ogni caso, lo *hate speech*, e particolarmente quello che si realizza attraverso Internet, è una specifica forma di discriminazione non espressamente contemplata dalla normativa suaccennata, che si estrinseca non attraverso azioni o omissioni, ma mediante deprecabili modalità di manifestazione del pensiero. Diffuse e reiterate attraverso Internet, tali forme espressive hanno l'effetto di alimentare i pregiudizi, consolidare gli stereotipi e rafforzare l'ostilità di taluni gruppi di persone, solitamente in maggioranza o in posizione di dominanza in un determinato contesto sociale, nei confronti di altri gruppi con diverse caratteristiche, in genere minoritari.

Un primo tentativo definitorio può rinvenirsi nella raccomandazione del Comitato dei Ministri del Consiglio d'Europa del 30 ottobre 1997[5], secondo la quale «the term "hate speech" shall be understood as covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, antisemitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin». Però questa definizione, oltre a non essere giuridicamente vincolante, essendo contenuta in un atto di *soft law*, non include fra le manifestazioni di odio taluni fenomeni fra cui, ad esempio, l'omofobia[6] o la

dere i provvedimenti opportuni per combattere le discriminazioni fondate sul sesso, la razza o l'origine etnica, la religione o le convinzioni personali, la disabilità, l'età o l'orientamento sessuale». Tale disposizione corrisponde all'art. 13 del precedente Trattato Ce.

[5] Recommendation No. R (97) 20, adopted by the Committee of Ministers on 30 October 1997, at the 607th meeting of the Minister's Deputies.

[6] Una definizione di odio omofobico può rinvenirsi nel punto B dei *Considerando* della risoluzione sulla lotta all'omofobia in Europa, approvata dal Parlamento europeo il 24 maggio 2012, n. 2012/2657(RSP): «Considerando che l'omofobia consiste nella paura e nell'avversione irrazionali provate nei confronti dell'omosessualità femminile e maschile e di lesbiche, gay, bisessuali e transgender (LGBT) sulla base di pregiudizi, ed è assimilabile al razzismo, alla xenofobia, all'antisemitismo e al sessismo; che si manifesta nella sfera pubblica e privata sotto diverse forme, tra cui incitamento all'odio e istigazione alla discriminazione, scherno e violenza verbale, psicologica e fisica, persecuzioni e uccisioni, discriminazioni a violazione del principio di uguaglianza e limitazione ingiustificata e irragionevole dei diritti, e spesso si cela dietro motivazioni fondate sull'ordine pubblico, sulla libertà religiosa e sul diritto all'obiezione di coscienza». In particolare, sulla giurisprudenza della Corte europea dei diritti dell'uomo relativamente all'omofobia si veda L. Goisis (2013), *Libertà d'espressione e odio omofobico. La Corte europea dei diritti dell'uomo equipara la discri-*

misoginia, né alcune altre forme di espressioni d'odio *ad personam*, fra cui ad esempio il *cyberbullying* o il *cyberstalking*.

Più in generale, sempre nell'ambito del Consiglio d'Europa, il Protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica firmato a Strasburgo il 28 gennaio 2003, relativo all'incriminazione di atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici, obbliga gli stati aderenti ad adottare sanzioni penali per punire la diffusione di materiale razzista e xenofobo attraverso i sistemi informatici, le minacce e gli insulti razzisti e xenofobi, la negazione, la minimizzazione, l'approvazione o la giustificazione di crimini di genocidio o contro l'umanità. La pertinente definizione, in questo caso, è quella di «any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors».

Non è esaustiva nemmeno la più recente definizione – stavolta giuridicamente vincolante – offerta, a livello di Unione europea, dalla decisione-quadro 2008/913/Gai del Consiglio del 28 novembre 2008 sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale. Tale decisione impegna gli Stati membri dell'Unione europea a rendere punibili i comportamenti di stampo razzista e xenofobo, in particolare «l'istigazione pubblica alla violenza o all'odio nei confronti di un gruppo di persone, o di un suo membro, definito in riferimento alla razza, al colore, alla religione, all'ascendenza o all'origine nazionale o etnica», nonché «l'apologia, la negazione o la minimizzazione grossolana dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra», quando però tali comportamenti siano posti in essere in modo atto a istigare alla violenza o all'odio nei confronti di gruppo – o di un suo membro – «definito in riferimento alla razza, al colore, alla religione, all'ascendenza o all'origine nazionale o etnica». Anche in questo caso, soltanto alcune fra le possibili categorie potenzialmente vulnerabili vengono indicate nella definizione, tralasciandone altre altrettanto rilevanti. Per questo il Parlamento europeo, con una risoluzione approvata il 14 marzo 2013, ha evidenziato l'esigenza di una revisione della decisione-quadro 2008/913/Gai, in modo da includervi anche le manifestazioni di antisemitismo, intolleranza religiosa, antiziganismo, omofobia e transfobia[7].

minazione in base all'orientamento sessuale alla discriminazione razziale, in *Rivista italiana di diritto e procedura penale*, n. 1, pp. 418-441.

[7] Risoluzione del Parlamento europeo del 14 marzo 2013 sul rafforzamento della lotta contro il razzismo, la xenofobia e i reati generati dall'odio, n. 2013/2543(RSP).

Se, dunque, un primo profilo problematico inerisce al reperimento di una definizione – normativa o di *soft law* – che sia davvero omnicomprensiva di tutte le possibili fattispecie attraverso cui le manifestazioni di odio possono estrinsecarsi, un secondo profilo di importanza non minore riguarda l'individuazione del confine esatto fra espressioni critiche, anche esageratamente veementi, e quelle di odio vero e proprio. La libertà di espressione, infatti, va garantita anche nei casi in cui possa risultare scomoda, sgradita, sopra le righe, offensiva, scioccante o disturbante[8]. Tuttavia, non bisogna dimenticare che proprio l'art. 10 della Cedu prevede al comma 2 che la libertà in questione possa incontrare delle limitazioni, purché previste dalla legge, proporzionate e necessarie al raggiungimento degli obiettivi propri di ogni società democratica, quali la sicurezza nazionale, l'integrità territoriale, la pubblica sicurezza, la difesa dell'ordine e la prevenzione dei reati, la protezione della salute o della morale, la protezione della reputazione o dei diritti altrui, la riservatezza di talune informazioni, la garanzia dell'autorità e dell'imparzialità del potere giudiziario.

Quindi, interrogata sulla legittimità e sulla proporzionalità di misure adottate a livello nazionale per reprimere o sanzionare le espressioni di

[8] S. Fois (1957), *Principi costituzionali e libera manifestazione del pensiero,* Milano, Giuffrè, pp. 159-160, rileva «l'incompatibilità costituzionale di ogni divieto che colpisca le manifestazioni del pensiero contrarie agli ordinamenti politici, sociali ed economici costituiti nello Stato» perché simili divieti «mirano alla difesa ad oltranza di un determinato "regime" politico e sociale» e «sono pensabili solo nell'ambito di un sistema non democratico e "totalitario»; quindi (pp. 167-168) sono consentite anche manifestazioni del pensiero rivoluzionarie, sovversive e sediziose, purché non comportino il passaggio dalle parole ai fatti, cioè all'uso della violenza. C. Esposito (1958), *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Milano, Giuffrè, p. 58, si dice convinto che «le affermazioni pericolose sarebbero state contraddette da altre che ne avrebbero posto in luce la pericolosità eliminandola, e la propaganda delle idee sovversive sarebbe stata vinta da quella delle idee costruttive e la verità avrebbe illuminato se stessa e l'errore»; dunque (p. 49), anche «la propaganda, l'apologia, la pubblica esaltazione e persino la manifestazione istigante alla realizzazione del pensiero espresso» costituiscono manifestazioni del pensiero costituzionalmente protette. Per P. Barile (1984), *Diritti dell'uomo e libertà fondamentali*, Bologna, Il Mulino, p. 266, l'art. 21 Cost. non ha inteso scriminare fra i vari scopi cui la libertà di manifestazione del pensiero può rivolgersi, e quindi «ogni manifestazione del pensiero gode della garanzia costituzionale, anche se tende a creare uno "stato emozionale"». Più in generale A. Pace ritiene che la categoria dei reati di opinione vada ricondotta alla lesione dell'ordine pubblico inteso strettamente in senso materiale (tutela della sicurezza e dell'incolumità pubblica, libero esercizio dei diritti costituzionali, esigenza di prevenzione e repressione dei reati) e che quindi un'eccessiva dilatazione del concetto di buon costume fino a ricomprendervi la "pubblica decenza" oppure del concetto di ordine pubblico fino a contemplare la lesione di un preteso "sentimento comune" finiscano per proiettare sulla libertà di manifestazione del pensiero un vincolo di natura ideale (cfr. A. Pace e M. Manetti (2006), *Art. 21. La libertà di manifestazione del proprio pensiero*, in G. Branca (a cura di), *Commentario della Costituzione*, Bologna, Zanichelli).

odio, la Corte di Strasburgo si è trovata più volte a dover operare un bilanciamento fra la protezione del diritto a manifestare liberamente il proprio pensiero e quella esigenze di tutela della società democratica espresse dal comma 2 dell'art. 10 Cedu. La Corte di volta in volta ha tenuto conto, senza seguire una costante e consolidata linea interpretativa e pervenendo a esiti differenti, della suscettibilità di talune manifestazioni del pensiero ad indurre in concreto ad atti di violenza, del loro impatto sull'ordine pubblico e sulla coesione sociale, dell'effettiva intenzione dell'autore delle espressioni contestate e del ruolo rivestito da tale persona nella società, del mezzo di comunicazione più o meno pervasivo attraverso cui lo *hate speech* è stato diffuso, dell'eventuale contesto artistico o satirico nell'ambito del quale tali espressioni hanno trovato luogo, del livello di vulnerabilità delle vittime delle espressioni di odio, soprattutto se minori, della particolare "sensibilità" del contesto politico-sociale in cui l'odio è stato espresso, infine del tipo e della gravità delle sanzioni comminate a livello nazionale ai responsabili delle condotte in questione. Il risultato di questa operazione per la verità non è stato particolarmente coerente nel corso del tempo[9]. La giurisprudenza più recente, comunque, sembra privilegiare la tendenza ad impedire almeno le manifestazioni più gravi delle opinioni che incitano all'odio e alla violenza, attraverso l'applicazione dell'art. 17 Cedu che vieta l'abuso di diritto[10]: l'art. 17 Cedu è stato talvolta impiegato come ausilio interpretativo all'art. 10 Cost., per valutare la necessità e la proporzionalità delle misure inibitorie e sanzionatorie irrogate dagli Stati nazionali ai responsabili di *hate speech*; talaltra invece, soprattutto nelle sentenze più recenti, l'art. 17 è stato impiegato in forma diretta, come causa di irricevibilità dei ricorsi, anche se in tal modo la Corte ha rinunciato a procedere al bilanciamento dei

[9] Non potendo approfondire in questa sede l'analisi della giurisprudenza della Corte europea dei diritti dell'uomo sullo *hate speech*, si rimanda a: P. Falletta (2015b), *Il contrasto all'hate speech*, in M. Mensi e P. Falletta (a cura di), *Il diritto del web. Casi e materiali*, Padova, Cedam, partic. pp. 187-192; P. Lobba (2014), *Il negazionismo come abuso della libertà di espressione: la giurisprudenza della corte di Strasburgo*, in *Rivista italiana di diritto e procedura penale*, n. 4, pp. 1815-1853; M. Orofino (2014), *La libertà di espressione tra Costituzione e carte europee dei diritti. Il dinamismo dei diritti in una società in continua trasformazione*, Torino, Giappichelli; O. Pollicino (2017a), *La prospettiva costituzionale sulla libertà di espressione nell'era di Internet*, in G. Pitruzzella, O. Pollicino e S. Quintarelli, *Parole e potere. Libertà d'espressione, hate speech e fake news*, Milano, Egea, pp. 1-55; M. Spatti (2014), *Hate speech e negazionismo tra restrizioni alla libertà d'espressione e abuso del diritto*, in *Studi sull'integrazione europea*, n. 9, pp. 341-358.

[10] Art. 17 Cedu: «Nessuna disposizione della presente Convenzione può essere interpretata nel senso di comportare il diritto di uno Stato, un gruppo o un individuo di esercitare un'attività o compiere un atto che miri alla distruzione dei diritti o delle libertà riconosciuti nella presente Convenzione o di imporre a tali diritti e libertà limitazioni più ampie di quelle previste dalla stessa Convenzione».

contrapposti interessi e a valutare l'effettiva necessità e proporzionalità delle misure restrittive della libertà di espressione[11].

Non è stata certamente la diffusione di Internet e dei siti di *social networking* a determinare il problema delle manifestazioni dell'odio. Tali forme espressive si sono sempre realizzate in passato, verbalmente o attraverso l'uso dei *media* tradizionali. Oggi però, tramite Internet e in particolare i *social network*, tali espressioni possono circolare con estrema rapidità, diffondersi su larghissima scala e raggiungere una enorme *audience*, con l'effetto di stimolare la proliferazione di ulteriori espressioni di tipo analogo. È indiscutibile che l'ambiente digitale – e in particolare quello dei *social network* – abbia un potere di diffusione e di pubblicità dell'odio ben maggiore rispetto ai media tradizionali, così come lo è il fatto che l'odio, una volta immesso in Rete, abbia una notevole capacità di persistenza e di resistenza ai tentativi di occultamento dei messaggi offensivi[12]. Un ulteriore elemento da considerare è il senso di impunità che deriva, per molti utenti di Internet, dalla (falsa) percezione di essere protetti dall'anonimato[13]. Quindi, la prima e più evidente ragione per cui il fenomeno dell'odio *online* è divenuto così preoccupante risiede nella capacità diffusiva della Rete: Internet come «mezzo facilitatore della diffusione e della potenzialità dell'odio che circola *online*»[14].

Una seconda ragione, invece, ha a che fare sugli effetti provocati dalle interazioni fra persone attraverso Internet in termini di estremizzazione – e quindi maggiore offensività – delle opinioni espresse. Come ha ben evidenziato Sunstein[15], i gruppi di persone che partecipano a un dibattito via Internet hanno la tendenza ad orientarsi ideologicamente verso posizioni estreme, tendenza che l'Autore definisce "polarizzazione di gruppo": «dopo un dibattito, l'opinione tende a spostarsi verso un punto estremo nella dire-

[11] Questo modo di procedere non va esente da critiche, su cui si veda Spatti (2014), cit., partic. pp. 353 ss.

[12] G. Ziccardi (2015b), *Internet e le espressioni d'odio: influenza della tecnologia e strategie di contrasto*, in *Ciberspazio e diritto*, n. 3, pp. 387-401.

[13] Secondo un documento pubblicato dall'Unesco nel 2015, intitolato *Countering online hate speech* (reperibile qui: http://unesdoc.unesco.org/images/0023/002332/233231e.pdf), i caratteri distintivi dell'odio espresso attraverso Internet rispetto a quello *offline* sarebbero i seguenti: la permanenza nel tempo della manifestazione di odio; il suo "ritorno imprevedibile", per via dello sfruttamento del medesimo contenuto da parte di utenti di varie piattaforme in tempi diversi; la percezione che sovente hanno gli autori dello *hate speech* di essere protetti dall'anonimato; la diffusione transnazionale dei contenuti e, conseguentemente, il loro maggiore impatto sociale rispetto ai contenuti *offline*; la diffusione di tali contenuti anche grazie ai *trending topics* selezionati dai principali *social network*.

[14] G. Ziccardi (2015b), cit., p. 387.

[15] C. R. Sunstein (2003), *Republic.com. Cittadini informati o consumatori di informazioni?*, Bologna, Il Mulino.

zione in cui i membri del gruppo erano originariamente orientati. Per quanto riguarda Internet e le nuove tecnologie di comunicazione, questo significa che gruppi di persone della stessa area ideologica, al termine di una discussione fra loro, finiranno per pensare la stessa cosa che pensavano prima, ma in forma più estremistica»[16]. Dunque, «Internet continua ad essere per molti un terreno fertile per l'estremismo, proprio perché persone della stessa area di pensiero trattano tra di loro con grande frequenza e facilità, e spesso senza sentire alcuna controparte. Un'esposizione ripetuta a una posizione estrema, unita all'idea che molte altre persone condividano quella posizione, prevedibilmente porterà le persone che vi sono esposte, e forse già propense, a credere in essa»[17]. Da questo punto di vista i *social network*, favorendo l'interazione e lo scambio di opinioni fra persone, non avrebbero un ruolo neutrale, ma agevolerebbero e amplificherebbero la diffusione di questo tipo di espressioni e la loro gravità.

Ciò considerato, rispetto all'atteggiamento da tenere per contrastare le manifestazioni di odio *online*, si fronteggiano due opposte correnti di pensiero[18]: un approccio secondo il quale la Rete andrebbe regolamentata più rigidamente, al fine di ostacolare la diffusione di opinioni discriminatorie e non rispettose del principio della dignità umana, e un altro secondo cui, invece, irreggimentare normativamente la libertà di espressione in Internet non servirebbe allo scopo ma, al contrario, avrebbe come conseguenza quella di alterare non solo il sistema di protezione della libertà di manifestazione del pensiero, ma anche le strategie commerciali dei grandi *player* dell'economia digitale.

L'approccio nordamericano, fondato sul primo emendamento della Costituzione, come è noto non tollera alcuna interferenza dei poteri pubblici nell'esercizio della *freedom of speech* e non prevede limitazioni con riguardo ai contenuti espressi o alle modalità con cui l'espressione avviene. Anche i messaggi più discutibili, impopolari e scabrosi, dunque, possono essere diffusi liberamente nel *free marketplace of ideas*[19], nel quale si presup-

[16] Ivi, p. 82.

[17] Ivi, p. 87.

[18] Riassunte da G. Ziccardi (2015a), *L'odio e la rete:un'introduzione e alcune possibili linee di ricerca*, in *Ciberspazio e diritto*, n. 2, pp. 255-267; G. Ziccardi (2015b), *Internet e le espressioni d'odio: influenza della tecnologia e strategie di contrasto*, in *Ciberspazio e diritto*, n. 3, pp. 387-401.

[19] Celebre metafora coniata dai giudici della Corte suprema statunitense Holmes e Brandeis nella *dissentig opinion* relativa al caso *Abrams v. United States* del 1919 e ripresa, con specifico riferimento a Internet, nel noto caso *Reno v. Aclu* del 1997. Tuttavia, anche il costituzionalismo americano non nega che l'esercizio del *free speech*, almeno nei casi in cui sia tale da determinare uno *strict and present danger* valutato in base a uno *strict scrutinty*, possa essere assoggettato a limitazioni per via legislativa (*dissenting opinion* del giudice

pone che la corretta informazione emerga attraverso il libero confronto fra idee contrastanti[20]. Per queste ragioni, ogni forma di responsabilizzazione degli intermediari digitali, soprattutto nel caso in cui preveda il ricorso a tecniche di filtraggio preventivo dei contenuti, è guardata con sospetto perché potrebbe dare luogo a forme di *collateral censorship*[21]. Il vigente art. 230 del *Communication Decency Act* (sect. *c*, 1), infatti, esclude categoricamente che il fornitore o l'utilizzatore di servizi interattivi digitali possa essere considerato responsabile, alla stregua di un editore (*publisher*), dei contenuti informativi prodotti da altri[22]. Eppure recentemente, dinanzi alla diffusione quella particolare – e particolarmente pericolosa – forma di *hate speech* attraverso i *social network* rappresentata dalla propaganda jihadista[23], anche negli Stati Uniti qualcuno inizia a sostenere la necessità di modificare il *Communication Decency Act*, prevedendo l'obbligo per i *provi-*

Holmes nel caso *Schenck v. United States* del 1919). Sul costituzionalismo americano in materia di *free speech* si veda O. Pollicino (2017a), cit., partic. pp. 23-27. Sulla metafora del *free marketplace of ideas*, fin dalle sue lontane origini risalenti al pensiero di John Milton e di John Stuart Mill, si veda G. De Gregorio (2017b), *The market place of ideas nell'era della post-verità: quali responsabilità per gli attori pubblici e privati online?*, in *Medialaws. Rivista di diritto dei media*, n. 1, pp. 91-105.

[20] Però «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"». Così M. Cuniberti (2017), *Il contrasto alla disinformazione in rete tra logiche del mercato e (vecchie e nuove) velleità di controllo*, in *Medialaws. Rivista di diritto dei media*, n. 1, p. 35. E ancora a p. 36: «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 inquietitudine, 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».

[21] J. M. Balkin (2014), *Old School/New School Speech Regulation*, in *Harward Law Review*, n. 127, pp. 2296–2342.

[22] «No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider».

[23] D. Cohen (2016), *The Evolution of Contemporary Terrorism in Cyberspace*, in *Gnosis. Rivista italiana di intelligence*, n. 2, pp. 118-127; M. Fiocca e al. (2016), *La Jihäd 2.0: profili economici, tecnologici, giuridici*, in *Ciberspazio e diritto*, n. 1-2, pp. 109-139; L. Scaife (2017), *Social Networks as the New Frontier of Terrorism*, New York, Routledge. Sugli esiti di taluni ricorsi giurisdizionali presentati dai parenti di alcune delle vittime di attentati terroristici di matrice jihadista contro i *social network* (soprattutto *Twitter*), considerati responsabili di aver contribuito alla diffusione e alla propaganda del terrorismo, si veda M. R. Allegri (2018), *Alcune considerazioni sulla responsabilità degli intermediari digitali, e particolarmente dei social network provider, per i contenuti prodotti dagli utenti*, in *Informatica e diritto*, in corso di pubblicazione.

der, in seguito a segnalazioni ricevute dagli utenti, di rendere inaccessibili i contenuti riferibili alla propaganda terroristica[24].

Nel contesto europeo invece, come si è visto *supra*, è la Cedu che giustifica talune limitazioni della libertà di espressione se necessarie allo sviluppo di una società democratica e che, in via generale, vieta che l'esercizio di qualsiasi diritto possa tradursi nell'eccessiva compressione dei diritti altrui. La possibilità di interventi normativi statali volti, da un lato, a sanzionare i responsabili delle manifestazioni del pensiero *contra ius* e, dall'altro, a regolare l'esercizio della libertà di espressione in Internet, anche attraverso interventi riguardanti gli intermediari digitali, non è esclusa in linea di principio, purché tali interventi normativi siano giudicati necessari e non sproporzionati rispetto all'obiettivo da raggiungere. Tuttavia, varie voci si oppongono alla tendenza alla repressione, attraverso gli strumenti del diritto penale nazionale[25], delle manifestazioni del pensiero riconducibili allo *hate speech*[26].

[24] S. Klein e C. Flinn (2017), *Social Media Compliance Programs and the War Against Terrorism*, in *Harvard National Security Journal*, n. 1, pp. 53-112; M. Rotter (2017), *With Great Power Comes Great Responsibility: Imposing a "Duty to Take Down" Terrorist Incitement on Social Media*, in *Hofstra Law Review*, n. 4, pp. 1379-1412; A. Tsesis (2017), *Terrorist Speech on Social Media*, in *Vanderbilt Law Review*, n. 2, pp. 651-708.

[25] In Italia, la legge n. 654 del 1957, con cui il nostro Paese ha ratificato la Convenzione di New York sull'eliminazione di tutte le forme di discriminazione razziale, punisce con pene reclusive chi *propaganda* idee fondate sulla superiorità o sull'odio razziale, ovvero *istiga* a commettere o commette atti di violenza o di provocazione alla violenza, nei confronti di persone perché appartenenti a un gruppo nazionale, etnico o razziale (art. 3 comma 1). Il dettato normativo oggi vigente è il risultato di una modifica avvenuta con legge n. 85 del 2006 che, oltre a ridurre i limiti edittali delle pene reclusive (peraltro già ridotti in precedenza con la "legge Mancino" del 1993) e a prevedere pene pecuniarie alternative alla reclusione, ha sostituito con «propaganda» la precedente espressione «diffonde in qualsiasi modo» e con «istiga» il precedente «incita». La modifica non è di poco conto, perché la qualificazione del reato deve oggi corrispondere a condotte di maggiore gravità (propaganda e istigazione in luogo di diffusione e incitamento). Già in precedenza, però, la "legge Mancino" (decreto legge n. 122 del 1993, convertito in legge n. 2015 del 1993) aveva ridotto i limiti edittali delle pene previste, distinto fra le condotte di incitamento alla discriminazione e quelle di incitamento alla violenza, e previsto due nuove fattispecie criminose: il reato commesso da chi a vario titolo partecipa ad associazioni, organizzazioni, movimenti o gruppi aventi finalità discriminatorie, e quello commesso da chi, in pubbliche riunioni, compie manifestazioni esteriori od ostenti emblemi o simboli propri o usuali delle organizzazioni, associazioni, movimenti o gruppi aventi finalità di discriminazione razziale. Va inoltre ricordata la legge n. 962 del 1967, che all'art. 8 sanziona l'apologia di genocidio e la pubblica istigazione a commettere qualcuno dei delitti di genocidio previsti dalla legge stessa. Più recentemente, la legge n. 115 del 2016 ha aggiunto un nuovo comma all'art. 3 della legge n. 654/1957, che prevede la reclusione da due a sei anni nei casi in cui la propaganda, l'istigazione e l'incitamento, commessi in modo che derivi concreto pericolo di diffusione, si fondino «in tutto o in parte sulla negazione della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra come definiti dallo Statuto della Corte pena-

Le ragioni addotte a sostegno di questa tesi sono molteplici: reprimere penalmente talune manifestazioni del pensiero in nome della tutela di "sentimenti" collettivi viola il principio di determinatezza e tassatività della fattispecie penale, oltre a privilegiare inevitabilmente il sentimento collettivo di taluni gruppi a discapito di altri[27]; ricostruire la libertà di espressione come esigenza funzionale ad interessi generali (l'ordine pubblico "ideale", la preservazione delle strutture dello Stato democratico) rischia di tradursi

le internazionale». È stato così inserito nel nostro ordinamento il cosiddetto "reato di negazionismo", già esistente in alcun Paesi europei ed extra-europei, come reazione al proliferare in Europa di movimenti di ispirazione razzista e antisemita. Tuttavia, se ben si comprendono le ragioni che sono alla base della previsione di questa nuova fattispecie penale, non si può non esprimere qualche perplessità circa il fatto che non è compito del diritto stabilire la verità o la falsità dei fatti storici. Proprio per questo, correttamente la nuova legge non punisce il negazionismo in sé e per sé, ma solo le opinioni negazioniste da cui derivi concretamente propaganda, istigazione o incitamento alla violenza o alla discriminazione. Va ricordata, infine, la legge n. 71 del 2017 volta a contrastare il fenomeno del cyberbullismo, con cui si intende «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» (art. 1 comma 2); la legge non prevede sanzioni penali, ma misure educative e preventive nonché procedure di *notice-and-take-down* affinché i contenuti offensivi vengano prontamente rimossi grazie al contributo proattivo degli intermediari digitali. Quando, come nel caso del cyberbullismo, l'odio *online* viene espresso nei confronti non di un gruppo di individui, ma di una specifica persona, le fattispecie penalmente rilevanti sono quelle "classiche" della diffamazione aggravata dall'utilizzo di un mezzo di pubblicità (art. 595 c. p.) e della minaccia (art. 612 c. p.) eventualmente aggravata (art. 339 c. p.). Ad esse si aggiunge il reato di atti persecutori (in cui rientra anche lo *stalking*) introdotto nel codice penale con decreto legge n. 11 del 2009; in questo caso, si tratta del reato commesso da «chiunque, con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita» (art. 612 *bis* c. p.). In una proposta di legge attualmente ferma in Senato (S. 2688, presentato il 7 febbraio 2017: «Disposizioni per prevenire la manipolazione dell'informazione *online*, garantire la trasparenza sul *web* e incentivare l'alfabetizzazione mediatica») la diffusione attraverso Internet «di campagne d'odio contro individui o di campagne volte a minare il processo democratico, anche a fini politici» verrebbe punita con reclusione non inferiore a due anni e con ammenda fino a diecimila euro.

[26] C. Caruso (2013), *Dignità degli "altri" e spazi di libertà degli "intolleranti". Una rilettura dell'art. 21 Cost*., in *Quaderni costituzionali*, n. 4, pp. 795-821; A. Pugiotto (2013), *Le parole sono pietre? I discorsi di odio e la libertà di espressione nel diritto costituzionale*, in *www.penalecontemporaneo.it*, pp. 1-18.

[27] Sulle perplessità relative all'utilizzo degli strumenti penalistici per tutelare il "comune sentimento" si vedano: F. Bacco (2013), *Dalla dignità all'eguale rispetto: libertà di espressione e limiti penalistici*, in *Quaderni costituzionali*, n. 4, pp. 823-848; F. Guella e C. Piciocchi (2013), *Libera manifestazione del pensiero tra fatti di sentimento e fatti di conoscenza*, in *Quaderni costituzionali*, n. 4, pp. 849-877.

in uno strumento nelle mani delle forze politiche dominanti per ostacolare la diffusione di idee antagoniste alle proprie; l'esercizio della libertà di espressione è funzionale alla formazione di un discorso pubblico, che può avvenire solo in uno spazio di neutralità, in modo che attraverso il confronto delle idee si costituiscano le basi per la reciproca comprensione e per la composizione dei conflitti identitari; l'esclusione di alcuni voci "disturbanti" dal dibattito pubblico può essere percepita come il tentativo di garantire un'ingiustificata posizione privilegiata solo ad alcuni gruppi culturali, traducendosi quindi in una forma di discriminazione; la nozione costituzionale di dignità umana non è un principio assoluto, ma un concetto relazionale (pari dignità sociale, art. 3 Cost.) e culturalmente orientato, che non può e non deve essere utilizzato a sostegno del sistema assiologico-normativo imposto dal gruppo sociale dominante; il principio di uguaglianza sostanziale (art. 3 Cost., comma 2) non può essere realizzato attraverso la repressione penalistica, ma solo attraverso strumenti promozionali; l'idea che non sia da reprimere il pensiero "puro", ma solo quello suscettibile di tradursi in azioni concrete incompatibili con l'ordine costituzionale (Corte costituzionale, sentenze n. 120 del 1957 e n. 100 del 1966), limita la garanzia dell'art. 21 Cost. alle sole forme di pensiero del tutto innocue, e quindi per lo più irrilevanti; il rispetto degli obblighi internazionali di natura pattizia, imposto dal primo comma dell'art. 117 Cost., non è messo in discussione, poiché né la Cedu né altre fonti del diritto internazionale impongono agli Stati aderenti l'adozione di sanzioni penali, ma si limitano ad ammetterne la possibilità, condizionata al vaglio di proporzionalità e necessità.

Una possibilità alternativa agli strumenti normativi repressivi, o comunque integrativa rispetto a questi ultimi, può essere rappresentata dai sistemi di autoregolamentazione. Proprio in questo senso si sono espressi, in una dichiarazione comune, i ministri della giustizia e degli interni dei paesi membri dell'Unione europea, riuniti in un Consiglio straordinario sugli attentati terroristici di Bruxelles (24 marzo 2016). Nel documento si sottolinea la necessità che la Commissione europea si faccia promotrice, presso le aziende informatiche, dell'attivazione di un processo volto a contrastare la propaganda terroristica in Internet e a mettere a punto un codice di condotta contro l'incitamento all'odio *online*. Peraltro, già da dicembre 2015 è attivo, su iniziativa della Commissione europea, un *Internet Forum*, che riunisce i Ministri degli Interni degli Stati membri dell'Unione europea, i rappresentanti dei principali fornitori di servizi via Internet, del Parlamento europeo, di *Europol*, nonché il coordinatore europeo per la lotta al terrorismo. L'obiettivo del Forum, da raggiungere attraverso un approccio volontario basato su una partnership pubblico-privata, è quello di individuare strategie per ostacolare la diffusione di contenuti che inneggiano all'odio, alla vio-

lenza e al terrorismo internazionale. Anche in base ai risultati dei lavori del Forum, le conclusioni del Consiglio europeo del 22-23 giugno 2017 hanno indicato chiaramente fra le priorità la lotta contro il terrorismo, l'odio e l'estremismo violento e il contrasto alla diffusione della radicalizzazione *online*, sollecitando lo sviluppo di nuove tecnologie e nuovi strumenti per migliorare la rilevazione e la rimozione automatiche dei contenuti che promuovono l'istigazione alla violenza.

Conseguentemente, il 31 maggio 2016 la Commissione europea, di concerto con *Facebook*, *Twitter*, *YouTube* e *Microsoft*, ha varato un Codice di condotta[28] in base al quale le aziende informatiche si impegnano a predisporre procedure chiare ed efficaci per esaminare le segnalazioni di contenuti incitanti all'odio da parte degli utenti dei loro servizi, in modo da poter rimuovere tali contenuti o renderli inaccessibili. Si legge infatti nel Codice: «Se da un lato l'applicazione effettiva delle disposizioni che prevedono il reato di incitamento all'odio dipende dall'esistenza di un solido sistema di applicazione delle sanzioni penali contro i singoli autori dei discorsi di incitamento all'odio, dall'altro questa azione deve essere integrata da iniziative atte a garantire che appena ricevono una valida segnalazione gli intermediari *online* e le piattaforme dei media sociali reagiscano prontamente, in tempi idonei, per contrastare le forme illegali di incitamento all'odio *online*. Per essere considerata valida, la segnalazione dovrebbe essere sufficientemente precisa e adeguatamente fondata». Con il Codice, quindi, le *web companies* aderenti si sono impegnate ad implementare un sistema di *notice-and-take-down* tale per cui i contenuti "odiosi" siano rimossi o resi inaccessibili entro ventiquattro ore dalla segnalazione a cura degli utenti, a collaborare «con le organizzazioni della società civile per fornire formazione sulle migliori pratiche per lottare contro la retorica dell'odio e i pregiudizi» e a incrementare «la portata del loro approccio proattivo nei confronti delle organizzazioni della società civile per aiutarle a realizzare campagne efficaci di lotta contro i discorsi di incitamento all'odio».

Un aspetto problematico rappresentato dal Codice – i risultati della cui applicazione da parte delle *web companies* aderenti vengono monitorati e valutati ogni sei mesi[29] – è che fra gli impegni che le imprese aderenti han-

[28] *Code of conduct on countering illegal hate speech online*. Il testo del Codice, anche in lingua italiana, è disponibile qui: http://ec.europa.eu/newsroom/just/itemdetail.cfm?item_id=54300.

[29] Dalla pagina *web* http://europa.eu/rapid/press-release_IP-17-1471_en.htm (*link* in fondo alla pagina) è possibile scaricare i *factsheets* relativi alla prima e alla seconda valutazione semestrale dei risultati ottenuti dal *Code of conduct*. Sugli risultati ottenuti nei primi mesi di applicazione si veda F. Pizzetti (2017), *Fake news e allarme sociale: responsabilità, non censura*, in *Medialaws. Rivista di diritto dei media*, n. 1, p. 57.

no assunto vi è anche quello di «di proseguire l'opera di elaborazione e promozione di narrazioni alternative indipendenti, di nuove idee e iniziative e di sostegno di programmi educativi che incoraggino il pensiero critico»: ciò potrebbe essere interpretato come una sorta di "licenza" di manipolare le informazioni di cui godrebbero gli operatori del *web*, in contrasto con il principio di libera manifestazione del pensiero. In linea generale, può essere discutibile affidare ad alcuni grandi aziende private – che rappresentano comunque solo una piccola parte degli operatori del *web* – il delicato compito di vagliare la fondatezza e l'attendibilità delle segnalazioni dei loro utenti circa contenuti incitanti all'odio e alla violenza e di decidere quali contenuti sia opportuno rimuovere, senza che la decisione sia assistita da una procedura in contraddittorio o da garanzie giurisdizionali.

2. Libera manifestazione del pensiero, dovere di verità e notizie false

Fake news: notizie false oppure anche solo distorte o artefatte, purché clamorose, in grado di catturare l'attenzione del pubblico, di suscitare reazioni emotive e di rimanere impresse nella mente[30]. Le *fake news* vengono diffuse per molteplici finalità: influenzare l'opinione pubblica a fini di propaganda politica, orientare (surrettiziamente) la comunicazione scientifica, ridefinire la conoscenza del passato e suggerire visioni del futuro, pubblicizzare prodotti commerciali o servizi, incrementare gli accessi degli utenti

[30] Sul fenomeno delle *fake news*, sulla loro rilevanza dal punto di vista giuridico, sulle cause della loro diffusione e su possibili strategie di contrasto si vedano: M. Bassini e G. E. Vigevani (2017), *Primi appunti su fake news e dintorni*, in *Medialaws. Rivista di diritto dei media*, n. 1, pp. 11-22; M. Cuniberti (2017), *Il contrasto alla disinformazione in rete tra logiche del mercato e (vecchie e nuove) velleità di controllo*, in *Medialaws. Rivista di diritto dei media*, n. 1, pp. 26-40; G. De Gregorio (2017b), *The market place of ideas nell'era della post-verità: quali responsabilità per gli attori pubblici e privati online?*, in *Medialaws. Rivista di diritto dei media*, n. 1, pp. 91-105; C. Melzi d'Eril (2017), *Fake news e responsabilità: paradigmi classici e tendenze incriminatrici*, in *Medialaws. Rivista di diritto dei media*, n. 1, pp. 60-67; M. Monti (2017a), *Le "bufale" online e l'inquinamento del public discourse*, in P. Passaglia e D. Poletti (a cura di), *Nodi virtuali, legami informali: Internet alla ricerca di regole*, Pisa University Press, pp. 179-192; M. Monti (2017b), *Fake news e social network: la verità ai tempi di Facebook*, in *Medialaws. Rivista di diritto dei media*, n. 1, pp. 79-90; C. Pinelli (2017), *"Postverità", verità e libertà di manifestazione del pensiero*, in *Medialaws. Rivista di diritto dei media*, n. 1, pp. 41-47; G. Pitruzzella (2017), *La libertà di informazione nell'era di Internet*, in G. Pitruzzella, O. Pollicino e S. Quintarelli, *Parole e potere. Libertà d'espressione, hate speech e fake news*, Milano, Egea, pp. 55-98; F. Pizzetti (2017), *Fake news e allarme sociale: responsabilità, non censura*, in *Medialaws. Rivista di diritto dei media*, n. 1, pp. 48-59; O. Pollicino (2017b), *Fake News, Internet and Metaphors (to be handled carefully)*, in *Medialaws. Rivista di diritto dei media*, n. 1, pp. 23-25; C. R. Sunstein (2010), *Voci, gossip e false dicerie*, Milano, Feltrinelli, 2010.

a una piattaforma informatica al fine di aumentarne il valore per gli inserzionisti pubblicitari. Il fenomeno ha assunto oggi dimensioni massicce, tanto che l'*Oxford Dictionary* ha proclamato come parola dell'anno 2016 la post-verità (*post-truth*)[31].

Le "bufale" certamente sono sempre esistite, non solo nell'ambito delle "chiacchiere fra amici", ma anche nel mondo dell'informazione professionale. Oggi però, tramite i *social network*, le *fake news* riescono a circolare con una velocità e una capacità di diffusione enormemente superiore al passato. Le ragioni di questo fenomeno sono state perfettamente spiegate da Sunstein[32] già da alcuni anni. In estrema sintesi, la circolazione delle *fake news* è favorita dal fatto che i *social network* formano un sistema di comunicazione fortemente decentralizzato, privo di barriere all'ingresso, di *gatekeeper* del flusso informativo e dei meccanismi di controllo e di responsabilità giuridicamente previsti per gli editori; inoltre, i sistemi di condivisione delle informazioni su cui si basano i *social network* contribuiscono alla propagazione delle notizie che più catturano l'attenzione degli utenti, sempre meno propensi a prestare fiducia ai media tradizionali e sempre più inclini a cercare *online* una conferma ai propri pregiudizi. Il punto è che più un'informazione – vera o falsa che sia – diventa "virale", maggiori saranno i guadagni per gli inserzionisti pubblicitari che traggono vantaggio dal gran numero dei fruitori di tale informazione, e quindi anche per i gestori dei *social media* che, utilizzando algoritmi che valorizzano taluni contenuti rispetto ad altri in base al numero delle interazioni fra gli utenti, riescono a selezionare le notizie più "appetibili" e a raccogliere intorno ad esse inserzioni pubblicitarie mirate.

Inoltre, studi recenti hanno messo in luce come l'individuo all'interno dei *social network* tenda ad esse condizionato da ciò che la maggioranza pensa; quindi se le *fake news* sono condivise da persone aventi molti legami virtuali con persone non connesse fra loro (rete non selettiva), la notizia falsa avrà più probabilità di essere ritenuta affidabile dalla maggioranza rispetto al caso in cui la sua diffusione avvenga per opera di qualcuno che ha connessioni solo all'intero di una rete selettiva (cioè una rete più ristretta, formata da persone tutte a loro volta interconnesse fra loro)[33].

Ma quale rilevanza ha il fenomeno delle notizie false dal punto di vista giuridico? È possibile rinvenire nel diritto positivo il divieto di distorcere la realtà e di diffondere, in nome del diritto a manifestare liberamente il proprio pensiero, informazioni non attendibili?

[31] https://en.oxforddictionaries.com/word-of-the-year/word-of-the-year-2016.

[32] C. R. Sunstein (2010), cit.

[33] K Lerman e al. (2016), *The "Majority Illusion" in Social Networks*, in *Plos One*, https://doi.org/10.1371/journal.pone.0147617, pp. 1-13.

2.1. La verità come bene giuridico costituzionalmente protetto

La risposta a tale interrogativo è assai complessa e non univoca. Si può assumere come punto di partenza l'antica contrapposizione fra Immanuel Kant e Benjamin Constant[34]: secondo Kant, la verità era un imperativo categorico, inderogabile, valido in qualsiasi circostanza, tanto che persino la menzogna a fin di bene era da considerarsi una condotta soggettivamente opportunistica; Constant, invece, riteneva che i principi astratti della morale non potessero essere applicati ai casi concreti senza essere temperati da principi intermedi, fra cui quello per cui nessuno avesse diritto a una verità che nuocesse ad altri. Attualizzando il discorso e calandolo nel contesto di uno Stato democratico costituzionale, anziché in quello della Francia post-rivoluzionaria, la questione va impostata in altri termini, e cioè se siano (costituzionalmente) legittime norme di diritto positivo che puniscano la falsità in sé, in quanto contraria al "patto sociale" che lega gli individui appartenenti allo Stato-comunità, o se piuttosto la repressione penale del falso debba essere in qualche modo relativizzata, ancorata cioè alla lesione di beni giuridici costituzionalmente protetti.

La soluzione al problema è stata individuata da Peter Häberle[35] nel senso che la ricerca della verità rappresenta la meta ultima dello stato costituzionale[36], essendo la verità un concetto inscindibile da quelli di giustizia e bene comune[37], pur nella consapevolezza della fallacia dell'uomo: «La pluralità delle verità, il fallire, l'errare umano, il sapere che ogni ricerca della verità resta perlopiù impantanata nelle procedure del "ricercare", tutto ciò non può indurci a congedarci dal concetto di verità o addirittura a rigettarlo in quanto giuridicamente irrilevante, "platonico", "formula vuota". Come si è detto, dopo l'esperienza del suo contro modello totalitario, lo stato costituzionale non può rinunciare alla verità come valore costituzionale. L'hobbesiano *auctoritas non veritas facit legem* non è la verità degli stati costituzionali»[38].

Venendo al contesto italiano, già nel dibattito intorno all'art. 21 Cost. occorso in sede di Assemblea costituente era emersa la preoccupazione per gli effetti che la pubblicazione per le notizie false e inventate avrebbe potuto avere sulla "fede pubblica"; per questo, la prima sottocommissione nella seduta del 27 settembre 1946 aveva licenziato una versione del quinto comma dell'art. 16 – poi divenuto art. 21 Cost. – secondo cui la legge pote-

[34] I. Kant e B. Constant (1996), *La verità e la menzogna*, Milano, Mondadori.
[35] P. Häberle (2000), *Diritto e verità*, Torino, Einaudi.
[36] Ivi, p. 99.
[37] Ivi, p. 106.
[38] Ivi, p. 105.

va stabilire controlli per l'accertamento delle fonti delle notizie e dei mezzi di finanziamento della stampa periodica. Sebbene il riferimento al controllo delle fonti sia poi caduto nella definitiva versione dell'articolo, per tema che ciò potesse comportare una limitazione della libertà di stampa ad opera del governo, nella seduta pomeridiana dell'Assemblea costituente del 14 aprile 1947 vennero espressi timori per il disorientamento dell'opinione pubblica che la circolazione di eventuali notizie false avrebbe potuto determinare, tanto da mettere a repentaglio la sicurezza del Paese[39].

Fra i primi interpreti della Carta costituzionale, Sergio Fois ha rilevato l'inapplicabilità in concreto del requisito della verità dei fatti inteso troppo rigidamente, in considerazione della velocità con cui gli organi di informazione diffondono le notizie, e ha evidenziato la necessità di un adattamento del principio della verità alle esigenze della cronaca in termini di mera verosimiglianza; ciò in considerazione dell'applicabilità del divieto di notizie false solo nel caso in cui la falsità pregiudichi l'esercizio di diritti costituzionalmente protetti[40].

Carlo Esposito[41] ha poi chiarito che il diritto a manifestare il *proprio* pensiero sancito dall'art. 21 Cost. esclude «le manifestazioni che non rispondono alle interiori persuasioni o all'interiore pensiero, le affermazioni o le negazioni che non corrispondono alle effettive convinzioni e valutazioni»[42]. In altre parole, l'art. 21 Cost. non protegge anche la diffusione di idee *consapevolmente* false, consentendo al legislatore ordinario di vietare, a tutela della fede pubblica, «il subiettivamente falso, la menzogna (deformante, reticente, patente, latente), il dolo, l'inganno, il raggiro, la frode, ove sia raggiunta la prova della divergenza della espressione dall'interiore pensiero»[43]. In linea con la giurisprudenza della Corte costituzionale in tema di ordine pubblico[44], per Esposito la libertà di manifestazione del pensiero non

[39] Si veda su questo Monti (2017b), cit., p. 82.

[40] S. Fois (1957), cit., pp. 208-212.

[41] C. Esposito (1958), cit.

[42] Ivi, p. 36.

[43] Ivi, p. 37.

[44] Corte costituzionale, sentenza 23 giugno 1956, n. 2, secondo la quale sono da considerarsi pericolose per l'ordine pubblico le «manifestazioni esteriori di insofferenza o di ribellione ai precetti legislativi ed ai legittimi ordini della pubblica Autorità, manifestazioni che possono facilmente dar luogo a stati di allarme e a violenze, indubbiamente minacciose per la "sicurezza" della generalità dei cittadini». Per la Corte, il concetto di sicurezza non va ristretto alla sola incolumità fisica, ma ha «il significato di situazione nella quale sia assicurato ai cittadini, per quanto è possibile, il pacifico esercizio di quei diritti di libertà che la Costituzione garantisce con tanta forza. Sicurezza si ha quando il cittadino può svolgere la propria lecita attività senza essere minacciato da offese alla propria personalità fisica e morale; è l'"ordinato vivere civile", che è indubbiamente la meta di uno Stato di diritto, libero e democratico».

può né turbare la pace sociale né andare contro i principi dell'ordinamento costituzionale[45]; fermo restando tale limite, l'art. 21 Cost. consente e garantisce anche forme espressive quali «la propaganda, l'apologia, la pubblica esaltazione e persino la manifestazione istigante alla realizzazione del pensiero espresso»[46].

Anche per Alessandro Pace[47] il "subiettivamente falso" va escluso dalla garanzia dell'art. 21 Cost., e pertanto il legislatore è libero di limitare le manifestazioni del pensiero non corrispondenti alle interiori persuasioni di chi lo manifesta; tuttavia, poiché l'elemento dirimente consiste nell'interiore persuasione del soggetto, può considerarsi tutelata dall'art. 21 Cost. anche la diffusione di informazioni e notizie false, che però il soggetto esternante ritiene essere vere in buona fede; il diritto di mentire consapevolmente è giuridicamente ammissibile solo nella misura in cui costituisce un aspetto del diritto inviolabile di difendersi in ogni stato e grado del giudizio (art. 24 Cost., comma 2).

A prescindere dalla consapevolezza del falso da parte del soggetto che si esprime, il punto è che, data la libertà di diffondere il proprio pensiero con ogni mezzo protetta dall'art. 21 Cost., la diffusione di notizie false non può essere considerata illecita in sé e per sé, ma solo quando il fine di inganno costituisca il frutto di attività illecite in quanto contrastanti con i principi costituzionali. Così secondo Paolo Barile[48], secondo il quale nemmeno l'obbligo di "aderenza ai fatti" richiesto al giornalista corrisponde alla verità, posto che «ricamare sui fatti esposti è sempre lecito»[49].

Se si assume, dunque, che è legittimo reprimere la circolazione di notizie false solo nel caso in cui dalla falsità deriva la lesione di beni giuridici di rilevanza costituzionale, ci si chiede se le *fake news* ledano, appunto, il "diritto ad essere informati" che la dottrina quasi unanime riconduce al profilo passivo della libertà di manifestazione del pensiero *ex* art. 21 Cost. Ma questo ragionamento sottintende una concezione "funzionale" della libertà di manifestazione del pensiero, secondo la quale quest'ultima dovrebbe essere garantita solo nei limiti della sua "utilità" rispetto alla preservazione e al consolidamento delle strutture dello stato democratico-costituzionale[50]. In ossequio a tale concezione, la libertà di diffondere anche notizie false o

[45] Esposito (1958), cit., p. 48.

[46] Ivi, p. 49.

[47] A. Pace e M. Manetti (2006), cit., pp. 88-96.

[48] P. Barile (1975), *Libertà di manifestazione del pensiero*, Milano, Giuffrè, pp. 17-18; Id. (1984), cit., p. 229.

[49] Ivi, p. 238.

[50] Sulla contrapposizione fra concezione funzionale e concezione individualistica della libertà di manifestazione del pensiero si veda A. Di Giovine (1988), *I confini della libertà di manifestazione del pensiero*, Milano, Giuffré, pp. 96 ss.

distorte andrebbe limitata, non possedendo in effetti tali notizie un reale contenuto informativo. Al contrario, se si privilegia una visione della libertà di manifestazione del pensiero come libertà individuale di stampo liberale, non si può non considerare che anche le *fake news*, pur nella loro inattendibilità, possono contribuire alla formazione dell'opinione pubblica e che la ricetta da contrapporre alle pretese censorie può essere quella di una sempre maggiore circolazione di informazioni, accompagnata da strumenti che permettano agli utenti il discernimento critico dei contenuti informativi[51].

2.2. L'obbligo della verità nella professione giornalistica

Se però assumiamo come punto di riferimento l'informazione giornalistica di natura professionale, non vi è alcun dubbio circa la sussistenza di un "dovere di verità" nel diritto positivo. I giornalisti sono tenuti al rispetto della verità dei fatti non solo come obbligo deontologico[52], ma anche in base all'art. 2 della legge 3 febbraio 1963, n. 69, che qualifica il rispetto della verità sostanziale dei fatti come un «obbligo inderogabile»[53].

Su queste basi, come ha chiaramente argomentato la Corte di Cassazione in una importante sentenza di pochi anni fa, «la libertà di opinione, nella dimensione del diritto di informazione, pur in presenza di ampia tutela costituzionale, non può travalicare lo scopo di informazione della collettività e tradursi in una divulgazione – indipendente dalla legalità – di notizie non vere o tendenzialmente rappresentate, limitando così i diritti della persona, costituenti patrimonio morale di ogni essere umano»[54]. In conclusione, ha proseguito la Cassazione, «l'affermato intreccio del dovere del giornalista

[51] Bassini e Vigevani (2017), cit., pp. 18-19.

[52] L'art. 2 lett. *a* del *Testo unico dei doveri del giornalista* stabilisce che il giornalista «ricerca, raccoglie, elabora e diffonde con la maggiore accuratezza possibile ogni dato o notizia di pubblico interesse secondo la verità sostanziale dei fatti». Inoltre, secondo l'art. 9 del Testo unico, il giornalista «rettifica, anche in assenza di specifica richiesta, con tempestività e appropriato rilievo, le informazioni che dopo la loro diffusione si siano rivelate inesatte o errate» (lett. *a*), «controlla le informazioni ottenute per accertarne l'attendibilità» (lett. *d*) e «non omette fatti, dichiarazioni o dettagli essenziali alla completa ricostruzione di un avvenimento».

[53] Legge n. 69 del 1962, art. 2: «È diritto insopprimibile dei giornalisti la libertà d'informazione e di critica, limitata dall'osservanza delle norme di legge dettate a tutela della personalità altrui ed è loro obbligo inderogabile il rispetto della verità sostanziale dei fatti, osservati sempre i doveri imposti dalla lealtà e dalla buona fede. Devono essere rettificate le notizie che risultino inesatte e riparati gli eventuali errori. Giornalisti e editori sono tenuti a rispettare il segreto professionale sulla fonte delle notizie, quando ciò sia richiesto dal carattere fiduciario di esse, e a promuovere lo spirito di collaborazione tra colleghi, la cooperazione fra giornalisti e editori, e la fiducia tra la stampa e i lettori».

[54] Corte di Cassazione, quinta sezione penale, sentenza 26 settembre 2012, n. 41249.

di informare e del diritto del cittadino di essere informato merita rilevanza e tutela costituzionale se ha come base e come finalità la verità e la sua diffusione. Se manca questa base di lancio, se non c'è verità, ma calcolata e calibrata sua alterazione, finalizzata a disinformare e a creare inesistenti responsabilità e a infliggere *fantasiose* condanne agli avversari, il richiamo a nobili e intangibili principi di libertà è intrinsecamente offensivo per la collettività e storicamente derisorio, beffardo per coloro che, in difesa della libertà di opinione, hanno sacrificato la propria vita. In un ordinamento e in una società che vivono e si sviluppano grazie al confronto d'idee, non può avere alcun riconoscimento l'invocato diritto di mentire, al fine di esercitare la libertà di opinione»[55].

A proposito del significato del termine "verità" in relazione all'informazione giornalistica, la Corte di Cassazione ha avuto modo di precisare, in varie occasioni, che «la verità dei fatti, cui il giornalista ha il preciso dovere di attenersi, non è rispettata quando, pur essendo veri i singoli fatti riferiti, siano, dolosamente o anche soltanto colposamente, taciuti altri fatti, tanto strettamente ricollegabili ai primi da mutarne completamente il significato. La verità non è più tale se è "mezza verità" (o comunque, verità incompleta): quest'ultima, anzi, è più pericolosa della esposizione di singoli fatti falsi per la più chiara assunzione di responsabilità (e, correlativamente, per la più facile possibilità di difesa) che comporta, rispettivamente, riferire o sentire riferito a sé un fatto preciso falso, piuttosto che un fatto vero sì, ma incompleto. La verità incompleta (nel senso qui specificato) deve essere, pertanto, in tutto equiparata alla notizia falsa»[56]. Inoltre, la verità non sussiste «quando i fatti riferiti siano accompagnati da sollecitazioni emotive ovvero da sottintesi, accostamenti, insinuazioni o sofismi obiettivamente idonei a creare rappresentazioni della realtà oggettiva false (in tutto o in parte) nella mente del lettore (o ascoltatore) in parte rilevante»[57]. La verità, raggiunta perseguendo con perizia e attenzione la corrispondenza tra fatti accaduti e fatti narrati «non può trovare equivalenti né nella verosimiglianza, ossia nel mero aspetto di verità che i fatti possono avere, né nella veridicità, ossia nell'attendibilità della fonte da cui la notizia di essi è attinta»[58]. Non esistono infatti fonti informative privilegiate

[55] *Ibid.*

[56] Corte di Cassazione, prima sezione civile, sentenza 18 ottobre 1984, n. 5259.

[57] Corte di Cassazione, terza sezione civile, sentenza 19 gennaio 2007, n. 1205.

[58] Corte di Cassazione, quinta sezione penale, sentenza 21 gennaio 1986. Mentre per Fois (1957), cit., pp. 211-212, è sufficiente che la cronaca rispetti il principio di verosimiglianza, per Barile (1984), cit., p. 238, il concetto di verosimiglianza è aberrante, perché una notizia verosimile può essere in realtà falsa, mentre una inverosimile può essere vera. Sempre Barile (1975) cit., p. 37, sottolinea come degradare la verità a verosimiglianza significhi attribuire alla stampa una causa di giustificazione praticamente illimitata; tuttavia, data

che svincolino il giornalista dall'onere di esaminare, controllare e verificare i fatti oggetto della sua narrazione, al fine di rispettarne la verità sostanziale[59].

Da queste e da altre pronunce della suprema Corte[60] si evince che alla verità fattuale può essere equiparata anche la "verità putativa" (cioè quella ritenuta tale dal giornalista in buona fede), purché il giornalista, prima di pubblicare la notizia, non abbia trascurato di valutare accuratamente i fatti e le circostanze e purché egli sia in grado di fornire la prova in giudizio degli elementi che lo hanno indotto in errore: l'errore non deve cioè fondarsi su una mera valutazione soggettiva dei fatti e delle circostanze, su elementi obiettivi tali da aver ragionevolmente indotto nel giornalista un'erronea convinzione.

Nel giornalismo di inchiesta, poi, è consentito esprimere in forma dubitativa, purché motivata e argomentata, sospetti di eventuali illeciti, accanto a suggerimenti rivolti agli organi inquirenti sulla direzione delle indagini e denunce di situazioni oscure su cui andrebbe fatta luce: l'importante è che il sospetto e la denuncia siano esternati sulla base di elementi obiettivi e rilevanti e non attraverso affermazioni capziose, suggestive, volte a spacciare un sospetto per verità conclamata[61].

In base a queste regole, si può sostenere senza tema di smentita che la pubblicazione di informazioni false o distorte ad opera di testate giornalistiche telematiche sia illegittima, oltre che contraria alla deontologia professionale[62], e che di ciò devono rispondere, sia dinanzi all'Ordine dei Giornalisti sia in sede processuale, i giornalisti autori degli articoli contenenti *fake news* e/o i direttori responsabili delle testate *ex* art. 57 c. p. A tal fine, però, è necessario che qualcuno, ritenendosi danneggiato dalla diffusione della notizia inattendibile, presenti un esposto all'Ordine dei Giornalisti o sporga querela per diffamazione contro l'autore dell'articolo e il direttore della testata, oppure esperisca nei loro confronti l'azione risarcitoria per danno ingiusto in sede civile *ex* art. 2043 c. c. Inutile dire che, tranne

l'impossibilità di pervenire ad una verità in senso assoluto, si richiede al cronista la semplice "aderenza ai fatti", raggiunta attraverso un accurato controllo sulle fonti svolto in buona fede.

[59] Corte di Cassazione, sezioni unite civili, sentenza 23 ottobre 1984, n. 8959.

[60] Fra le quali le seguenti sentenze emesse dalla terza sezione civile della Corte di Cassazione: 16 maggio 2007, n. 11259; 14 ottobre 2008, n. 25157; 3 marzo 2010, n. 5081; 3 ottobre 2013, n. 22600; 13 ottobre 2016, n. 20617.

[61] Corte di Cassazione, quinta sezione penale, sentenza 12 dicembre 2012, n. 9337.

[62] Tuttavia P. Barile (1975), cit.,p. 17, si è espresso molto criticamente contro tutte le ricostruzioni per cui, in nome della garanzia di cui all'art. 21 Cost., sarebbero vietate le notizie di cronaca non rispettose della verità, «come se la verità fosse sempre e soltanto una, e bastasse sollevare il moggio per scoprirla, e non farlo significasse malafede o dolo».

nei casi in cui la notizia falsa riguardi singole persone che possono avere un diretto interesse a ricorrere in giudizio, spessissimo le *fake news* riguardano tematiche di interesse generale, che è assai arduo ricondurre alla lesione di un diritto individuale.

Inoltre, l'obbligo inderogabile del rispetto della verità di cui all'art. 2 della legge n. 69 del 1963 può essere fatto valere solo nei confronti di coloro che possono rientrare nella categoria dei giornalisti propriamente detti, cioè gli iscritti all'Albo dei Giornalisti in qualità di professionisti o pubblicisti, nonché gli iscritti nell'elenco dei praticanti. Analogamente, solo costoro sono assoggettati al controllo e alla disciplina cui è preposto l'Ordine dei Giornalisti. Dunque, se le norme suaccennate possono rappresentare un argine – comunque fragile – alla diffusione di *fake news* tramite gli organi di informazione *online* dotati di una qualche "ufficialità" (testate telematiche registrate oppure siti Internet, *blog* e profili *social* riconducibili a giornalisti professionisti o pubblicisti), a nulla valgono contro il proliferare di informazioni inattendibili, diffuse e riproposte da tutti gli utenti di Internet non qualificabili come giornalisti.

Il problema è che oggi, a fronte di regole normative e deontologiche destinate solo a chi svolge la *professione* giornalistica, l'attività giornalistica – intesa come «prestazione del lavoro intellettuale volta alla raccolta, al commento e all'elaborazione di notizie destinate a formare oggetto di comunicazione interpersonale attraverso gli organi di informazione»[63] – può di fatto essere svolta da chiunque grazie alle opportunità offerte dai *new media*, con un livello di serietà, impegno e attendibilità estremamente variabile, in forma del tutto de-regolamentata. Data una situazione – già ben delineata nei capitoli precedenti di questo libro – in cui gli utenti dei *social network* sono essi stessi produttori di contenuti informativi e in cui i gestori delle piattaforme di *social networking* svolgono un ruolo sempre più simile a quello degli editori tradizionali, ci si chiede se non sia il caso di aggiornare le vigenti regole relative all'attività giornalistica, in modo da tenere in considerazione anche il vastissimo ed eterogeneo settore dell'informazione non professionale, al fine di migliorare la qualità dell'informazione nel suo complesso. In quest'ottica, la distinzione fra informazione professionale e non professionale non dovrebbe più essere affidata a regole di diritto pubblico relative ai soggetti (abilitazione professionale) o al prodotto (registrazione della testata), ma all'autorevolezza della fonte riconosciuta dai suo utenti: si tratta però di un parametro assai sfuggente e soprattutto incline ad essere condizionato da meccanismi di persuasione occulta e di condiziona-

[63] Corte di Cassazione, sezione lavoro, sentenza 20 febbraio 1995 n. 1827.

mento propri delle logiche del mercato, prestandosi ad interpretazioni arbitrarie[64].

2.3. La diffusione notizie false come pericolo per l'ordine pubblico

Al di là di quanto previsto per la professione giornalistica, esiste nell'ordinamento giuridico italiano una norma generale rappresentata dall'art. 656 del codice penale, che punisce con pene reclusive o pecuniarie di modesta entità[65]«chiunque pubblica o diffonde notizie false, esagerate o tendenziose, per le quali possa essere turbato l'ordine pubblico»[66]. Solo un concreto pregiudizio all'ordine pubblico, dunque, e non la semplice disinformazione, può determinare l'applicazione della fattispecie, che la dottrina dominante ricostruisce come reato di pericolo concreto.

Bisogna però distinguere la notizia falsa in senso oggettivo da quelle manifestazioni di opinioni personali che, proprio in quanto tali, difettano di una assoluta obiettività. Quindi, dalle affermazioni false va distinto il diritto di critica, che rientra nella libertà di manifestazione del pensiero costituzionalmente tutelata, in quanto fondata sull'interpretazione soggettiva di fatti e comportamenti, che esprimono l'opinione di chi la manifesta[67]. Parimenti, in un contesto satirico non rileva la verità dell'affermazione, poiché «il diritto di satira, a differenza da quello di cronaca, è sottratto al parametro della verità del fatto»[68], purché, però, la satira resti confinata all'ambito di espressione artistica che mira all'ironia sino al sarcasmo ed alla irrisione di chi eserciti un pubblico potere; se invece, sia pure in veste satirica, l'espressione del pensiero ha un contenuto informativo, occorre rispettare la verità dei fatti e non riferire notizie false[69].

La Corte costituzionale, chiamata a decidere della legittimità dell'art. 656 c. p. con riferimento all'art. 21 Cost., ha spiegato che «l'espressione

[64] Cuniberti (2017), cit., p. 37.

[65] Si tratta di un reato contravvenzionale. Le pene consistono nell'arresto fino a tre mesi o nell'ammenda fino a trecentonove euro.

[66] Su questa figura di reato si veda E. Dinacci (2014), *Divulgazione di notizie false*, in *http://www.treccani.it/enciclopedia/divulgazione-di-notizie-false_(Diritto-on-line)/*, nonché alla vasta bibliografia ivi citata. Si veda inoltre M. Bardi (2012), *Difendersi dalle notizie: il sistema normativo posto a tutela della sicurezza e dell'ordine pubblico minacciati dall'informazione*, in *Crimen et delictum*, n. 4, partic. pp. 85 ss.

[67] Corte di Cassazione, quinta sezione penale, sentenza 6 dicembre 1993, n. 112111. Più recentemente: quinta sezione penale, sentenze 7 giugno 2006, n. 19509; 24 novembre 2014, n. 48712. Inoltre terza sezione civile, 14 marzo 2016, n. 4897.

[68] Corte di Cassazione, terza sezione civile, sentenza 7 aprile 2016, n. 6787.

[69] Corte di Cassazione, prima sezione penale, sentenza 16 marzo 2006, n. 9246; quinta sezione penale, sentenza 18 ottobre 2012, n. 5065.

"notizie false, esagerate o tendenziose" impiegata nell'art. 656 del cod. pen. è una forma di endiadi, con la quale il legislatore si è proposto di abbracciare ogni specie di notizie che, in qualche modo, rappresentino la realtà in modo alterato»[70]; che l'art. 21 Cost. sancisce la libertà di manifestare il pensiero, ma «non importa tuttavia in alcun caso un "esonero da responsabilità" per il pensiero ormai manifestato»[71]; che la finalità dell'art. 656 c. p. è quella di preservare l'ordine pubblico, che è un bene collettivo «inteso nel senso di ordine legale su cui poggia la convivenza sociale»[72]; che «l'esigenza dell'ordine pubblico, per quanto altrimenti ispirata rispetto agli ordinamenti autoritari, non è affatto estranea agli ordinamenti democratici e legalitari, né è incompatibile con essi. In particolare, al regime democratico e legalitario, consacrato nella Costituzione vigente, e basato sull'appartenenza della sovranità al popolo (art. 1), sull'eguaglianza dei cittadini (art. 3) e sull'impero della legge»[73]. Quindi, è indubbio che «il mantenimento [dell'ordine pubblico] – nel senso di preservazione delle strutture giuridiche della convivenza sociale, instaurate mediante le leggi, da ogni attentato a modificarle o a renderle inoperanti mediante l'uso o la minaccia illegale della forza – sia finalità immanente del sistema costituzionale».

In una sentenza successiva[74], la Corte ha ribadito che «la tutela costituzionale dei diritti, come quello cui ha riguardo l'art. 21, ha sempre un limite non derogabile nell'esigenza che attraverso il loro esercizio non vengano sacrificati beni anche essi voluti garantire dalla Costituzione, e che tale deve ritenersi non solo la tutela del buon costume, cui l'articolo stesso fa espresso riferimento, ma anche il mantenimento dell'ordine pubblico, che è da intendere come ordine legale su cui poggia la convivenza sociale. Ora non sembra contestabile che anche la diffusione di notizie comunque consapevolmente inventate o alterate, così da non corrispondere alla realtà effettuale, deve ritenersi suscettibile di compromettere l'ordine che si vuole

[70] Corte costituzionale, sentenza 16 marzo 1962, n. 19. Tuttavia, già alcuni anni prima di questa sentenza Fois (1957) cit., p. 223, aveva giudicato costituzionalmente inammissibile l'accostamento delle notizie esagerate o tendenziose a quelle false: se infatti la falsità poteva rappresentare un pericolo per l'ordine pubblico, non altrettanto poteva dirsi per l'esagerazione e la tendenziosità, essendo queste ultime caratteristiche non solo largamente comuni alla cronaca contemporanea, ma anche imprecise e quindi facilmente soggette ad arbitraria interpretazione e applicazione. Così anche P. Barile (1953), *Il soggetto privato nella Costituzione italiana*, Padova, Cedam, p. 121, per il quale le notizie esagerate o tendenziose rientrano nell'interpretazione soggettiva di notizie vere, a differenza delle notizie del tutto false.

[71] Sentenza della Corte costituzionale citata nella nota precedente.

[72] *Ibid.*

[73] *Ibid.*

[74] Corte costituzionale, sentenza 19 dicembre 1972, n. 199.

proteggere, allorché, in considerazione del contenuto delle medesime o delle circostanze di tempo e di luogo della diffusione stessa, risultino idonee a determinare un turbamento consistente nell'insorgenza di un completo ed effettivo stato di minaccia dell'ordine stesso». Questo principio, però, non si traduce nel divieto di critica delle istituzioni pubbliche e del sistema politico e di governo, in quanto «la semplice e generica contrarietà agli ordinamenti costituiti non può essere titolo sufficiente a giustificare il divieto in uno stato democratico, che non solo consente la critica alle istituzioni vigenti, ma anzi da essa trae alimento per assicurare, in una libera dialettica delle idee, l'adeguamento delle medesime ai mutamenti intervenuti nella coscienza sociale»[75]. Infine, con una terza sentenza[76] la Corte ha escluso che il diritto a manifestare liberamente il proprio pensiero protetto dall'art. 21 Cost. possa legittimamente comportare una lesione del bene dell'ordine pubblico inteso nel senso indicato nelle sentenze precedenti.

Nel caso di moltissime *fake news*, è assai arduo rinvenire un pericolo (non potenziale, ma concreto e attuale) per l'ordine pubblico; tuttavia in qualche caso – si pensi alle campagne contro le vaccinazioni, sulla base di presunti pericoli per la salute dei bambini scientificamente non dimostrati, oppure alla capacità di talune campagne di disinformazione di influenzare gli esiti delle elezioni politiche, come avvenuto nel caso delle ultime elezioni americane – è possibile sostenere ragionevolmente che l'ordine pubblico sia stato turbato. Anche in questi casi, però, l'applicazione della norma penale risulta praticamente impossibile, perché praticamente impossibile è individuare i singoli responsabili della diffusione della notizia falsa attraverso i *social network*; inoltre, anche qualora ciò avvenisse, occorrerebbe dimostrare in giudizio l'intenzionalità della condotta (cioè la consapevolezza della falsità dell'informazione pubblicata), posto che la dottrina dominante propende per la ricostruzione della fattispecie come ipotesi prevalentemente dolosa, residuando la punibilità a titolo di colpa solo nel caso di errore inescusabile[77].

Tra l'altro, sempre più spesso oggi le notizie false non vengono diffuse da persone fisiche, ma da sistemi informatici automatici che simulano la comunicazione umana (i cosiddetti *bot*, abbreviazione di *robot*) e che

[75] *Ibid.*

[76] Corte costituzionale, sentenza 3 agosto 1976, n. 210.

[77] Del resto, configurare l'ipotesi colposa del reato di diffusione di notizie false significherebbe, nel caso della diffusione di queste ultime tramite i *social network*, poter sanzionare anche l'utente che impropriamente condivida la notizia senza verificarne l'attendibilità. Si veda M. Monti (2017a), p. 188.

vengono usati per la creazione di contenuti[78]: questi strumenti vengono sovente utilizzati per rendere più efficiente e potenziare il lavoro delle redazioni giornalistiche, talvolta possono servire anche a combattere la disinformazione e lo *hate speech* attraverso strategie automatizzate di moderazione dei contenuti[79], ma sempre più spesso purtroppo vengono utilizzati per manipolare l'opinione pubblica (*robotrolling*)[80], tanto da suscitare recentemente anche l'allarme della Nato per le possibili ripercussioni sulla stabilità delle istituzioni democratiche di alcuni paesi[81]. In questi casi, appare assai problematico individuare chi possa essere ritenuto responsabile – non solo giuridicamente, ma anche eticamente – dello scorretto utilizzo dei *bot*[82], provocando un pericolo per l'ordine pubblico.

Tralasciando momentaneamente il problema – certamente destinato ad attirare l'attenzione del giurista negli anni a venire – dell'attribuzione della responsabilità in caso di utilizzo di strumenti automatizzati, è evidente che la questione dell'"obbligo di verità" giuridicamente vincolante rileva non tanto dal punto di vista dell'esistenza delle garanzie normative in tal senso, quanto da quello della loro reale efficacia, sia per via del rapido mutamento dei processi di informazione e comunicazione dovuti alle innovazioni tecnologiche, sia per via dell'inadeguatezza dei sistemi giuridici nazionali a regolare fenomeni che travalicano i confini dello Stato.

[78] S. Di Gennaro (2017), *Cosa sono i content-bot e come ci ruberanno il mestiere*, in *http://www.ninjamarketing.it/*; F. Ferrando (2017), *Ecco Heliograf, il reporter-robot del Washington Post*, in *http://tg24.sky.it/tecnologia/*. Inoltre Pizzetti (2017), cit., p. 52 e p. 53, che sottolinea come l'uso dei *bot* talvolta sia finalizzato non tanto a distorcere la notizia, ma a incrementare gli accessi alla stessa.

[79] S. Moraca (2017), *Loudemy, una piattaforma italiana per combattere l'odio online*, in *Wired.it*. Il sito di *Loudemy* è www.loudemy.com. Sui rimedi tecnici per realizzare una efficace *content moderation*, con particolare riferimento a quelli utilizzati da *Google* e da *Facebook*, si veda S. Quintarelli (2017), *Content moderation: i rimedi tecnici*, in G. Pitruzzella, O. Pollicino e S. Quintarelli, *Parole e potere. Libertà d'espressione, hate speech e fake news*, Milano, Egea, pp. 99-146.

[80] A. Kleckova e F. Naumann (2017), *I, the Robotroll: Kremlin on Twitter*, in *http://4liberty.eu/*.

[81] Si veda in proposito la ricerca pubblicata dallo Strategic Communication Centre of Excellence della Nato in *Robotrolling*, n. 2017-1 (https://www.stratcomcoe.org/robotrolling-20171) e n. 2017-2 (https://www.stratcomcoe.org/robotrolling-20172).

[82] C. Alves de Lima e N. Berente (2017), *Is That Social Bot Behaving Unethically?*, in *Communications of the ACM*, n. 9, pp. 29-31; S. Wolley e al. (2017), *Il Manifesto dei Bot*, in https://motherboard.vice.com/it/.

2.4. Tentativi di reazione alla proliferazione delle fake news *e dell'odio* online

Altrettanto inefficaci sembrano essere gli strumenti di rettifica previsti dall'ordinamento giuridico nazionale per tutelare non solo diritti della personalità dei singoli, ma anche l'interesse pubblico all'obiettività dell'informazione[83], tanto più che nessuno di tali rimedi è specificamente applicabile alle notizie false diffuse attraverso Internet né, in generale, alle informazioni diffuse attraverso organi "informali" di diffusione delle notizie, come *social network* o *blog*.

Anche volendo immaginare – come ha fatto una recente proposta di legge di iniziativa parlamentare (on. Gambaro e altri) al momento giacente in Senato[84] – che l'amministratore della «piattaforma informatica destinata alla pubblicazione o diffusione di informazione presso il pubblico» sia tenuto a pubblicare le rettifiche richieste da coloro che ritengono che le informazioni pubblicate ledano la loro dignità o siano contrarie a verità, i nodi problematici non verrebbero sciolti, ma resi semmai ancora più intricati. In primo luogo, infatti, la proposta legislativa non chiarisce se la nozione di «piattaforma informatica destinata alla pubblicazione o diffusione di informazione presso il pubblico» possa comprendere anche i *social network*: il tenore letterale della disposizione lascia presupporre che non sia così, e che l'intenzione dei proponenti sia stata quella di considerare solo i siti *web* dedicati all'informazione, anche se non qualificabili come testate registrate (quindi prevalentemente i *blog*). In secondo luogo, il gestore della piattaforma sarebbe tenuto ad ottemperare alle richieste di rettifica provenienti dagli utenti, senza poter vagliare in alcun modo la loro fondatezza, in assenza di qualsiasi procedura in contraddittorio volta ad accertarla. In terzo

[83] Corte costituzionale, sentenza 15 maggio 1974, n. 133. Il diritto a chiedere e ottenere la rettifica delle notizie false o inesatte diffuse dagli organi di informazione è previsto in materia di stampa dall'art. 8 della legge n. 47 del 1948 e in materia radiotelevisiva dall'art. del d. lgs. n. 277 del 2005, mentre il corrispondente dovere in capo ai giornalisti è sancito, oltre che dalla deontologia professionale, anche dall'art. 2 della legge n. 69 del 1963. Sulla rettifica come mezzo di contrasto alle *fake news* si veda Monti (2017b), cit., pp. 85-86. L'Autore ritiene che non sia più rimandabile l'approvazione di una regolamentazione che permetta di applicare l'istituto della rettifica anche ai *social network*. Infatti, l'eventuale correzione della notizia scorretta sul sito *web* che la ha proposta non impedirebbe la circolazione della notizia falsa fra gli utenti dei *social network*. Di conseguenza, l'unico rimedio efficace potrebbe essere quello di affiancare alla rettifica sul sito sorgente anche una rettifica all'interno del *social network*, per esempio nella sezione dedicata alle *news* o nelle pagine personali dei singoli utenti che hanno condiviso o commentato la notizia falsa.

[84] S. 2688, presentato il 7 febbraio 2017, intitolato «Disposizioni per prevenire la manipolazione dell'informazione *online*, garantire la trasparenza sul *web* e incentivare l'alfabetizzazione mediatica». Si vedano in proposito le osservazioni di Cuniberti (2017), cit., pp. 29 ss.

luogo, poiché i gestori delle piattaforme verrebbero gravati dell'onere di controllare sistematicamente l'attendibilità e la veridicità delle informazioni immesse *online*, si rileva che tale delicato compito verrebbe delegato interamente a soggetti privati, che probabilmente opererebbero in base ai propri interessi – primo fra tutti quello di evitare le sanzioni previste a loro carico per la mancata rimozione dei contenuti inattendibili – e non all'interesse pubblico a ricevere le informazioni[85]. Ciò non solo darebbe luogo a forme di "censura privata" dell'informazione[86], ma contrasterebbe con la posizione di neutralità rispetto agli *user-generated contents* che la direttiva europea sul commercio elettronico avrebbe previsto per gli intermediari digitali. Infine, appare discutibile la scelta di reprimere penalmente, con sanzioni che possono arrivare a cinquemila euro, la pubblicazione su piattaforme informatiche di notizie false, esagerate o tendenziose anche a prescindere dalla loro capacità di turbare l'ordine pubblico[87], perché colpirebbe il falso in sé e per sé e non, come messo in luce dalla dottrina costituzionalistica riassunta nelle pagine precedenti, per la sua eventuale idoneità a pregiudicare un bene giuridico costituzionalmente protetto[88]. Riassumendo, almeno due motivi portano a ritenere inappropriata la repressione penale del falso: «l'ostilità ad affidare ad un organo statale, dotato di poteri coercitivi, la

[85] Particolarmente discutibile è infatti l'art. 5, secondo il quale i gestori delle piattaforme informatiche sono tenuti ad effettuare un costante monitoraggio dei contenuti diffusi attraverso le stesse, con particolare riguardo ai contenuti verso i quali gli utenti manifestano un'attenzione diffusa e improvvisa, per valutarne l'attendibilità e la veridicità. I gestori sono tenuti a rimuovere dalla piattaforma i contenuti giudicati da essi stessi inattendibili, anche in base alle segnalazioni ricevute dagli utenti e, qualora non provvedano, sono soggetti a sanzioni pecuniarie. Come si vede, la procedura non prevede alcun contraddittorio con gli utenti della piattaforma, né alcun controllo ad opera di un'Autorità amministrativa indipendente o giurisdizionale.

[86] M. Bettoni (2011), *Profili giuridici della privatizzazione della censura*, in *Ciberspazio e diritto*, n. 4, pp. 363-383. A p. 369 l'Autore scrive: «sono i soggetti privati coloro che hanno nella propria disponibilità la gestione dell'infrastruttura delle telecomunicazioni, a partire dalle piattaforme con cui il cittadino digitale interagisce […]. Da questa disponibilità diretta della materialità dei beni coinvolti, dati e relativi canali di trasmissione, discende che le attività di sorveglianza e prevenzione e quelle specifiche di controllo e repressione, che comportano interventi proprio su quegli stessi canali di comunicazione e su quei dati trasmessi, possono essere condotte con estrema agilità da parte degli stessi intermediari, operatori commerciali o meno, ai diversi livelli sui quali si trovino ad operare, rispetto a quanto non potrebbe fare direttamente lo Stato».

[87] Nel caso in cui le notizie false, esagerate o tendenziose siano tali da destare pubblico allarme o recare nocumento agli interessi pubblici o fuorviare settori dell'opinione pubblica sarebbe prevista una pena reclusiva non inferiore a dodici mesi e un'ammenda fino a cinquemila euro.

[88] Sul "ddl Gambaro" si vedano: Cuniberti (2017), cit., pp. 29 ss.; Melzi d'Eril (2017), cit., pp. 62 ss.; Monti (2017b), cit., p. 87.

possibilità di attribuire patenti di verità» e «la estrema difficoltà, a volte la impossibilità, di distinguere il grano del vero dal loglio del falso»[89].

Il problema è che, nell'attuale sistema dei mezzi di comunicazione, la disinformazione si diffonde frammentato e polarizzato, in assenza di contraddittorio, moltiplicando i rischi di manipolazione dell'utente. Ciò che più conta, quindi, non è tanto reprimere la disinformazione, ma aumentare i mezzi attraverso cui il contraddittorio in Rete possa esplicarsi[90]. Più in generale, il concetto di pluralismo rapportato al sistema dell'informazione *online* andrebbe ripensato e concettualizzato sotto forma di impegno delle istituzioni pubbliche a fornire ai cittadini strumenti critici per l'approccio e l'utilizzo della rete[91]. Ma per il momento, al di là di qualche dichiarazione di principio, questo obiettivo resta confinato nel regno delle buone intenzioni.

La proposta di legge Gambaro è stata motivata, pur con risultati insoddisfacenti, dall'intento di rispondere alla risoluzione n. 2143, intitolata *Online media and journalism: challenges and accountability*, adottata il 25 gennaio 2017 dall'Assemblea parlamentare del Consiglio d'Europa, sulla base di un rapporto preparato dal Committee on Culture, Science, Education and Media, di cui è stata relatrice la stessa on. Gambaro. Nella risoluzione l'Assemblea ha espresso preoccupazione per il gran numero di campagne mediatiche atte a sviare l'opinione pubblica attraverso false informazioni, e di manifestazioni di odio *online* volte a pregiudicare la partecipazione politica democratica. Per questo, gli Stati membri sono stati invitati ad adottare misure legislative e tecniche per prevenire il rischio che l'opinione pubblica sia distorta o manipolata dalle informazioni scorrette, a far sì che i servizi pubblici di informazione esercitino «the greatest editorial diligence with regard to user-generated or third-party content published on their internet portals», a inserire la «media literacy» nei programmi scolastici, a cooperare con i *provider* per la definizione di linee-guida volte ad ostacolare la diffusione di contenuti illeciti *online*, con particolare riguardo quelli incitanti all'odio e alla violenza. Analogamente, ai «professional media» viene chiesto di «uphold their editorial standards in their internet presence, including their own media content, advertising, third-party content, as well as user-generated content such as feedback or comments by users», posto che «all third-party content posted on the websites of professional media falls under the editorial responsibility of these media». Infine, gli *Internet service provider* sono stati invitati a mantenere la massima trasparenza su even-

[89] Melzi d'Eril (2017, cit., p. 63.
[90] Cuniberti (2017), cit., p. 39.
[91] *Ibid.*

tuali interessi commerciali, politici o di altra natura in grado di pregiudicare la loro posizione di neutralità, a sollecitare gli utenti a segnalare la presenza *online* di notizie false, a correggere o a rimuovere le informazioni distorte, ad adottare meccanismi di allerta e di esclusione nei confronti dei *troll*, ovvero di coloro che «regularly post insulting or inflammatory text».

Fra i paesi europei, quello che con maggiore decisione ha intrapreso la strada della responsabilizzazione, per via legislativa, dei gestori dei *social network* è stata la Germania. La *Netzwerkdurchsetzungsgesetz*, approvata a giugno 2017[92] e in vigore dal 1° ottobre, ha innanzitutto la caratteristica di rivolgersi specificamente ai *social network*: più precisamente, alle piattaforme informatiche la cui attività, svolta *a scopo di profitto*, consista nel permettere agli utenti la condivisione di contenuti di qualsiasi tipo. La legge non si applica ai *social nework* "piccoli" (con meno di due milioni di utenti) né alle piattaforme create per permettere la comunicazione individuale o la comunicazione di contenuti specifici (come i servizi di messaggistica istantanea o quelli che permettono il *download* di determinati contenuti a pagamento) né alle piattaforme che offrono contenuti di tipo giornalistico ed editoriale, la responsabilità dei quali ricade per legge sul fornitore del servizio. La legge, inoltre, non menziona esplicitamente le *fake news*, ma si riferisce genericamente a tutti i "contenuti illeciti", rimandandone la definizione a specifiche disposizioni del codice penale[93]. I gestori delle piattaforme di *social networking* sono stati gravati da obblighi di rendicontazione[94], di monitoraggio[95], di formazione[96], di predisposizione di procedure

[92] *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken* (*Netzwerkdurchsetzungsgesetz* o *NetzDG*), 30 giugno 2017, n. 536. Una traduzione in Italiano della legge, a cura di G. Giannone Codiglione, si trova in appendice al n. 1/2017 della rivista *Medialaws*. Commentano la legge Bassini e Vigevani (2017), cit., p. 19; De Gregorio (2017), cit., pp. 97 ss.; Pizzetti (2017), cit., p. 56. Si veda inoltre l'accurata analisi della *NetzDG* svolta dall'associazione *Article 19* (www.article19.org) e pubblicata ad agosto 2017 (https://www.article19.org/wp-content/uploads/2017/12/170901-Legal-Analysis-German-NetzDG-Act.pdf), nella quale si esprime molta preoccupazione per il pregiudizio che la *NetzDG* provoca alla libertà di espressione.

[93] Fra le condotte indicate figurano: la diffusione della propaganda di organizzazioni anticostituzionali e l'uso di simboli di tali organizzazioni; la preparazione di azioni sovversive; l'incitamento alla commissione di reati contro lo Stato; l'istigazione pubblica a commettere atti criminali, l'apologia di reato e la creazione di organizzazioni criminali e terroristiche; la falsificazione (nel cui ambito possono essere comprese le *fake news*) nonché la falsificazione di elementi probatori; il disturbo della quiete pubblica; l'incitamento all'odio, l'ingiuria e la diffamazione; la diffusione di immagini violente; il vilipendio di confessioni religiose e di associazioni religiose o ideologiche; la distribuzione, l'acquisizione e il possesso di materiale pedopornografico.

[94] Devono infatti redigere e pubblicare sulla propria *home page*, nonché sulla Gazzetta federale, un rapporto annuale riguardante il numero e il tipo delle segnalazioni ricevute ri-

rapide, efficaci e facilmente accessibili per accogliere le segnalazioni degli utenti, vagliarle e rimuovere o bloccare i contenuti illeciti[97]; di individuazione di una specifica persona abilitata a ricevere notifiche e richieste da parte delle autorità nazionali giudiziarie e amministrative. La procedura di *notice-and-take-down* si svolge sotto la supervisione di un'autorità amministrativa definita "indipendente" (l'Ufficio federale di giustizia), nonché in contraddittorio con l'utente, che può ricorrere contro la decisione del *provider* ad un organismo di autoregolamentazione, anch'esso indipendente e accreditato dalla suddetta autorità. Tuttavia, non può non rilevarsi che l'affidamento della supervisione e della gestione del contraddittorio ad un'autorità amministrativa, anziché giurisdizionale, non offre sufficienti garanzie rispetto al fatto che la procedura rimanga scevra da condizionamenti di natura politica.

L'aspetto che più desta perplessità, oltre all'inopportunità della scelta di affidare a soggetti privati funzioni che avrebbero invece rilevanza pubblica, è quello sanzionatorio: in caso di inottemperanza dolosa o colposa agli obblighi suindicati si applicano infatti sanzioni amministrative pecuniarie da cinquecentomila a cinque milioni di euro, in base alla gravità della condotta. L'entità delle sanzioni, congiuntamente ai limiti di tempo assai ristretti entro i quali i *provider* devono vagliare le segnalazioni di contenuti illeciti, potrebbero portare alla tendenza alla rimozione di contenuti in base anche al mero sospetto di illiceità, onde evitare le sanzioni, tanto più che la legge non riconduce alcuna conseguenza alla rimozione arbitraria di contenuti non illeciti né prevede la possibilità che gli utenti della piattaforma ricorrano al giudice avverso la decisione del *provider* di rimuovere taluni contenuti. Un altro aspetto non chiaro è quello della dichiarata applicabilità delle sanzioni anche in caso di fatti compiuti al di fuori della Repubblica federale tedesca: l'intento della disposizione è probabilmente quello di indurre al rispetto della legge anche i gestori di piattaforme di *social networking* aventi sede legale al di fuori della Germania, ma il riferimento territoriale

guardanti la presenza di contenuti illeciti, nel caso in cui tali segnalazioni siano più di cento in un anno solare.

[95] La gestione delle segnalazioni deve essere monitorata dal gestore del *social network* con controlli mensili. Ogni carenza organizzativa nella gestione delle segnalazioni ricevute deve essere immediatamente corretta.

[96] Il gestore del *social network* deve garantire ai soggetti preposti alla gestione delle segnalazioni corsi di formazione e programmi di supporto in lingua tedesca con cadenza semestrale.

[97] La rimozione deve avvenire entro un giorno nel caso di contenuti *manifestamente* illeciti, altrimenti entro una settimana. Certamente, la distinzione fra contenuti "manifestamente illeciti" e quelli semplicemente "illeciti" è piuttosto sfuggente ed evidentemente lasciata alla libera valutazione del gestore della piattaforma.

applicato alla dimensione di Internet è senz'altro incongruo, senza contare che non si vede come un'autorità amministrativa – non giudiziaria – nazionale possa intervenire nei confronti di un soggetto giuridicamente estraneo allo Stato. Sarebbe forse stata più idonea la previsione dell'applicabilità delle sanzioni nei casi in cui il contenuto illecito fosse caricato o condiviso da utenti della piattaforma residenti nella Repubblica federale tedesca.

A prescindere dagli interventi *ope legis* approvati o semplicemente proposti[98] per tentare di arginare il dilagante fenomeno delle *fake news*, ultimamente sono stati gli stessi gestori dei *social network – Facebook* per primo, ma anche *Google* – a scendere in campo, implementando meccanismi di autoregolamentazione che prevedono il controllo delle notizie che gli utenti segnalano come false da parte di *fact-checkers* professionisti esterni[99]. Questi sistemi, però, finora non sembrano aver funzionato bene[100], senza contare le perplessità che qualcuno ha sollevato circa la possibilità che i *fact-checkers* possano agire in base a logiche politicamente orientate o alle pressioni del mercato. Attraverso tali sistemi, al di là della loro reale efficacia, le maggiori *web companies* difendono e consolidano la loro reputazione, oltre a rafforzare la propri posizione dominante rispetto agli operatori minori, che non sarebbero in grado di offrire prestazioni analoghe[101]. Ma, operando in questo modo, è evidente che viene meno la asserita posi-

[98] All'inizio dei gennaio 2018, il Presidente francese Macron ha espresso l'intenzione di proporre una legge volta ad ostacolare la diffusione di *fake news* durante le campagne elettorali. Lo stesso ha fatto negli stessi giorni il governo spagnolo, preoccupato soprattutto che la disinformazione possa incentivare la propaganda secessionista in Catalogna.

[99] Monti (2017b), cit., pp. 87-88. Inoltre: M. Isaac (2016a), *Facebook Mounts Effort to Limit Tide of Fake News*, in *www.nytimes.com*; M. Isaac (2016b), *How Facebook's Fact-Checking Partnership Will Work*, in *www.nytimes.com*. Si segnala, in particolare, l'iniziativa di alcuni media francesi – in particolare *Le Monde* – di collaborare con *Facebook* al fine di segnalare taluni contenuti come "inattendibili" al termine di una procedura di *fact-checking*; i contenuti segnalati non vengono però cancellati o bloccati, ma rimangono liberamente condivisibili fra gli utenti, pur con un "marchio" di inattendibilità. Si veda su questo A. Delcambre (2017), *Huit médias français s'allient à Facebook contre les "fake news"*, in *www.lemonde.fr*.

[100] J. Christian (2017), *Is There Any Hope for Facebook's Fact-Checking Efforts?*, in *www.theatlantic.com*; S. Levin (2017), *Facebook promised to tackle fake news. But the evidence shows it's not working*, in *www.theguardian.com*; B. Nyhan (2017), *Why the Fact-Checking at Facebook Needs to Be Checked*, in *www.nytimes.com*; J. Schwartz (2017), *Tagging fake news on Facebook doesn't work, study says*, in *www.politico.eu*. Ultimamente *Facebook* ha annunciato un cambio di strategia nella lotta alle *fake news*: anziché contrassegnare le notizie inattendibili, proverà a mostrare accanto ad esse altri articoli provenienti da fonti informative ritenute affidabili, in modo da offrire agli utenti adeguati strumenti per vagliare la veridicità delle notizie.

[101] Cuniberti (2017), cit., p. 34.

zione di neutralità del *provider* rispetto ai contenuti *user-generated*[102], lasciando peraltro gli utenti del tutto privi di garanzie giuridiche rispetto alla decisione del *provider* di rimuovere o rendere inaccessibili taluni contenuti.

«L'approccio che pare più accettabile – sostiene Cuniberti[103] – 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». Si tratterebbe, in altre parole, di puntare sulla responsabilizzazione degli utenti del *web* anziché su quella degli intermediari digitali. Proprio in questa direzione pare essersi mosso ultimamente *Facebook*, che ha annunciato un cambio di strategia nella lotta alle *fake news*: anziché contrassegnare le notizie inattendibili, proverà a mostrare accanto ad esse altri articoli provenienti da fonti informative ritenute affidabili dagli stessi utenti, in modo da offrire ad essi adeguati strumenti per vagliare la veridicità delle notizie[104]. Altre possibili soluzioni potrebbero essere rappresentate nella collaborazione fra autorità amministrative indipendenti (come l'AgCom), le forze di polizia e i gestori delle piattaforme per individuare le notizie inattendibili e per rimuovere i *bot* che sono responsabili di gran parte della loro diffusione, oltre a una piena *disclosure* degli algoritmi utilizzati per selezionare i *newsfeed*, accompagnata da periodiche sessioni sperimentali per testarne e migliorarne il funzionamento[105].

3. Le indicazioni della Commissione europea per contrastare la diffusione di contenuti illeciti in Internet

L'approccio adottato recentemente dalla Commissione europea è in qualche modo intermedio rispetto alle due opzioni sopra indicate. Nel maggio del 2015, la Commissione europea ha adottato una comunicazione inti-

[102] Ivi pp. 34-35.

[103] Ivi, p. 35.

[104] Sulla nuova tattica di *Facebook*, appena inaugurata in via sperimentale, si rimanda alle notizie Ansa del 5 gennaio 2018 (*Facebook cambia tattica contro fake news, mostra più notizie*) e del 20 gennaio 2018 (*Facebook e fake news, utenti decideranno testate affidabili*), reperibili *online*. Si segnalano inoltre: M. Bruschi (2018), *Rivoluzione Facebook, gli utenti decideranno l'autorevolezza delle testate*, in *www.repubblica.it*; A. Hern (2018), *Why Facebook's news feed is changing and how it will affect you*, in *www.theguardian.com.*

[105] Questi rimedi sono suggeriti da F. Di Porto (2018), *Fake news, una possibile soluzione: algoritmi più trasparenti*, in *www.agendadigitale.eu*.

tolata *Strategia per il mercato unico digitale in Europa*, nella quale si evidenziava la necessità di avviare una consultazione pubblica sul ruolo delle piattaforme *online* e sull'efficacia delle misure per contrastare la diffusione di contenuti illeciti attraverso Internet[106]. La consultazione pubblica si è effettivamente svolta fra il 24 settembre 2015 e il 6 gennaio 2016. Sulla base dei risultati emersi, la Commissione europea ha pubblicato nel mese di settembre 2017 una comunicazione concernente proprio la lotta alla diffusione *online* dei contenuti illeciti attraverso una maggiore responsabilizzazione delle piattaforme[107]. Con questo atto la Commissione ha raccolto l'invito rivoltole dal Parlamento europeo nella risoluzione del 15 giugno 2017 sulle piattaforme *online* e il mercato unico digitale[108].

La comunicazione della Commissione europea evidenzia un elemento di debolezza nella direttiva europea sul commercio elettronico del 2000, e cioè il fatto che essa non preveda una definizione normativa di "contenuto illecito", lasciando che a ciò provvedano gli ordinamenti giuridici nazionali, oltre ad alcuni interventi legislativi settoriali adottati a livello di Unione europea. Di conseguenza, la nozione di responsabilità (o di irresponsabilità) degli Isp presente nella direttiva del 2000 si applica a tipologie di attività illegali molto diverse fra loro, comportanti violazioni di diritti tanto personali quanto patrimoniali. La Commissione auspica invece che il quadro giuridico possa essere meglio armonizzato a livello nazionale, in modo da ridurre anche l'onere di adeguarsi a diverse discipline che grava sugli operatori del settore, nonché razionalizzato con riguardo alla differenziazione delle misure di adottare in conseguenza dei diversi tipi di illecito.

Il tipo di approccio che la Commissione europea ritiene più funzionale è quello della cooperazione fra autorità competenti (giudiziarie e amministrative, nazionali ed europee) da un lato, e piattaforme digitali dall'altro: i gestori delle piattaforme, in ottemperanza al principio della *due diligence*, dovrebbero approntare soluzioni tecniche idonee a raccogliere efficacemente le segnalazioni riguardanti i contenuti illeciti, in modo da poter provvedere alla loro rapida rimozione; le autorità competenti dovrebbero individuare regole chiare, da indirizzare agli operatori del settore, sulla definizione dei contenuti illeciti e sulle corrette procedure da seguire per eliminarli; l'intero processo di *governance* dei contenuti dovrebbe avvenire in continua cooperazione fra tutti gli attori coinvolti. Solo in questo modo si potrà fronteggiare efficacemente il duplice rischio che, da un lato, alcuni contenuti illeciti

[106] Com(2015) 192 del 6 maggio 2015.

[107] Commissione europea, Com(2017) 555 del 28 settembre 2017, *Lotta ai contenuti illeciti online. Verso una maggiore responsabilizzazione delle piattaforme online*.

[108] Parlamento europeo, risoluzione del 15 giugno 2017 sulle piattaforme *online* e il mercato unico digitale, 2016/2276(INI).

non vengano segnalati o non vengano rimossi con prontezza e che, dall'altro, i gestori delle piattaforme, per eccesso di cautela, eccedano nel controllo preventivo o rimuovano contenuti non davvero illeciti, limitando così gravemente la libertà di espressione.

Uno dei problemi che la Commissione europea ha evidenziato è quello che le segnalazioni di contenuti illeciti siano infondate o non attendibili. Questa possibilità è alla base di ciò che può essere definito come "il dilemma dell'Isp": poiché non esiste nel diritto europeo alcuna norma che sollevi pregiudizialmente il *provider* dalla responsabilità civile nel caso di rimozione abusiva di contenuti non illeciti[109], e poiché non necessariamente gli intermediari digitali posseggono le competenze adeguate a discernere i contenuti illeciti da quelli che non lo sono, l'Isp è chiamato di volta in volta a valutare discrezionalmente se rischiare di incorrere in responsabilità civile per mancata rimozione di contenuti illeciti o per rimozione abusiva di contenuti leciti. Per ovviare a questo inconveniente e offrire agli intermediari digitali una guida più certa, la Commissione europea suggerisce di valorizzare il ruolo dei cosiddetti "segnalatori attendibili", cioè «entità specializzate dotate di competenza specifica nell'identificazione di contenuti illegali e di strutture dedicate per l'individuazione e l'identificazione di tali contenuti *online*», che lavorano in base a parametri qualitativi elevati. Come esempio di segnalatori attendibili la Commissione europea ha indicato l'unità di *Europol* specializzata per le segnalazioni di contenuti terroristici su Internet oppure la rete di linee dirette per la segnalazione di pornografia minorile (Inhope), ma ha anche indicato la necessità di elaborare indicatori più precisi, per quanto dotati di un certo grado di flessibilità, per qualificare talune entità come segnalatori attendibili.

Per quanto riguarda, invece, le segnalazioni provenienti dagli utenti comuni, a parte la necessità di approntare delle interfacce chiare e comprensi-

[109] Tale garanzia, invece, esiste nel diritto americano e rende più agevole e spedita la procedura di *notice-and-take-down*. Essa è prevista dall'art. 230(c)(2) del *Communication Decency Act* in favore dei *publisher* di contenuti prodotti da altri, che non possono essere ritenuti responsabili per aver scelto di rimuovere o di restringere l'accesso a contenuti osceni, volgari, lascivi, violenti, sessualmente molesti o inappropriati sotto altri aspetti. Analogamente, nel campo della protezione dei diritti di proprietà intellettuale e industriale, il *Digital Millennium Copyright Act* del 1998 – artt. 512(c)(1)(C), 512(d)(3) e 512(g)(1) – solleva da ogni responsabilità il *service provider* che, una volta ricevuta una segnalazione di contenuti illeciti da parte del titolare dei diritti che si presumono violati o di qualcuno autorizzato ad agire in sua vece, provveda immediatamente a rimuovere il materiale o a renderlo inaccessibile, anche qualora venga successivamente dimostrata la non illiceità di tali contenuti. L'intera disposizione può essere letta qui: https://www.law.cornell.edu/uscode/text/17/512 . Sull'irresponsabilità del *provider* nel diritto americano si veda R. Bocchini (2017), *La responsabilità di Facebook per la mancata rimozione di contenuti illeciti*, in *Giurisprudenza italiana*, n. 3, partic. pp. 633-635.

bili che facilitino la cooperazione da parte degli utenti, il principale problema è costituito dal bilanciamento fra la garanzia dell'anonimato di chi effettua la segnalazione e l'attendibilità della stessa. La Commissione europea ritiene che l'identificazione dell'utente che effettua la segnalazione debba avvenire solo su base volontaria; tuttavia, per evitare di dare credito eccessivo a segnalazioni anonime che potrebbero essere inoltrate con eccessiva leggerezza, risultando poi infondate, una possibilità potrebbe essere quella di favorire il contatto fra utenti anonimi e segnalatori attendibili, in modo che le segnalazioni anonime possano essere preventivamente vagliate da questi ultimi.

In linea di principio, la Commissione europea vedrebbe di buon occhio l'adozione di misure proattive da parte degli operatori del settore per individuare e rimuovere i contenuti illegali, che dovrebbero essere rese note agli utenti al momento della sottoscrizione delle clausole d'uso del servizio. Il problema è che finora gli intermediari digitali hanno mostrato qualche resistenza verso l'applicazione di tali misure proattive – consistenti, per esempio, nell'individuazione di taluni contenuti mediante tecniche di filtraggio automatico – per il timore che ciò possa mettere i *provider* in condizione di acquisire conoscenza del contenuto illecito, perdendo così il beneficio della limitazione della responsabilità a favore degli Isp "neutrali" prevista dalla direttiva *e-commerce*. A tale proposito, la Commissione ha sottolineato che l'esenzione dalla responsabilità sarebbe comunque mantenuta per gli intermediari digitali che, essendo venuti a conoscenza della presenza *online* di contenuti illeciti, si attivino prontamente per la loro rimozione.

Nello specifico, gli strumenti di filtraggio automatico per individuare i contenuti potenzialmente illegali, pur rappresentando un valido ausilio, dovrebbero essere integrati dal controllo sui contenuti da parte di esperti umani e, comunque, dovrebbero essere utilizzati entro i limiti fissati delle norme applicabili del diritto dell'Ue e nazionale, in particolare in materia di tutela della vita privata e dei dati personali, e dal divieto nei confronti degli Stati membri di imporre obblighi generali di sorveglianza ai *provider*. Dovrebbero inoltre essere disponibili solide garanzie per limitare il rischio di rimuovere contenuti leciti, sostenute da una serie di obblighi significativi di trasparenza volti ad aumentare la responsabilità dei processi di rimozione.

In considerazione del fatto che i diversi tipi di contenuti richiedono una diversa quantità di informazioni contestuali al fine di determinarne la liceità o l'illiceità, non sempre è possibile effettuare la loro cancellazione o sospensione con tecniche completamente automatizzate. Ciò può essere possibile nei casi in cui le circostanze lasciano pochi dubbi sull'illiceità del materiale, ma spesso occorre procedere a una valutazione più accurata, che

può determinare un rallentamento nelle procedure e nei tempi di rimozione. Il problema, dunque, consiste proprio nell'individuare dei criteri idonei a bilanciare la rapidità della risposta del *provider* in termini rimozione dei contenuti illeciti – affinché la permanenza *online* del contenuto non ne aggravi le conseguenze dannose – con l'accuratezza delle procedure di accertamento.

La trasparenza è uno dei concetti-chiave richiamato nella comunicazione della Commissione. Affinché il sistema funzioni, le piattaforme *online* dovrebbero indicare, nelle condizioni del servizio che gli utenti sono chiamati a sottoscrivere, in modo chiaro, facilmente comprensibile e sufficientemente dettagliato, la propria *policy* sul trattamento sia dei contenuti illegali sia di quelli che non rispettano le condizioni del servizio previste dalla piattaforma. Gli utenti dovrebbero ricevere chiare e precise informazioni sulle restrizione alla diffusione di determinati contenuti e sulle procedure da seguire per opporsi alle decisioni di rimozione, anche nel caso in cui queste ultime siano state attivate da segnalatori attendibili. Infatti, è importante che i *provider* garantiscano il ripristino dei contenuti rimossi erroneamente e quindi, a tal fine, occorre predisporre procedure idonee a far sì che gli utenti possano contestare una decisione di rimozione dei contenuti. Occorre anche approntare un sistema che consenta al gestore della piattaforma di replicare alle segnalazioni effettuate in malafede o infondate, in modo da scoraggiare l'abuso di tali pratiche. Infine, occorre fare in modo che, una volta rimossi, i contenuti illeciti non ricompaiano *online*, obiettivo che può essere raggiunto attraverso il miglioramento della cooperazione fra i diversi prestatori di servizi, l'adozione di misure sanzionatorie per i trasgressori recidivi, e l'utilizzo di filtri automatici.

Ciò che non emerge chiaramente da questa comunicazione è se, nella visione della Commissione europea, i suggerimenti debbano essere implementati solo attraverso pratiche di volontaria cooperazione e di autoregolamentazione oppure anche un intervento normativo volto a integrare o a modificare la direttiva sul commercio elettronico, ormai molto datata. Dal tenore della comunicazione, sembra che la Commissione propenda per la prima soluzione: infatti, non vi è alcun accenno esplicito alla revisione della direttiva 2000/31/Ce e, anzi, è ribadito che la direttiva costituisce «la base adeguata per elaborare sistemi rapidi e affidabili, idonei a rimuovere le informazioni illecite e a disabilitare l'accesso alle medesime»; inoltre, la comunicazione contiene un preciso riferimento alla «necessità che le piattaforme *online* agiscano in modo più responsabile e intensifichino l'impegno di autoregolamentazione a livello dell'Ue per rimuovere i contenuti illegali».

Il rischio insito nell'approccio normativo è che le misure legislative proposte possano essere tacciate di ledere il diritto alla libera manifestazio-

ne del pensiero, protetto non solo dalla Cedu ma anche dalla *Carta dei diritti fondamentali dell'Unione europea*. Per non dire delle difficoltà insite nell'armonizzare le diverse "sensibilità" degli ordinamenti giuridici nazionali rispetto a queste tematiche, superando anche le resistenze di quegli Stati che riterrebbero un intervento legislativo dell'Unione esorbitante rispetto ai imiti dettati dal rispetto dei principi di sussidiarietà e proporzionalità. L'approccio basato sulla *self-regulation*, però, pur avendo il pregio di adattarsi con sufficiente flessibilità ai rapidi mutamenti del contesto conseguenti all'evoluzione delle tecnologie, rischia di risultare inefficace dinanzi alla pressione derivante dagli interessi economici degli operatori del settore, tendenzialmente preponderanti su quelli degli utenti. Insomma, solo la periodica valutazione dei risultati eventualmente ottenuti dalle pratiche di autoregolamentazione potrà confermarne la reale efficacia, o piuttosto declassarle ad operazioni essenzialmente "cosmetiche" a ridotto impatto. Nell'attesa, la rapidissima evoluzione tecnologica rischia di aggravare ulteriormente l'obsolescenza di norme che già adesso appaiono inadeguate, indebolendo e rendendo ancor più disomogenea la protezione dei diritti individuali.

La Commissione europea, comunque, sembra decisa a proseguire la sua strada per contrastare la diffusione delle *fake news*. A tal fine, nel gennaio 2018, al termine di una procedura di selezione ad evidenza pubblica, è stato nominato un gruppo di alto livello composto da trentanove esperti, con funzioni consultive nei confronti della Commissione europea sulle questioni legate alle *fake news* e alla disinformazione *online*[110]. La riunione inaugurale del gruppo si è svolta il 15 gennaio 2018. Inoltre, il 13 novembre 2017 è stata lanciata una consultazione pubblica su questi temi, che si concluderà il 23 febbraio 2018[111].

[110] https://ec.europa.eu/digital-single-market/en/news/experts-appointed-high-level-group-fake-news-and-*online*-disinformation.

[111] https://ec.europa.eu/info/consultations/public-consultation-fake-news-and-*online*-disinformation_en.

CONCLUSIONI

Cosa può concludersi da quanto scritto fin qui? Sebbene il termine "conclusioni" suggerisca il raggiungimento di alcuni punti fermi ben argomentati e dimostrati, in realtà la prima e più evidente conclusione cui si perviene al termine di questo viaggio nel labirinto normativo e giurisprudenziale in cui si dipanano i *social network* , e particolarmente le responsabilità ricadenti sui gestori delle piattaforme, è l'impossibilità di addivenire a conclusioni univoche. Si sono piuttosto raggiunte conclusioni interlocutorie, da esprimere in forma dubitativa. Ciò a causa della difficoltà di ridurre alle categorie già previste nel diritto positivo un fenomeno relativamente nuovo e soprattutto in rapidissima espansione e continuo mutamento.

La consistenza del fenomeno – più della metà della popolazione italiana e quasi il quaranta per cento di quella mondiale utilizzano oggi i *social network* – impone di attribuire ad esso una rilevanza giuridica che vada al di là della tradizionale categoria di mezzo attraverso cui l'individuo si esprime. Se, infatti, si guarda ai *social network* solo come strumenti di esercizio di una libertà individuale non si coglie appieno, e si rischia di considerare giuridicamente irrilevante, la loro straordinaria capacità di ridisegnare il sistema delle relazioni umane. Questo aspetto è stato ben messo in luce nell'ambito degli studi sociologici: non a caso, l'espressione *network society* utilizzata da Castells e da altri mette in evidenza l'impatto sociale dei *social network*, più che quello sulla libertà di manifestazione del pensiero. Peraltro, il fine preminente dei *social network* – come sottolineato da abbondante letteratura – non è tanto quello di diffondere informazioni, quanto quello di creare interazioni fra individui in modo "disincarnato", cioè svincolato dalla fisicità. Si tratta però di legami deboli, mutevoli, fluidi; per dirla con Bauman, liquidi.

Si tratta inoltre di legami che privilegiano l'individualità anziché l'alterità: paradossalmente, in un reticolo di relazioni sociali assai più esteso e articolato rispetto al passato, la centralità del singolo individuo non tende affatto a svanire, ma viene anzi potenziata (*networked individualism*).

Se il singolo individuo, infatti, utilizza il *social network* per potenziare la proiezione esterna della propria personalità, producendo e diffondendo contenuti di vario tipo, lo stesso singolo individuo diviene anche bersaglio di strategie di *marketing* personalizzato che sfruttano le informazioni ricavate dalla profilazione degli utenti delle piattaforme, realizzate attraverso appositi algoritmi.

A tal fine, le *web companies* non tralasciano alcun mezzo, ivi compresi il controllo e la personalizzazione delle informazioni che raggiungono il singolo utente, proprio al fine di condizionarne le scelte; non solo scelte di consumo, ma anche scelte valoriali. Ciò ha trasformato Internet da uno spazio sconfinato di libera informazione a uno spazio controllato da pochi grandi operatori, che controllano e filtrano l'accesso alle informazioni e la loro diffusione attraverso l'utilizzo di algoritmi. Per questo, chiedersi quale sia il ruolo rivestito, in questo processo, dagli intermediari digitali e quali siano – o potrebbero/dovrebbero essere – le loro responsabilità acquista un significato che va al di là del problema di riuscire a garantire un'efficace protezione dei diritti individuali.

Se, dal punto di vista giuridico, i *social network* vengono considerati solo come mezzi di manifestazione del pensiero, e se quindi ci si preoccupa solo di tutelare i diritti e le libertà individuali, tutte le implicazioni cui si è accennato sopra perdono di rilevanza. Invece, provando a guardare alle comunità degli utenti dei *social network* come formazioni sociali *ex* art. 2 Cost. si valorizza la loro funzione di ambiente relazionale nel quale i singoli svolgono la propria personalità: ciò impone, allora, di prestare attenzione non soltanto alla protezione dei singoli all'interno del *social network* (rispetto agli abusi provenienti sia dagli altri utenti sia dai gestori della piattaforma), ma anche alla libertà della formazione sociale nel suo complesso (la *community*) rispetto all'ingerenza di poteri (soprattutto pubblici, ma anche privati) esterni ad essa.

Pur segnalando la presenza di qualche voce contraria, in realtà non paiono sussistere ostacoli alla configurazione delle *social network communities* alla stregua di formazioni sociali, data la consapevolezza degli utenti di farne parte e la presenza di un interesse comune (identificabile nell'interesse a condividere, che costituisce la stessa ragion d'essere della *community*) trascendente e ulteriore rispetto a quello dei singoli e a quello generale dello Stato. Rispetto a quest'ultimo, l'interesse della *community* potrebbe essere addirittura antitetico, posto che i contenuti condivisi possono essere tali da ledere i diritti individuali, che lo Stato democratico-costituzionale ha certamente interesse a proteggere, o da mettere a repentaglio la sicurezza e l'incolumità pubblica, più volte richiamate in Costituzione. Si pone allora il problema di definire il *quantum* di regolamentazione

che può essere imposta alle *social network communities* senza che venga intaccata la loro stessa *raison d'être* consistente nella libera condivisione di informazioni, nonché il *quomodo* del controllo sui comportamenti degli appartenenti alla formazione sociale (non solo gli utenti, ma anche i gestori delle piattaforme).

Più complesso è capire se i *social network* possano essere assimilati a qualcuna delle formazioni sociali di rilevanza costituzionale, come ad esempio le associazioni (art. 18 Cost.), data l'assenza nel vigente ordinamento giuridico di norme definitorie del concetto di associazione. Le *social network communities* sembrano possedere alcune caratteristiche comuni alle associazioni – la plurisoggettività, la comunanza del fine, una qualche struttura organizzativa, un *corpus* di regole interne che i membri devono rispettare – ma ben difficilmente le clausole d'uso sottoscritte dagli utenti al momento dell'iscrizione alla piattaforma possono essere parificate a un contratto associativo, sia pure a forma libera, poiché in esse non vi è alcun riferimento ad un vincolo associativo né agli scopi che la presunta associazione intenderebbe perseguire. Però l'eventuale assimilazione dei *social network* alle associazioni, rispetto alla quale la dottrina per lo più dissente, potrebbe servire ad ostacolare la formazione di gruppi di utenti delle piattaforme che si formano con l'intento di condividere contenuti illeciti: poiché, infatti, le associazioni non possono perseguire finalità vietate ai singoli dalla legge penale, per reprimere eventuali condotte illecite si potrebbe intervenire sciogliendo coattivamente il gruppo anziché perseguire i singoli responsabili degli illeciti, spesso difficili da individuare; inoltre il gestore della piattaforma, in quanto membro della presunta associazione, verrebbe considerato corresponsabile.

L'attività di *social networking*, se consistente in interazioni simultanee, potrebbe essere considerata anche una riunione ex art. 17 Cost., a patto però di considerare Internet, o più precisamente il *social network*, come un "luogo". Nel caso del *social network*, un luogo aperto al pubblico, come ha stabilito nel 2014 la Corte di Cassazione a proposito di *Facebook*, non senza sollevare commenti critici. Sebbene qualcuno, come Pace, abbia evidenziato l'elemento della fisicità come determinante per caratterizzare la riunione, in realtà non è affatto scontato che la nozione di luogo debba coincidere con quella di spazio fisico, così come non è affatto detto che solo un'interazione di tipo fisico fra persone possa pregiudicare l'ordine pubblico (anche l'ordine pubblico "materiale") o la sicurezza e l'incolumità pubbliche. Al contrario, talune interazioni fra gli utenti del *social network* volte a propagare notizie false o distorte, oppure a incitare all'odio, alla violenza o alla discriminazione, possono certamente nuocere all'ordine pubblico inteso come preservazione delle strutture dello Stato democratico-costituzionale, oltre a incentivare

comportamenti socialmente pericolosi. In sintesi, l'analogia, per quanto problematica, fra attività di *social networking* e libertà di riunione potrebbe contribuire a porre un argine alla diffusione incontrollata di contenuti idonei a recare pregiudizio all'ordine pubblico, quali i discorsi d'odio o le *fake news*.

Oltre ad inquadrare i *social network* nell'ambito del "costituzionalmente rilevante", occorre considerare la peculiare posizione del gestore della piattaforma, che la direttiva europea sul commercio elettronico n. 2000/31/Ce esonera dalla responsabilità per gli illeciti commessi dagli utenti attraverso la diffusione di contenuti *user-generated*, a condizione che il *provider* si limiti a svolgere attività di *hosting* in modo passivo e neutrale e che, una volta acquisita la conoscenza dell'illecito, provveda tempestivamente ad informarne le competenti autorità; su richiesta dell'autorità, sorge inoltre in capo al *provider* un obbligo di rimozione dei contenuti illeciti, l'inadempienza al quale comporta l'attribuzione di responsabilità civile. Ciò non significa, però, che gli intermediari digitali possano essere assoggettati ad obblighi di sorveglianza sulle informazioni trasmesse o memorizzate o di attiva ricerca di fatti o circostanze che indichino la presenza di attività illecite; diversamente, i *provider* sarebbero gravati da oneri eccessivi che recherebbero grave intralcio alle loro attività, ostacolando lo sviluppo del commercio elettronico e, più in generale, di tutti i servizi della società dell'informazione.

La Corte di Giustizia dell'Unione europea, in alcune sentenze emanate a partire dal 2010, riguardanti per lo più l'ambito della protezione dei diritti di proprietà intellettuale, ha messo in evidenza principalmente due aspetti: quello dell'irresponsabilità dei *provider*, a condizione che mantengano una posizione effettivamente neutrale rispetto ai comportamenti degli utenti, e quello dell'illegittimità di obblighi di sorveglianza preventiva o di filtraggio dei contenuti in capo ad essi. Il punto è che il ruolo dei *provider* oggi è profondamente cambiato, per via dell'evoluzione tecnologica, rispetto a quello prefigurato dalla normativa europea ed italiana dei primi anni Duemila. Gli intermediari digitali non si limitano più ad essere neutrali fornitori di servizi di interconnessione, ma intervengono sui contenuti diffusi dagli utenti, mettendo in evidenza quelli più idonei a catturare l'attenzione di determinati *target*, a fini pubblicitari e di *marketing*; inoltre, attraverso gli algoritmi di profilazione monitorano i comportamenti degli utenti delle piattaforme al fine di individuarne gusti e preferenze. La normativa vigente, dunque, risulta per molti versi inadeguata.

Un ruolo creativo è stato assunto in vari casi dalla giurisprudenza italiana di merito, attraverso il ricorso alla discussa categoria – non esplicitamente prevista dalla normativa vigente – dell'*hosting provider* "attivo", che non beneficia dell'esenzione dalla responsabilità per il fatto di avere contri-

buito attivamente e con finalità di lucro alla gestione e all'organizzazione dei contenuti presenti sulla piattaforma. In altri casi, invece, la condanna del *provider* è avvenuta solo sulla base della dimostrazione del suo essere effettivamente a conoscenza delle condotte illecite degli utenti, pur senza adoperarsi per reprimerle. All'obiezione per cui l'effettiva conoscenza dell'illecito da parte del *provider* possa realizzarsi solo in seguito a comunicazione da parte dell'autorità giudiziaria o amministrativa e non alla mera diffida di parte, il giudice che si è occupato del caso di Tiziana Cantone ha obiettato che l'obbligo di procedere tempestivamente alla rimozione dei contenuti illeciti sussiste nel caso di conoscenza acquisita in qualsiasi modo, soprattutto nel caso in cui sia in gioco una lesione dei diritti della personalità non suscettibile di reintegrazione patrimoniale.

Dalla giurisprudenza esaminata emerge certamente l'esigenza di una revisione dell'attuale disciplina, a partire dalla direttiva europea sul commercio elettronico, in modo da renderla più aderente al ruolo effettivamente rivestito dai gestori delle piattaforme. Occorrerebbe però vincere le pressioni esercitate dalle grandi *web companies*, il cui interesse è quello di muoversi nel mercato digitale sfuggendo il più possibile alle connesse responsabilità. A tal fine, esse tendono a mostrare ampia disponibilità all'implementazione di sistemi di autoregolamentazione, visti come alternativa meno onerosa all'attribuzione di responsabilità *ex lege*. Il paradosso, però, è che più i gestori delle piattaforme si mostrano collaborativi e proattivi nella ricerca ed eliminazione dei contenuti illeciti, più appare incongrua la rivendicazione della loro presunta neutralità rispetto alle condotte degli utenti, su cui si fonda il regime di irresponsabilità previsto dalla normativa europea e nazionale vigente.

Chiunque utilizzi la rete Internet, e a maggior ragione chiunque partecipi a un *social network*, lascia delle "tracce digitali" che possono essere trattate al fine di ricostruire importanti aspetti della personalità individuale. Tramite l'immenso potere di aggregazione degli algoritmi digitali, piccoli frammenti che singolarmente sarebbero insignificanti vengono riuniti in modo da acquistare senso. Si può parlare allora di *habeas data* come diritto a poter mantenere il controllo su tali frammenti, a consentire consapevolmente che altri ne facciano un uso conforme alla nostra volontà, ad opporci ai trattamenti indesiderati, a poter cancellare le tracce digitali che riteniamo non ci rappresentino più correttamente o che semplicemente desideriamo mantenere nascoste a tutti o ad alcuni, ad avere la garanzia che dalla riaggregazione dei frammenti non emerga una rappresentazione falsa o distorta della nostra identità o della nostra personalità.

I gestori delle piattaforme di *social networking* si trovano a trattare una enorme quantità di informazioni personali, spesso senza che l'utente ne sia

pienamente consapevole, per non aver predisposto correttamente le impostazioni della *privacy* del proprio profilo o per non aver prestato sufficiente attenzione alle clausole d'uso del servizio, che in linea generale sottolineano come solo l'utente sia responsabile delle informazioni personali che sceglie di condividere. Però dal 25 maggio 2018 – data in cui il nuovo regolamento Ue sul trattamento dei dati personali (n. 2016/679) diventa applicabile – non sarà più possibile per i *provider* smarcarsi dalla scomoda posizione di responsabili del trattamento dei dati per il fatto che l'utente ha sottoscritto talune clausole di tale tenore; infatti, anche qualora si dubitasse della qualificazione del *social network provider* come "titolare" del trattamento dei dati (in quanto in realtà è l'utente, e non il gestore della piattaforma, a determinare finalità e mezzi del trattamento), si potrà comunque applicare ad esso la qualifica di "responsabile" (in quanto tratta i dati personali in base al consenso prestato dagli utenti e alle modalità e finalità da essi definite). Ammesso che, in linea con quanto dichiarato dagli stessi *social network provider* nelle clausole contrattuali, il responsabile del trattamento dei propri dati sia l'utente, essi non possono sfuggire a tale qualifica almeno per quanto riguarda l'attività di profilazione degli utenti con finalità di *marketing* diretto, poiché in questo caso sono proprio i gestori delle piattaforme a determinare le finalità (il *behavioural advertising*) e i mezzi (gli algoritmi di profilazione) del trattamento. Per giunta, poiché il trattamento dei dati degli utenti avviene a fini di profitto, non si può escludere in via teorica l'applicabilità ai *provider* del reato di cui all'art. 167 del Codice della *privacy* (trattamento illecito dei dati), di cui il profitto per sé o per altri è elemento costitutivo.

Anche la cosiddetta "esenzione domestica", applicabile alle sole persone fisiche utenti dei servizi (quindi anche agli utenti dei *social network*) a condizione che trattamento dei dati non avvenga nell'ambito di attività professionali o commerciali, non potrà più essere applicata agli intermediari digitali, per il fatto che l'attività del *provider* è sempre di tipo professionale: verrà così sgombrato il campo dall'ambiguità che caratterizza la disciplina attualmente vigente, che obbliga ad una verifica caso per caso dell'effettivo ruolo svolto dai *provider* nel trattamento dei dati degli utenti. Inoltre, il nuovo regolamento sostituisce al principio dell'*opt-out* quello dell'*opt-in*, per cui i gestori dei *social network* non potranno più declinare la responsabilità per il trattamento dei dati personali degli utenti, a meno che gli utenti esplicitamente lo accettino. Analogamente, gli utenti dovranno esplicitamente consentire ad essere profilati tramite algoritmi, dopo essere stati debitamente informati delle caratteristiche, modalità e finalità della profilazione.

Il nuovo regolamento, in sintesi, alza il livello di tutela di cui l'utente gode nei confronti del fornitore del servizio, correggendo alcune delle più evidenti storture dell'attuale disciplina. Ciò corrisponde ad un aumento delle responsabilità dei *social network provider* che presuppone proprio il loro ruolo attivo – non più dunque solo passivo e neutrale – nel trattamento dei dati personali. Questo elemento risulta in contrasto con quanto previsto dalla direttiva sul commercio elettronico risalente al 2000, il cui presupposto è invece la neutralità dell'intermediario.

Se qualche anno fa l'assoluzione dei manager di *Google* (caso *Google-ViviDown*) dal reato di trattamento illecito dei dati personali si è fondata sulla posizione neutrale del fornitore del servizio, che non era a conoscenza del contenuto del video e si era comunque adoperato immediatamente per la sua rimozione in seguito alla richiesta dell'interessato, oggi probabilmente questi principi non sarebbero più applicabili ai *social network provider* che svolgono attività di organizzazione, aggregazione e indicizzazione dei contenuti, nonché di profilazione degli utenti a fini commerciali. Questo è il motivo per cui i gestori dei principali *social network* si stanno via via dotando di sistemi sempre più sofisticati che consentono agli utenti di segnalare contenuti potenzialmente illeciti e al *provider*, previa verifica dell'attendibilità della segnalazione, di rimuovere il contenuto. Queste dinamiche possono prestarsi ad essere interpretate come un'implicita assunzione di responsabilità da parte dei gestori delle piattaforme, in vista della prossima entrata in vigore del nuovo regolamento europeo sul trattamento dei dati personali.

Una questione connessa al trattamento dei dati personali è quella del cosiddetto "diritto all'oblio", che si va trasformando da "diritto ad essere dimenticati", decaduto l'interesse pubblico di conoscenza per via del decorso temporale, a "diritto ad essere correttamente rappresentati" attraverso l'accostamento di informazioni più aggiornate a quelle passate oppure, secondo quanto emerso dalla sentenza *Google Spain*, a "diritto alla deindicizzazione" una volta venuta meno l'attualità della notizia. Il nodo critico risiede nell'oggettiva difficoltà di stabilire fino a quando ricorrono le condizioni della permanenza *online* di informazioni riferite al passato, ovvero fino a quando e in base a quali presupposti queste ultime risultano avere ancora un apprezzabile interesse pubblico per la collettività, per non parlare della dubbia idoneità di un soggetto privato – nella fattispecie, il motore di ricerca – a effettuare una valutazione equilibrata del rapporto fra tutela della *privacy* e interesse pubblico all'informazione, in difetto dei necessari requisiti di imparzialità e obiettività. Può apparire inoltre criticabile la scelta di aver onerato il motore di ricerca del compito di valutare le richieste di

deindicizzazione senza che alcuna attività di rimozione dei contenuti venga richiesta, invece, al titolare del "sito sorgente".

Si evidenza anche una discrasia fra quanto deciso in *Google Spain* e in *Google-ViviDown*: se si considera che, nel caso *Google Spain*, i dati personali di cui si chiede la rimozione si presumono contenuti in siti *web* equiparabili a testate giornalistiche, mentre nel caso *Google-ViviDown* si trattava di contenuti *user-generated*, si potrebbe giungere alla paradossale conclusione che un *provider* (nella fattispecie, un motore di ricerca) debba essere considerato "titolare" del trattamento dei dati personali quando questi dati provengono da soggetti comunque tenuti, a loro volta, al rispetto della normativa sulla *privacy*, mentre il medesimo *provider* non possa essere considerato titolare del trattamento quando i dati personali diffusi attraverso i servizi da esso prestati siano presenti in *user-generated content*, quindi provenienti da soggetti che potrebbero godere dell'esenzione domestica.

Chiare evidenze mostrano che oggi la commistione fra l'attività svolta dai *social network* e quella tipica degli editori di informazione giornalistica è sempre più marcata. I gestori delle piattaforme di *social networking* svolgono un'attività tipicamente editoriale nel momento in cui mettono in luce le notizie più interessanti per ciascun utente, opportunamente corredate da pubblicità mirata; quindi il gestore della piattaforma *social*, al pari del direttore di una testata giornalistica, contribuisce a distinguere e a mettere in risalto ciò che davvero "fa notizia". D'altro canto, già da tempo gli editori tradizionali, una volta approdati *online*, hanno iniziato a corredare l'informazione giornalistica di strumenti di interazione *social*, come ad esempio la possibilità per gli utenti di segnalare gli articoli più graditi e di arricchirli con propri commenti, oppure a sviluppare sinergie con i *social media*, come avviene ad esempio nel caso degli *instant articles* di *Facebook*.

Attraverso la collaborazione con gli editori tradizionali, i *social media* stanno gradualmente sviluppando strategie per sfruttare a loro vantaggio l'affidabilità e la credibilità di cui gode la stampa, con l'effetto di occupare progressivamente lo spazio appartenuto finora all'editoria. D'altro canto gli editori tradizionali, per fronteggiare la posizione dominante detenuta dai *social media* in termini di volume di traffico e di raccolta pubblicitaria, ricercano con essi alleanze per sfruttare in modo proficuo le nuove opportunità offerte dalla digitalizzazione, nel tentativo di raggiungere un pubblico più ampio e meglio profilato, incrementando così gli introiti derivanti dalla raccolta pubblicitaria. Ci si chiede, allora, se i *social network provider* possano essere paragonati in qualche modo agli editori di stampa tradizionale non periodica e gravati, alla stregua degli editori, della responsabilità per i contenuti illeciti (per esempio diffamatori) prodotti dagli utenti.

La Corte di Strasburgo ha esaminato la questione per la prima volta in occasione del caso *Delfi*: un portale di informazione giornalistica, ritenuto responsabile di diffamazione non per il contenuto degli articoli pubblicati, ma per quello di alcuni commenti caricati autonomamente dagli utenti, giudicati non solo diffamatori, ma anche suscettibili di incitare all'odio e alla violenza. La Corte ha ritenuto che la natura "professionale" di *Delfi* implicasse la materiale possibilità – e quindi l'obbligo – di esercitare un controllo di tipo editoriale anche sui contenuti *user-generated*. Tuttavia questo principio, che *mutatis mutandis* potrebbe essere applicato anche ai *social network provider*, è stato temperato dalla constatazione che l'obbligo di rimozione dei contenuti illeciti sussiste per la particolare attitudine di tali contenuti ad incitare all'odio e alla violenza. Infatti, in un caso successivo (*Mte e Index*), la minore gravità della condotta degli utenti – che avevano postato commenti certamente lesivi della reputazione di una società commerciale, ma non tali da incitare all'odio e alla violenza – ha suggerito ai giudici la conclusione che l'attribuzione di responsabilità per diffamazione ai *provider* rappresentasse una violazione dell'art. 10 della Cedu. Questa stessa tendenza al ridimensionamento sembra confermata dalla decisione relativa al più recente caso *Pihl*, che ha ribadito che il gestore di un *blog* (nel caso di specie si trattava di una piccola associazione non-profit) non potesse essere ritenuto responsabile per la pubblicazione di un commento diffamatorio immesso da un utente rimasto anonimo, a meno che il commento non contenga espressioni che trasmodino nell'incitamento all'odio e alla violenza e purché il gestore abbia provveduto tempestivamente alla sua rimozione a seguito della segnalazione della persona offesa.

Dunque, la Corte di Strasburgo ha ammesso la possibilità che i *provider* possano essere ritenuti responsabili per i contenuti illeciti *user-generated*, ma solo in base a una valutazione caso per caso che tenga conto della natura e del ruolo svolto dall'intermediario digitale, nonché del tipo di contenuto. Va segnalata, inoltre, l'opinione dissenziente che ha accompagnato la sentenza *Delfi* e che, richiamando le considerazioni di Balkin sulla "censura collaterale", ha evidenziato che l'imposizione di responsabilità agli intermediari digitali ha sempre rappresentato e continua a rappresentare un ostacolo alla libertà di espressione.

I reati – come ad esempio la diffamazione – frequentemente commessi dagli utenti attraverso la diffusione di contenuti *user-generated* impongono di considerare anche se il gestore della piattaforma che non abbia svolto un ruolo completamente passivo e neutrale possa essere considerato penalmente responsabile a titolo di concorso nel reato. Gli appigli giurisprudenziali sono assai scarsi, ma non inesistenti. Certamente occorre procedere a una valutazione caso per caso, verificando se l'attività del gestore della piatta-

forma sia di tipo esclusivamente automatizzato oppure se, sia pure in forma semi-automatica, il *provider* sia in qualche modo intervenuto nell'*editing* dei contenuti prodotti dall'utente. Occorre anche accertare che l'apporto del *provider* sia stato necessario e indispensabile, e non meramente accessorio, per la realizzazione dell'evento delittuoso, o almeno che si sia realizzato il modello della cosiddetta "causalità agevolatrice". Un ostacolo rispetto a questa ricostruzione, però, è rappresentato dal fatto che la maggior parte dei reati commessi dagli utenti di Internet sono reati di condotta e non di evento: poiché la condotta del *provider* che mantiene *online* i contenuti illeciti o omette di cancellarli è successiva alla commissione del reato da parte dell'utente, non si può propriamente parlare di concorso nel reato stesso.

Ancora più problematica, oltre a non essere suffragata dalla giurisprudenza, è la possibilità di attribuire al *provider* la responsabilità per il reato omissivo improprio ex art. 40 c. p., poiché le norme vigenti non sembrano individuare in capo ai gestori delle piattaforme alcun obbligo giuridico di impedire danno provocato dall'utente né alcuna posizione di garanzia.

Non infrequentemente accade che i contenuti prodotti dagli utenti e messi in circolazione attraverso le varie piattaforme di *social networking* contengano incitamento all'odio, alla violenza e alla discriminazione (*hate speech*) che, secondo la giurisprudenza della Corte di Strasburgo, sono manifestazioni del pensiero incompatibili con l'art. 10 Cedu. Gli autori di tali condotte sono responsabili, anche penalmente, ai sensi della decisione-quadro europea 2008/913/Gai e, in Italia, ai sensi di varie disposizioni di legge che puniscono la discriminazione e l'odio razziale, l'istigazione alla violenza, l'apologia di genocidio, il cyberbullismo, gli atti persecutori commessi anche *online*, la diffamazione e la minaccia aggravate dall'utilizzo di mezzi di pubblicità. Tuttavia, varie voci si oppongono alla tendenza alla repressione, attraverso gli strumenti del diritto penale, delle manifestazioni del pensiero riconducibili allo *hate speech*, soprattutto per il timore che l'esclusione di alcuni voci "disturbanti" dal dibattito pubblico possa tradursi in uno strumento in mano ai gruppi dominanti per reprimere il dissenso.

Ci si chiede, inoltre, se oltre a perseguire penalmente gli autori delle espressioni di odio non sia opportuno intervenire anche sugli intermediari digitali, attribuendo ad essi oneri di controllo e filtraggio dei contenuti. A ciò si oppone il fatto che tanto la direttiva europea sul commercio elettronico quanto la conseguente giurisprudenza della Corte di Giustizia escludono che il *provider* possa essere gravato da obblighi di sorveglianza sui contenuti prodotti dagli utenti, senza contare che ogni forma di responsabilizzazione degli intermediari digitali, soprattutto nel caso in cui preveda il ricorso a tecniche di filtraggio preventivo dei contenuti, è guardata con sospetto perché potrebbe dare luogo a forme di "censura privata". L'unica via prati-

cabile, caldeggiata sia dal Consiglio d'Europa sia dall'Unione europea, sembra allora essere quella dell'autoregolamentazione. Proprio questo è il senso del Codice di condotta varato nel 2016, in base al quale alcune grandi *web companies* si sono impegnate ad approntare procedure chiare ed efficaci per esaminare le segnalazioni di contenuti incitanti all'odio da parte degli utenti dei loro servizi, in modo da poter rimuovere tali contenuti o renderli inaccessibili. Anche così, però, può apparire discutibile la scelta di affidare a soggetti privati il delicato compito di vagliare la fondatezza e l'attendibilità delle segnalazioni degli utenti circa contenuti incitanti all'odio e alla violenza e di decidere quali contenuti sia opportuno rimuovere, senza che la decisione sia assistita da una procedura in contraddittorio o da garanzie giurisdizionali.

Fra i contenuti che circolano frequentemente *online*, anche attraverso i social *network*, vi sono anche le notizie false, distorte o inattendibili, ma tali da suscitare attenzione o allarme. Le *fake news* vengono prodotte e fatte circolare talvolta dagli utenti delle piattaforme, non sempre consapevoli della loro falsità, talaltra da sistemi informatici (i *troll-bot*), utilizzati da chi ha interesse a manipolare l'opinione pubblica a fini commerciali o persino politici. Se, in alcuni casi, la circolazione di tali notizie può essere relativamente innocua, in altri casi invece è tale da recare pregiudizio all'ordine pubblico e alla sicurezza e incolumità pubbliche. Sebbene l'art. 21 della Costituzione italiana possa essere interpretato nel senso di non estendere alcuna garanzia alle manifestazioni del pensiero "subiettivamente falso", sebbene il "dovere della verità" sia imposto *ope legis* a chi esercita la professione giornalistica, e sebbene l'art. 656 del codice penale punisca la pubblicazione e la diffusione di notizie false, esagerate o tendenziose, per le quali possa essere turbato l'ordine pubblico, le norme giuridiche non sembrano in grado di arginare il fenomeno delle *fake news*, favorito dalla difficoltà di individuare i responsabili della messa in circolazione delle "bufale" e dalla dimensione transnazionale di Internet.

Anche in questo caso, la soluzione è stata individuata nella maggiore responsabilizzazione dei *provider*. In Germania è stata approvata una legge che impone ai gestori delle piattaforme di *social networking* di vagliare le segnalazioni provenienti dagli utenti circa la presenza *online* di contenuti inappropriati e, se ritenute fondate, di rimuoverli celermente, pena l'applicazione di ingenti sanzioni pecuniarie. Oltre all'inopportunità della scelta di affidare a soggetti privati funzioni che avrebbero invece rilevanza pubblica, desta perplessità la scelta di aver affidato la supervisione della procedura di *notice-and-take-down* a un organo amministrativo, anziché giurisdizionale, che non offre sufficienti garanzie rispetto al fatto che la procedura rimanga scevra da condizionamenti di natura politica. Altri paesi,

però, come la Francia e la Spagna, hanno annunciato di voler presto seguire l'esempio tedesco.

A prescindere dagli interventi *ope legis*, ultimamente sono stati gli stessi gestori dei *social network – Facebook* per primo, ma anche *Google* – a scendere in campo, implementando meccanismi di autoregolamentazione che prevedono il controllo delle notizie che gli utenti segnalano come false da parte di *fact-checkers* professionisti esterni. Questi sistemi, però, finora non sembrano aver ben funzionato, senza contare le perplessità che qualcuno ha sollevato circa la possibilità che i *fact-checkers* possano agire in base a logiche politicamente orientate o alle pressioni del mercato. Comunque, questo atteggiamento proattivo degli intermediari digitali mette ancora più in evidenza il fatto che la loro posizione di neutralità rispetto ai contenuti *user-generated*, presunta dalla ormai datata direttiva europea sul commercio elettronico, non corrisponde più assolutamente alla realtà dei fatti.

La Commissione europea suggerisce, invece, un approccio basato sulla cooperazione autorità competenti (giudiziarie e amministrative, nazionali ed europee) e piattaforme informatiche. Solo in questo modo si potrà fronteggiare efficacemente il duplice rischio che, da un lato, alcuni contenuti illeciti non vengano segnalati o non vengano rimossi con prontezza e che, dall'altro, i gestori delle piattaforme, per eccesso di cautela, eccedano nel controllo preventivo o rimuovano contenuti non davvero illeciti, limitando così gravemente la libertà di espressione. Per vincere le resistenze dei *provider*, timorosi di mostrarsi "attivi" e di perdere così il beneficio dell'irresponsabilità previsto per gli intermediari digitali neutrali dalla direttiva europea sul commercio elettronico, la Commissione europea ha precisato che l'esenzione dalla responsabilità sarebbe comunque mantenuta per quelli che, essendo venuti a conoscenza della presenza *online* di contenuti illeciti, si attivino prontamente per la loro rimozione.

Le indicazioni della Commissione europea non si spingono fino a prospettare la necessità di una revisione della direttiva 2000/31/Ce, evidentemente per via delle pressioni provenienti dalle *web companies*, che non vogliono rischiare di essere gravate da oneri che ostacolerebbero la loro libertà di iniziativa economica nel mercato digitale. Tuttavia, se non si intraprende con coraggio e decisione la via dell'innovazione legislativa, a cominciare da una revisione della direttiva europea sul commercio elettronico risalente a ben diciotto anni fa, non sarà possibile sgombrare il campo dall'ambiguità in cui attualmente versano gli intermediari digitali, che rende debole e disomogenea la protezione dei diritti individuali.

Sfatando una volta per tutte il "mito" della neutralità del *provider*, che non corrisponde più alla realtà dei fatti, si potrebbero imporre *ex lege* taluni obblighi ai gestori delle piattaforme di maggiori dimensioni, da individuare

in base al duplice criterio della finalità di lucro e del numero degli iscritti. Tali obblighi potrebbero consistere nel filtraggio automatico, tramite algoritmi, dei contenuti *user-generated* immessi *online*, finalizzato a mettere in evidenza, mediante appositi avvisi, quelli ritenuti presumibilmente inappropriati in base a criteri che il legislatore dovrebbe definire in modo da ridurre al massimo l'arbitrarietà. Dovrebbe però essere sempre consentito ai titolari dei contenuti indicati come inappropriati di opporsi a tale "stigma", ricorrendo in prima battuta allo stesso *provider* e successivamente a un'autorità amministrativa indipendente. A questa prima fase di monitoraggio potrebbe seguirne un'altra di effettiva rimozione dei contenuti segnalati dagli utenti – da molti utenti o da alcuni "segnalatori attendibili" – come falsi, distorti, incitanti all'odio, alla violenza o alla discriminazione oppure illeciti sotto altri profili. Tale procedura di *notice-and-take-down* dovrebbe però essere congegnata in modo tale da garantire il contraddittorio con i titolari dei contenuti resi inaccessibili, nonché la possibilità che la decisione del *provider* venga contestata, con ricorso dapprima all'autorità amministrativa indipendente e poi eventualmente anche al giudice.

RIFERIMENTI BIBLIOGRAFICI

G. P. Accinti (2017), *Profili di responsabilità penale dell'hosting provider "attivo"*, in *Archivio penale*, n. 2, pp. 1-21.

F. Agnino (2012), *Fino a che punto è possibile disporre contrattualmente dei propri diritti? (Vedi contratto FB)*, in *Giurisprudenza di merito*, n. 12, pp. 2555-2568.

M. R. Allegri (2018), *Alcune considerazioni sulla responsabilità degli intermediari digitali, e particolarmente dei social network provider, per i contenuti prodotti dagli utenti*, in *Informatica e diritto*, in corso di pubblicazione.

S. Alvanini (2010), *La responsabilità dei service providers*, in *Il diritto industriale*, n. 4, pp. 239-337.

C. Alves de Lima e N. Berente (2017), *Is That Social Bot Behaving Unethically?*, in *Communications of the ACM*, n. 9, pp. 29-31.

M. Augè (2015) Voce "*Nonluogo*", in *Enciclopedia italiana*, Appendice IX, Roma, Treccani.

Aristotele (1967), *La Fisica*, Napoli, Loffredo.

F. Bacco (2013), *Dalla dignità all'eguale rispetto: libertà di espressione e limiti penalistici*, in *Quaderni costituzionali*, n. 4, pp. 823-848.

J. M. Balkin (2014), *Old School/New School Speech Regulation*, in *Harward Law Review*, n. 127, pp. 2296–2342.

S. Baraldi (2016), *Editori e social media: fare informazione nell'era digitale*, in *www.markpr.it*.

A. Barbera (1975), *Art. 2*, in G. Branca (a cura di), *Commentario della Costituzione italiana*, Bologna, Zanichelli, pp. 50-122.

M. Bardi (2012), *Difendersi dalle notizie: il sistema normativo posto a tutela della sicurezza e dell'ordine pubblico minacciati dall'informazione*, in *Crimen et delictum*, n. 4, pp. 74-92.

P. Barile (1953), *Il soggetto privato nella Costituzione italiana*, Padova, Cedam.

P. Barile (1975), *Libertà di manifestazione del pensiero*, Milano, Giuffrè.

P. Barile (1984), *Diritti dell'uomo e libertà fondamentali*, Bologna, Il Mulino.

J. A. Barnes (1954), *Class and Committees in a Norwegian Island Parish*, in *Human Relations*, n. 7, pp. 39-58.

S. B. Barnes (2006), *A privacy paradox: Social networking in the United States*, in *First Monday*, n. 9, http://firstmonday.org/article/view/1394/1312.

R. Bartoli (2013), *Brevi considerazioni sulla responsabilità penale dell'Internet Service Provider*, in *Diritto penale e processo*, n. 5, pp. 600-606.

M. Bassini (2016), *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in *Quaderni costituzionali*, n. 3, pp. 587-590.

M. Bassini e G. E. Vigevani (2017), *Primi appunti su fake news e dintorni*, in *Medialaws. Rivista di diritto dei media*, n. 1, pp. 11-22.

E. Bassoli (2013), *Esclusa la responsabilità penale di Google per violazione di dati personali da parte di materiale multimediale immesso da terzi*, in *Rivista penale*, n. 5, pp. 558-563.

E. Bassoli (2014), *L'approdo finale della vicenda Google-ViviDown*, in *Rivista penale*, n. 5, pp. 501-503.

Z. Bauman (2002), *Il disagio della postmodernità*, Milano, Mondadori.

Z. Bauman (2011), *Modernità liquida*, Roma-Bari, Laterza.

Z. Bauman (2013), *Danni collaterali*, Roma-Bari, Laterza.

E. Bell (2016a), *Who owns the news consumer: social media platforms or publishers?*, in *Columbia Journalism Review*, www.cjr.org.

E. Bell (2016b), *Facebook is eating the world*, in *Columbia Journalism Review*, www.cjr.org.

M. Bellezza (2013), *Delfi vs. Estonia: la libertà della Rete è davvero in pericolo?*, in *Newsletter Inform@ Digital*, www.portolano.it.

Y. Benkler (2006), *The Wealth of Networks. How Social Production Transforms Markets and Freedom*, New Haven and London, Yale University Press.

M. Bettoni (2011), *Profili giuridici della privatizzazione della censura*, in *Ciberspazio e diritto*, n. 4, pp. 363-383.

M. Betzu (2011), *Anonimato e responsabilità in Internet*, in *Costituzionalismo.it*, n. 2, pp. 1-25.

M. Betzu (2012), *Interpretazione e sovra-interpretazione dei diritti costituzionali nel cyberspazio*, in *Rivista Aic*, n. 4, pp. 1-8.

M. Bianca (2016), *Il caso Google-ViviDown: un caso di cyberbulismo*, in M. Bianca, A. Gambino, R. Messinetti (a cura di), *Libertà di manifestazione del pensiero e diritti fondamentali*, Milano, Giuffrè, pp. 92-95.

N. Bilton (2010), *Price of Facebook Privacy? Start Clicking*, in *The New York Times*, www.nytimes.com.

E. Birritteri (2017), *Diffamazione e Facebook: la Cassazione conferma il suo indirizzo ma apre a un'estensione analogica in malam partem delle norme sulla stampa*, in *Diritto penale contemporaneo*, n. 4, pp. 286-289.

R. Bocchini (2017), *La responsabilità di Facebook per la mancata rimozione di contenuti illeciti*, in *Giurisprudenza italiana*, n. 3, pp. 632-643.

G. Boccia Artieri (2012), *Stati di connessione. Pubblici, cittadini e consumatori nella (Social) Network Society*, Milano, FrancoAngeli.

M. Bruschi (2018), *Rivoluzione Facebook, gli utenti decideranno l'autorevolezza delle testate*, in *La Repubblica*, www.repubblica.it.

F. Buffa (2017), *Responsabilità del gestore di sito Internet*, in *www.questionegiustizia.it*.

D. M. Boyd e N. B. Ellison (2008), *Social Network Sites: Definition, History,and Scholarship*, in *Journal of Computer-Mediated Communication*, n. 13, pp. 210-230.

L. Bugiolacchi (2015), *Ascesa e declino della figura del "provider attivo"? Riflessioni in tema di fondamento e limiti del regime privilegiato di responsabilità dell'hosting provider*, in *Responsabilità civile e previdenza*, n. 4, pp. 1261-1270.

L. Bugiolacchi (2016), *Quale responsabilità per il motore di ricerca in caso di mancata deindicizzazione su legittima richiesta dell'interessato?*, in *Responsabilità civile e previdenza*, n. 2, pp. 571-582.

L. Bugiolacchi (2017), *I presupposti dell'obbligo di rimozione dei contenuti da parte dell'*hosting provider *tra interpretazione giurisprudenziale e dettato normativo*, in *Responsabilità civile e previdenza*, n. 2, pp. 536-561.

G. Caggiano (2015), *L'interpretazione del criterio di collegamento del "contesto delle attività di stabilimento" dei responsabili del trattamento dei dati personali*, in G. Resta e V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE Press, pp. 43-61.

S. Calzolaio (2017a), *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in *Federalismi.it*, n. 24, pp. 1-21.

S. Calzolaio (2017b), *Protezione dei dati personali*, in *Digesto delle discipline pubblicistiche. Aggiornamento*, Torino, Utet, pp. 594-635.

R. Carbone (2017), *Responsabilità del* blogger*: parziale* revirement *della Cassazione?*, in *Cassazione penale*, n. 7-8, pp. 2782-2790.

P. Caretti e G. Tarli Barbieri (2017), *I diritti fondamentali*, Torino, Giappichelli.

C. Caruso (2013), *Dignità degli "altri" e spazi di libertà degli "intolleranti". Una rilettura dell'art. 21 Cost*., in *Quaderni costituzionali*, n. 4, pp. 795-821.

M. Castells (2007), *Communication, Power and Counter-power in the Network Society*, in *International Journal of Communication*, n. 1, pp. 238-266.

M. Castells (2009), *Comunicazione e potere*, Milano, Università Bocconi.

G. Cassano (2010), *Google v. Vividown. Responsabilità "assolute" e fine di internet*, in *Vita notarile*, n. 2, pp. 579-594.

S. A. Cerrato (2011), *I rapporti contrattuali (anche associativi) tra i soggetti del social network*, in *Aida. Annali del diritto d'autore, della cultura e dello spettacolo*, pp. 168-218.

J. Christian (2017), *Is There Any Hope for Facebook's Fact-Checking Efforts?*, in *www.theatlantic.com.*

M. Cocuccio (2015), *La responsabilità civile per fatto illecito dell'Internet Service Provider*, in *Responsabilità civile e previdenza*, n. 4, pp. 1312-1330.

D. Cohen (2016), *The Evolution of Contemporary Terrorism in Cyberspace*, in *Gnosis. Rivista italiana di intelligence*, n. 2, pp. 118-127.

C. Comella (2015), *Indici, sommari, ricerche e aspetti tecnici della "deindicizzazione"*, in G. Resta e V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE Press, pp. 177-198.

P. Costanzo (2011), *La "stampa" telematica nell'ordinamento italiano*, in *Costituzionalismo.it*, n. 2, pp. 1-14.

P. Costanzo (2017), *Quando in internet la Corte di Strasburgo continua a navigare a vista*, in *DPCE On Line*, n. 3, pp. 767-771.

M. Cuniberti (2015), *Tecnologie digitali e libertà politiche*, in *Il diritto dell'informazione e dell'informatica*, n. 2, pp. 275-312.

M. Cuniberti (2017), *Il contrasto alla disinformazione in rete tra logiche del mercato e (vecchie e nuove) velleità di controllo*, in *Medialaws. Rivista di diritto dei media*, n. 1, pp. 26-40.

C. Curreli (2017), *La diffamazione su Facebook, tra diritto sostanziale e profili probatori*, in *Responsabilità civile e previdenza*, n. 1, pp. 189-198.

M. C. D'Arienzo (2015), *I nuovi scenari della tutela della privacy nell'era della digitalizzazione alla luce delle recenti pronunce sul diritto all'oblio*, in *Federalismi.it,* n. 2, pp. 1-31.

M. De Cata (2010), *La responsabilità civile dell'internet service provider*, Milano, Giuffrè.

L. De Grazia (2013), *La libertà di stampa e il diritto all'oblio nei casi di diffusione di articoli attraverso Internet: argomenti comparativi*, in *Rivista Aic*, n. 4, pp. 1-9.

G. De Gregorio (2017a), *Il regime di responsabilità degli Isp alla luce della sentenza della Corte di Cassazione n. 54946/2016*, in *www.medialaws.eu*.

G. De Gregorio (2017b), *The market place of ideas nell'era della post-verità: quali responsabilità per gli attori pubblici e privati online?*, in *Medialaws. Rivista di diritto dei media*, n. 1, pp. 91-105.

A. Delcambre (2017), *Huit médias français s'allient à Facebook contre les "fake news"*, in *Le Monde*, www.lemonde.fr.

R. De Meo (2013), *Autodeterminazione e consenso nella profilazione dei dati personali*, in *Diritto dell'informazione e dell'informatica*, n. 3, pp. 587-608.

F. Di Ciommo (2003), *Diritti della personalità, tra media tradizionali e avvento di Internet*, in G. Comandè (a cura di), *Persona e tutele giuridiche*, Torino, Giappichelli, pp. 3-47.

F. Di Ciommo (2014), *Quello che il diritto non dice. Internet e oblio*, in *Danno e responsabilità*, n. 12, pp. 1101-1113.

S. Di Gennaro (2017), *Cosa sono i content-bot e come ci ruberanno il mestiere*, in *www.ninjamarketing.it.*

A. Di Giovine (1988), *I confini della libertà di manifestazione del pensiero*, Milano, Giuffré.

F. Di Porto (2018), *Fake news, una possibile soluzione: algoritmi più trasparenti*, in *www.agendadigitale.eu*.

E. Dinacci (2014), *Divulgazione di notizie false*, in *http://www.treccani.it/enciclopedia/divulgazione-di-notizie-false_(Diritto-on-line)/*.

L. Diotallevi (2012), *Internet e social network, tra "fisiologia" costituzionale e "patologia" applicativa*, in *Giurisprudenza di merito*, n. 12, pp. 2507-2521.

L. Diotallevi (2014), *Reato di molestia e* Facebook*, tra divieto di analogia in materia penale, (presunta) interpretazione evolutiva dell'art. 17 Cost. e configurabilità di un diritto di accesso a Internet*, in *Giurisprudenza costituzionale*, n. 5, pp. 4104-4111.

R. Ducato (2016), *I social network*, in G. Pascuzzi (a cura di), *Il diritto nell'era digitale*, Bologna, Il Mulino, pp. 269-288.

C. Esposito (1958), *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Milano, Giuffrè.

P. Falletta (2015a), *La responsabilità degli Internet service provider*, in M. Mensi e P. Falletta (a cura di), *Il diritto del web. Casi e materiali*, Padova, Cedam, pp. 141-155.

P. Falletta (2015b), *Il contrasto all'hate speech*, in M. Mensi e P. Falletta (a cura di), *Il diritto del web. Casi e materiali*, Padova, Cedam, pp. 173-196.

F. Ferrando (2017), *Ecco Heliograf, il reporter-robot del Washington Post*, in *http://tg24.sky.it/tecnologia/*.

G. Fiandaca e R. Musco (2001), *Diritto penale. Parte generale*, Bologna, Zanichelli.

G. Finocchiaro (2015), *Il diritto all'oblio nel quadro dei diritti della personalità*, in G. Resta e V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE Press, pp. 29-42.

M. Fiocca e al. (2016), *La Jihäd 2.0: profili economici, tecnologici, giuridici*, in *Ciberspazio e diritto*, n. 1-2, pp. 109-139.

G. Fioriglio (2015), *La "dittatura" dell'algoritmo: motori di ricerca web e neutralità della indicizzazione. Profili informatico-giuridici*, in *Bocconi Legal Papers*, n. 5.

R. Flor (2012), *Social networks e violazioni penali dei diritti d'autore. Quali prospettive per la responsabilità del fornitore del servizio?*, in *Rivista trimestrale di diritto penale dell'economia*, n. 3, pp. 647-694.

R. Flor (2015), *Dalla "data retention" al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di Giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive "de jure condendo"*, in G. Resta e V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE Press, pp. 223-253.

S. Fois (1957), *Principi costituzionali e libera manifestazione del pensiero,* Milano, Giuffrè.

T. E. Frosini (2014a), *Google e il diritto all'oblio preso sul serio*, in *Il diritto dell'informazione e dell'informatica*, n. 4-5, p. 563-567.

T. E. Frosini (2014b), *Internet come ordinamento giuridico*, in M. Nisticò e P. Passaglia (a cura di), *Internet e Costituzione*, Torino, Giappichelli, pp. 57-69.

A. Gaglioti (2017), *La partecipazione ad associazioni con finalità di terrorismo internazionale e la dottrina degli scambi senza accordo*, in *Sicurezza e giustizia*, n. 2, pp. 31-33.

P. Galdieri (2012), *Il trattamento illecito del dato nei social network*, in *Giurisprudenza di merito*, n. 12, pp. 2697-2713.

F. Galgano (1976), *Delle associazioni non riconosciute e dei comitati*, in A. Scialoja e G. Branca (a cura di), *Commentario del codice civile*, Bologna, Zanichelli.

F. Galgano (2010), *Trattato di diritto civile. Volume primo*, Padova, Cedam.

M. Gambini (2011), *Gli hosting providers tra doveri di diligenza professionale e assenza di un obbligo generale di sorveglianza sulle informazioni memorizzate*, in *Costituzionalismo.it*, n. 2, pp. 1-43.

A. Gardino Carli (1997), *Riunione (libertà di)*, in *Digesto delle discipline pubblicistiche*, vol. XIII, Torino, Utet, pp. 479-493.

G. Gentilini (2009), *Sulla responsabilità derivante dall'esercizio di attività pericolose. Alcune casistiche pratiche*, in *Diritto.it*, 22 gennaio 2009, pp. 1-14.

G. Giannone Codiglione (2017), *I dati personali come corrispettivo della fruizione di un servizio di comunicazione elettronica e la "consumerizzazione" della privacy*, in *Il diritto dell'informazione e dell'informatica*, n. 2, pp. 419-425.

F. Giovannella (2016), *La responsabilità civile degli Internet Service Provider*, in G. Pascuzzi (a cura di), *Il diritto nell'era digitale*, Bologna, Il Mulino, pp. 227-247.

T. Giovannetti (2014), Governance *della Rete e il ricorso alla sanzione penale: il caso della responsabilità dell'*Internet Service Provider *tra tentazioni punitive e rispetto dei principi costituzionali*, in M. Nisticò e P. Passaglia (a cura di), *Internet e Costituzione*, Torino, Giappichelli, pp. 315-335.

L. Goisis (2013), *Libertà d'espressione e odio omofobico. La Corte europea dei diritti dell'uomo equipara la discriminazione in base all'orientamento sessuale alla discriminazione razziale*, in *Rivista italiana di diritto e procedura penale*, n. 1, pp. 418-441.

D. Granara (2015), *Il fronte avanzato del diritto alla riservatezza*, in *Rivista italiana di diritto pubblico comunitario*, n. 3-4, pp. 897-915.

F. Guella e C. Piciocchi (2013), *Libera manifestazione del pensiero tra fatti di sentimento e fatti di conoscenza*, in *Quaderni costituzionali*, n. 4, pp. 849-877.

G. Guzzetta (2003), *Il diritto costituzionale di associarsi. Libertà, autonomia, promozione*, Milano, Giuffrè.

J. Habermas (1988), *Storia e critica dell'opinione pubblica*, Roma-Bari, Laterza.

P. Häberle (2000), *Diritto e verità*, Torino, Einaudi.

A. Hern (2018), *Why Facebook's news feed is changing and how it will affect you*, in *The Guardian*, www.theguardian.com.

J. Herrman (2016), *Social Media Finds New Role as News and Entertainment Curator*, in *The New York Times*, www.nytimes.com.

S. Hubbard (2017a), *Why Fake News Is An Antitrust Problem*, in *Forbes,* www.forbes.com.

S. Hubbard (2017b), *Fake News Is A Real Antitrust Problem*, in *CPI Antritrust Chronicle*, pp. 1-6.

M. Iaselli (2014), *Caso Vividown: la decisione della Cassazione nel solco della legalità*, in *Vita notarile*, n. 2, pp. 663-673.

M. Iaselli (2017a), *Come esercitare il diritto all'oblio in Internet*, Roma, Dike.

M. Iaselli (2017b), *Facebook: l'offesa in bacheca è diffamazione aggravata*, in *www.altalex.com*.

A. Ingrassia (2012), *Il ruolo dell'Isp nel ciberspazio: cittadino, controllore o tutore dell'ordine*?, in *www.penalecontemporaneo.it*.

A. Ingrassia (2013), *La Corte d'Appello assolve i manager di Google anche dall'accusa di illecito trattamento dei dati personali*, in *www.penalecontemporaneo.it*.

A. Ingrassia (2014), *La sentenza della Cassazione sul caso Google*, in *www.penalecontemporaneo.it*.

A. Ingrassia (2017), *Responsabilità penale degli* Internet service provider*: attualità e prospettive*, in *Diritto penale e processo*, n. 12, pp. 1621-1628.

N. Irti (2001), *Norma e luoghi. Problemi di geo-diritto*, Roma-Bari, Laterza.

N. Irti (2004), *Voce "Geo-diritto*", in *Enciclopedia del Novecento*, supplemento III, Roma, Treccani.

M. Isaac (2016a), *Facebook Mounts Effort to Limit Tide of Fake News*, in *The New York Times*, www.nytimes.com.

M. Isaac (2016b), *How Facebook's Fact-Checking Partnership Will Work*, in *The New York Times*, www.nytimes.com.

I. Kant e B. Constant (1996), *La verità e la menzogna*, Milano, Mondadori.

A. M. Kaplan e M. Haenlein (2010), *Users of The World, Unite! The Challenges and Opportunities of Social Media*, in *Business Horizons*, n. 53, pp. 59-68.

H. Kelsen (2000), *Teoria generale del diritto e dello Stato*, Milano, Etas.

S. Klein e C. Flinn (2017), *Social Media Compliance Programs and the War Against Terrorism*, in *Harvard National Security Journal*, n. 1, pp. 53-112.

A. Kleckova e F. Naumann (2017), *I, the Robotroll: Kremlin on Twitter*, in *http://4liberty.eu/*.

E. B. Laidlaw (2015), *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility*, Cambridge University Press.

A. G. Lana (2016), *Hate speech online: strategie di contrasto e prevenzione*, in *I diritti dell'uomo*, n. 3, pp. 499-504.

S. Landini (2017), *Identità digitale tra tutela della persona e proprietà intellettuale*, in *Rivista di diritto industriale*, n. 4-5, pp. 180-200.

K Lerman e al. (2016), *The "Majority Illusion" in Social Networks*, in *Plos One*, https://doi.org/10.1371/journal.pone.0147617, pp. 1-13.

S. Leucci (2017), *Diritto all'oblio, verità, design tecnologico: una prospettiva di ricerca*, in *MediaLaws. Rivista di diritto dei media*, n. 1, pp. 116-125.

S. Levin (2017), *Facebook promised to tackle fake news. But the evidence shows it's not working*, in *The Guardian*, www.theguardian.com.

N. Lofranco (2015), *Corte di Appello Milano (Rti/Yahoo) versus Corte di Giustizia (Papasavvas/Fileleftheros). Sulla effettiva portata delle deroghe all'ordinario regime di responsabilità del provider*, in *www.diritto.it*.

S. Logroscino (2011), *Il direttore del periodico on-line non è responsabile di omesso controllo ai sensi dell'art. 57 c. p.*, in *www.penale.it*.

V. Lubello (2011), *Commento alla sentenza della Corte di Cassazione n. 35511/2010*, in *www.medialaws.eu*.

E. Maggio (2016), *Il diritto d'autore. La responsabilità del fornitore di accesso a Internet*, in M. Bianca, A. Gambino e R. Messinetti (a cura di), *Libertà di manifestazione del pensiero e diritti fondamentali*, Milano, Giuffrè, pp. 159-167.

M. Manetti (2014), *Libertà di pensiero e anonimato in Rete*, in *Osservatorio costituzionale Aic*, n. 1, pp. 1-11.

S. Mangiameli (2006), *Il contributo dell'esperienza costituzionale italiana alla dommatica europea della tutela dei diritti fondamentali*, in *Consulta Online,* pp. 1-56.

M. Manetti (2014), *Libertà di pensiero e anonimato in Rete*, in *Osservatorio costituzionale Aic*, n. 1, pp.1-11.

A. Mantelero (2015), *Il futuro regolamento EU sui dati personali e la valenza "politica" del caso Google: ricordare e dimenticare nella* digital economy, in G. Resta e V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE Press, pp. 125-146.

G. Marchetti (2013), *Diritto di cronaca* on-line *e tutela del diritto all'oblio*, in Aa. Vv., *Da Internet ai Social Network. Il diritto di ricevere e comunicare informazioni e idee*, Rimini, Maggioli, pp. 71-90.

P. Marsocci (2011), *Lo spazio di Internet nel costituzionalismo*, in *Costituzionalismo.it*, n. 2, pp.1-22.

P. Marsocci (2015), *Cittadinanza digitale e potenziamento della partecipazione politica attraverso il web: un mito così recente già da sfatare?*, in *Rivista Aic*, n. 1, pp. 1-15.

C. Martani (2016), *Tra tutela dell'identità personale e tutela dell'account nella decisione n. 56 dell'11 febbraio 2016 del Garante per la protezione dei dati personali*, in *Ciberspazio e diritto*, n. 1-2, pp. 141-162.

C. Melzi d'Eril (2014), *La Cassazione esclude l'estensione ai siti internet delle garanzie costituzionali previste per il sequestro di stampati*, in *www.penalecontemporaneo.it*.

C. Melzi d'Eril (2016), *Contrordine compagni: le Sezioni Unite estendono le garanzie costituzionali previste per il sequestro degli stampati alle testate online registrate*, in *www.penalecontemporaneo.it*.

C. Melzi d'Eril (2017), *Fake news e responsabilità: paradigmi classici e tendenze incriminatrici*, in *Medialaws. Rivista di diritto dei media*, n. 1, pp. 60-67

C. Melzi d'Eril e S. Vimercati (2017), *Diffamazione, il gestore del sito risponde dei commenti*, in *Il Sole24Ore*, www.ilsole24ore.com.

E. Menduni (2008), *Voce "prosumer"*, in *Enciclopedia della scienza e della tecnica*, Roma, Treccani.

M. Mensi e P. Falletta (2015), *Il diritto del web. Casi e materiali*, Padova, Cedam.

M. Mezzanotte (2009), *Il diritto all'oblio*, Napoli, Esi.

G. Miceli (2017), *Profili evolutivi della responsabilità in Rete: il ruolo degli* Internet Service Provider *tra prevenzione e repressione*, in *MediaLaws. Rivista di diritto dei media*, n. 1, pp. 106-115.

M. Miglio (2016), *La responsabilità dell'amministratore di un gruppo Facebook per i commenti offensivi pubblicati da altri utenti: un travagliato percorso giurisprudenziale*, in *Giurisprudenza penale web*, n. 9.

M. Miglio (2017), *I gestori di un sito internet rispondono penalmente per i commenti offensivi pubblicati dagli utenti*, in *Giurisprudenza penale web*, n. 1.

F. Modugno (1995), *I "nuovi diritti" nella giurisprudenza costituzionale*, Torino, Giappichelli.

M. Montanari (2017), *La responsabilità delle piattaforme on-line (il caso Rosanna Cantone)*, in *Il diritto dell'informazione e dell'informatica*, n. 2, pp. 254-283.

M. Monti (2017a), *Le "bufale" online e l'inquinamento del public discourse*, in P. Passaglia e D. Poletti (a cura di), *Nodi virtuali, legami informali: Internet alla ricerca di regole*, Pisa University Press, pp. 179-192.

M. Monti (2017b), *Fake news e social network: la verità ai tempi di Facebook*, in *Medialaws. Rivista di diritto dei media*, n. 1, pp. 79-90.

M. Monti (2017c), *Regolazione, Internet e tecnica: le implicazioni di motori di ricerca e social networks sulla libertà di informazione*, in *Federalismi.it*, n. 24, pp. 1-31.

S. Moraca (2017), *Loudemy, una piattaforma italiana per combattere l'odio online*, in *Wired.it*.

D. Mula (2016), *La responsabilità del portale*, in M. Bianca, A. Gambino e R. Messinetti (a cura di), *Libertà di manifestazione del pensiero e diritti fondamentali*, Milano, Giuffrè, pp. 73-87.

N. Negroponte (1995), *Essere digitali*, Milano, Sperling & Kupfer.

K. Newman (2011), *The ultimate guide to the Facebook Edgerank algorithm*, 17 agosto 2011, https://econsultancy.com/blog/7885-the-ultimate-guide-to-the-facebook-edgerank-algorithm.

S. Niger (2008), *Il diritto all'identità personale*, in G. Finocchiaro (a cura di), *Diritto all'anonimato: anonimato, nome e identità personale*, Padova, Cedam, pp. 113-129.

R. Nigro (2015), *La responsabilità degli Internet service providers e la Convenzione europea dei diritti umani: il caso Delfi AS*, in *Diritti umani e diritto internazionale*, n. 3, pp. 681-689.

B. Nyhan (2017), *Why the Fact-Checking at Facebook Needs to Be Checked*, in *The New York Times*, www.nytimes.com.

M. Orofino (2014), *La libertà di espressione tra Costituzione e carte europee dei diritti. Il dinamismo dei diritti in una società in continua trasformazione*, Torino, Giappichelli.

A. Pace (1967), *La libertà di riunione nella costituzione italiana*, Milano, Giuffrè.

A. Pace (1977), *Art. 17-18*, in G. Branca (a cura di), *Commentario della Costituzione*, Bologna, Zanichelli, pp. 145-237.

A. Pace (1988), *Problematica delle libertà costituzionali. Lezioni. Parte speciale II*, Padova, Cedam.

A. Pace (2001), *Metodi interpretativi e costituzionalismo*, in *Quaderni costituzionali*, n. 1, pp. 35-61.

A. Pace e M. Manetti (2006), *Art. 21. La libertà di manifestazione del proprio pensiero*, in G. Branca (a cura di), *Commentario della Costituzione*, Bologna, Zanichelli.

E. C. Pallone (2015), *La profilazione degli individui connessi a Internet: privacy online e valore economico dei dati personali*, in *Ciberspazio e diritto*, n. 2, pp. 295-327.

E. C. Pallone (2016), "*Internet of Things" e l'importanza del diritto alla privacy tra opportunità e rischi*, in *Ciberspazio e diritto*, n. 1-2, pp. 163-183.

A. Papa (2009), *Espressione e diffusione del pensiero in Internet. Tutela dei diritti e progresso tecnologico*, Torino, Giappichelli.

E. Pariser (2012), *Il filtro. Quello che Internet ci nasconde*, Milano, Il Saggiatore.

G. Pascuzzi e F. Giovannella (2016), *Dal diritto alla riservatezza alla computer privacy*, in G. Pascuzzi (a cura di), *Il diritto nell'era digitale*, Bologna, Il Mulino, pp. 43-75.

F. Pasquale (2015), *The Black Box Society. The Secret Algorithms That Control Money and Information*, Cambridge (Massachusetts) and London (England), Harvard University Press.

E. Pasqualetto (2017), *Come funziona il nuovo algoritmo di Instagram: i fattori chiave*, in *https://elisapasqua-letto.it/come-funziona-il-nuovo-algoritmo-di-instagram/.*

P. Passaglia (2014), *Internet nella Costituzione italiana: considerazioni introduttive*, in M. Nisticò e P. Passaglia (a cura di), *Internet e Costituzione*, Torino, Giappichelli, pp. 1-55 (pubblicato anche in *Consulta Online*, 4 febbraio 2013).

P. Passaglia (2016), *Privacy e nuove tecnologie, un rapporto difficile. Il caso emblematico dei social media tra regole generali e ricerca di una specificità*, in *Consulta Online*, n. 3, pp. 332-348.

R. Pastena (2014), *Internet e privacy: una relazione complicata (A margine della sentenza della Corte di Giustizia del 13 maggio 2014)*, in *Osservatorio Aic*, n. 2, pp. 1-13.

E. Pelino (2008), *L'anonimato su Internet*, in G. Finocchiaro (a cura di), *Diritto all'anonimato*, Padova, Cedam, pp. 289-320.

E. Pelino, L. Bolognini e C. Bistolfi (2016), *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Giuffrè.

L. Picotti (2012), *I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali*, in *Giurisprudenza di merito*, n. 12, pp. 2522-2547.

S. Pietropaoli (2017), *La rete non dimentica. Una riflessione sul diritto all'oblio*, in *Ars intrepretandi*, n. 1, pp. 67-80.

C. Pinelli (2017), *"Postverità", verità e libertà di manifestazione del pensiero*, in *Medialaws. Rivista di diritto dei media*, n. 1, pp. 41-47.

G. Pino (2006), *Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, Giuffrè, pp. 257-321.

P. Piroddi (2015), *Profili internazional-privatistici della responsabilità del gestore di un motore di ricerca per il trattamento dei dati personali*, in G. Resta e V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE Press, pp. 63-97.

A. Pirozzoli (2004), *La libertà di riunione in Internet*, in *Il diritto dell'informazione e dell'informatica*, n. 4-5, pp. 595-627.

A. Pirozzoli (2012), *La responsabilità dell'Internet Service Provider*. *Il nuovo orientamento giurisprudenziale nell'ultimo caso Google*, in *Rivista Aic*, n. 3, pp. 1-10.

P. Pirruccio (2012), *Diritto d'autore e responsabilità del provider*, in *Giurisprudenza di merito*, n. 12, pp. 2591-2620.

F. Piselli (1995) (a cura di), *Reti. L'analisi di network nelle scienze sociali*, Roma, Donzelli.

G. Pitruzzella (2017), *La libertà di informazione nell'era di Internet*, in G. Pitruzzella, O. Pollicino e S. Quintarelli, *Parole e potere. Libertà d'espressione, hate speech e fake news*, Milano, Egea, pp. 55-98.

F. Pizzetti (2013) (a cura di), *Il caso del diritto all'oblio*, Torino, Giappichelli.

F. Pizzetti (2016), *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Torino, Giappichelli.

F. Pizzetti (2017), *Fake news e allarme sociale: responsabilità, non censura*, in *Medialaws. Rivista di diritto dei media*, n. 1, pp. 48-59.

A. R. Popoli (2014), *Social network e concreta protezione dei dati sensibili: luci ed ombre di una difficile convivenza*, in *Il diritto dell'informazione e dell'informatica*, n. 6, pp. 981-1017.

O. Pollicino (2014), *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider*, in *Percorsi costituzionali*, n. 1, pp. 45-74 (pubblicato anche in *Consulta Online*, 3 febbraio 2014).

O. Pollicino (2015), *Un* digital right to privacy *preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel* reasoning *di Google Spain*, in G. Resta e V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE Press, pp. 7-28.

O. Pollicino (2017a), *La prospettiva costituzionale sulla libertà di espressione nell'era di Internet*, in G. Pitruzzella, O. Pollicino e S. Quintarelli, *Parole e potere. Libertà d'espressione, hate speech e fake news*, Milano, Egea, pp. 1-55.

O. Pollicino (2017b), *Fake News, Internet and Metaphors (to be handled carefully)*, in *Medialaws. Rivista di diritto dei media*, n. 1, pp. 23-25.

P. Prandini (2016), *La responsabilità dei provider*, in M. Megale (a cura di), *Ict e diritto della società dell'informazione*, Torino, Giappichelli, pp. 263-285.

A. Pugiotto (2013), *Le parole sono pietre? I discorsi di odio e la libertà di espressione nel diritto costituzionale*, in *www.penalecontemporaneo.it*, pp. 1-18.

A. Puliafito (2017), *Algoritmo Facebook: il News Feed, come funziona e come cambia*, in *www.albertopuliafito.it/algoritmo-facebook/.*

S. Quintarelli (2017), *Content moderation: i rimedi tecnici*, in G. Pitruzzella, O. Pollicino e S. Quintarelli, *Parole e potere. Libertà d'espressione, hate speech e fake news*, Milano, Egea, pp. 99-146.

E. C. Raffiotta (2010), *Appunti in materia di diritto all'identità personale*, in *www.forumcostituzionale.it*.

L. Ranie e B. Wellman (2012), *Networked. Il nuovo sistema operativo sociale*, a cura di A. Marinelli e F. Comunello, Milano, Guerini.

P. Rescigno (1966), *Persona e comunità: saggi di diritto privato*, Bologna, Il Mulino.

F. Resta (2013a), *Diritti individuali e libertà della rete nel caso Vivi Down*, in *Giurisprudenza di merito*, n. 7-8, pp. 1589-1600.

F. Resta (2013b), *Libertà della rete e protezione dei dati personali: ancora sul caso Google - Vivi Down*, in *Il diritto dell'informazione e dell'informatica*, n. 3, pp. 502-514.

F. Resta (2014), *La rete e le utopie regressive (sulla conclusione del caso Google/Vividown*), in *Il diritto dell'informazione e dell'informatica*, n. 2, pp. 237-241.

G. Resta e V. Zeno-Zencovich (2015) (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, TrE-Press.

S. Ricci (2015), *Le ricadute penali della sentenza della Corte di giustizia europea sul diritto all'oblio*, in *Cassazione penale*, n. 3, pp. 1247-1254.

G. M. Riccio (2013), *Google/Vividown: "leading case" o abbaglio giurisprudenziale?*, in *Vita notarile*, n. 2, pp. 606-624.

G. M. Riccio (2015), *Diritto all'oblio e responsabilità dei motori di ricerca*, in G. Resta e V. Zeno Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, TrE-Press, pp. 199-221.

V. Riglietti (2016), *Diffamazione a mezzo stampa e diffamazione online: problematiche giuridiche*, in *Ciberspazio e diritto*, n. 3, pp. 437-467.

G. Riva (2010), *I social network*, Bologna, Il Mulino.

S. Rodotà (2014), *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, Laterza.

S. Romano (1945), *L'ordinamento giuridico*, Firenze, Sansoni.

C. Rossello (2010), *Riflessioni de jure condendo sulla responsabilità del provider*, in *Il diritto dell'informazione e dell'informatica*, n. 4-5, pp. 617-629.

E. Rossi (1989), *Le formazioni sociali nella Costituzione italiana*, Padova, Cedam.

M. Rotter (2017), *With Great Power Comes Great Responsibility: Imposing a "Duty to Take Down" Terrorist Incitement on Social Media*, in *Hofstra Law Review*, n. 4, pp. 1379-1412.

L. E. Rozo Acuña (2002), *Habeas data costituzionale: nuova garanzia giurisdizionale del diritto pubblico latinoamericano*, in *Diritto pubblico comparato ed europeo*, n. 4, pp. 1921-1945.

L. E. Rozo Acuña (2006), *Le garanzie costituzionali nel diritto pubblico dell'America Latina*, Torino, Giappichelli.

A. Ruggieri (2016), *Dignità dell'uomo, diritto alla riservatezza, strumenti di tutela (prime notazioni*), in *Consulta Online*, pp. 1-12.

S. Russo e A. Sciuto (2011), *Habeas data e informatica*, Milano, Giuffrè.

F. Sabatini e V. Coletti (2008), *Dizionario della lingua italiana*, Firenze, Sansoni.

A. Salerno (2014), *Byoid: l'identità digitale la gestisce il social network*, in *www.corrierecomunicazioni.it*.

R. Salvi (2014), *La Corte di Cassazione sul caso Google vs. Vivi Down: l'host provider non governa il mare magnum della rete*, in *www.diritto.it*.

F. Sassano (2015), *Il diritto all'oblio tra Internet e mass media*, Vicalvi (FR), Key.

S. Sassi (2013), *La libertà di associazione nel "nuovo ecosistema mediatico": spunti problematici sull'applicazione dell'art. 18 della Costituzione. Il (recente)*

caso dell'associazione xenofoba on-line, in Aa. Vv., *Da Internet ai Social Network. Il diritto di ricevere e comunicare informazioni e idee*, Rimini, Maggioli, pp. 91-123.

S. Scagliarini (2017), *In tema di privacy: virtù e vizi della cultura giuridica*, in *Ars Interpretandi*, n. 1, pp. 49-66.

L. Scaife (2017), *Social Networks as the New Frontier of Terrorism*, New York, Routledge.

S. Scalzini (2012), *I servizi di online social network tra privacy, regole di utilizzo e violazione dei diritti dei terzi*, in *Giurisprudenza di merito*, n. 12, pp. 2569-2590.

J. Schwartz (2017), *Tagging fake news on Facebook doesn't work, study says*, in *www.politico.eu*.

M. Scialdone (2013), *Il nuovo ruolo degli utenti nella generazione di contenuti creativi*, in *Diritto, mercato, tecnologia*, n. 4, pp. 8-19.

G. Scotti (2015), *Dall'habeas corpus all'habeas data: il diritto all'oblio e il diritto all'anonimato nella loro dimensione costituzionale*, in *Diritto.it*, pp. 1-28.

S. Seminara (2014), *Internet (diritto penale*), in *Enciclopedia del diritto*, Annali VII, Milano, Giuffrè, pp. 567-606.

M. Siano (2011), *La sentenza Scarlet della Corte di Giustizia: punti fermi e problemi aperti*, in F. Pizzetti (a cura di), *I diritti nella "rete" della rete. Il caso del diritto di autore*, Torino, Giappichelli, pp. 81-96.

S. Sica e G. Giannone Codiglione (2012), *Social network sites e il "labirinto" delle responsabilità*, in *Giurisprudenza di merito*, n. 12, pp. 2714-2733.

S. Sica e V. D'Antonio (2015), *La procedura di de-indicizzazione*, in G. Resta e V. Zeno Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, TrE-Press, pp. 147-176.

A. Sirotti Gaudenzi (2017), *Diritto all'oblio: responsabilità e risarcimento del danno*, Rimini, Maggioli.

M. Spatti (2014), *Hate speech e negazionismo tra restrizioni alla libertà d'espressione e abuso del diritto*, in *Studi sull'integrazione europea*, n. 9, pp. 341-358.

M. G. Stanzione (2016), *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Europa e diritto privato*, n. 4, pp. 1249-1264.

E. Stradella (2016), *Cancellazione e oblio: come la rimozione del passato, in bilico tra tutela dell'identità personale e protezione dei dati, si impone anche nella Rete, quali anticorpi si possono sviluppare e, infine,* cui prodest*?*, in *Rivista Aic*, n. 4, pp. 1-29.

C. R. Sunstein (2003), *Republic.com. Cittadini informati o consumatori di informazioni?*, Bologna, Il Mulino.

C. R. Sunstein (2010), *Voci, gossip e false dicerie*, Milano, Feltrinelli.

E. Tosi (2012), *La responsabilità civile per fatto illecito degli Internet Service Provider e dei motori di ricerca a margine dei recenti casi "Google Suggest" per errata programmazione del software di ricerca e "Yahoo! Italia" per "link" illecito in violazione dei diritti di proprietà intellettuale*, in *Rivista di diritto industriale*, n. 1, pp. 44-66.

E. Tosi (2017), *Contrasti giurisprudenziali in materia di responsabilità civile degli hosting provider – passivi e attivi – tra tipizzazione normativa e interpretazione evolutiva applicata alle nuove figure soggettive dei motori di ricerca, social network e aggregatori di contenuti*, in *Rivista di diritto industriale*, n. 1, pp. 75-122.

A. Tsesis (2017), *Terrorist Speech on Social Media*, in *Vanderbilt Law Review*, n. 2, pp. 651-708.

S. Turchetti (2010), *L'art. 57 c.p. non è applicabile al direttore del periodico online*, in *www.penalecontemporaneo.it*.

G. E. Vigevani (2014), *La responsabilità civile dei siti per gli scritti anonimi: il caso Delfi c. Estonia*, in *www.forumcostituzionale.it*, 4 febbraio 2014.

S. Vimercati (2016a), *Magyar c. Ungheria: la Corte europea ritorna sulla responsabilità dei portali web*, in *Quaderni costituzionali*, n. 2, pp. 393-400.

S. Vimercati (2016b), *La Cassazione conferma l'inestensibilità ai blog delle garanzie costituzionali previste per gli stampati in tema di sequestro*, in *www.penalecontemporaneo.it*.

S. Vimercati (2017), *La Corte di Strasburgo torna sulla responsabilità del gestore del sito: il caso Rolf Anders Daniel Pihl c. Svezia*, in *www.filodiritto.com*.

S. Wolley e al.(2017), *Il Manifesto dei Bot*, in *https://motherboard.vice.com/it/*.

S. Zamagni e P. Venturi (2017), *Da spazi a luoghi*, short paper n. 13, in *www.aiccon.it*.

F. Zani (2014), *Il difficile bilanciamento fra tutela della libertà di manifestazione del pensiero e diritto alla riservatezza nell'era dei social network*, in *Osservatorio costituzionale Aic*, n. 2, pp. 1-9.

V. Zeno-Zencovich (1993), *Voce: identità personale*, in *Digesto delle discipline privatistiche*, vol. IX, Torino, Utet, pp. 294-315.

G. Ziccardi (2015a), *L'odio e la rete: un'introduzione e alcune possibili linee di ricerca*, in *Ciberspazio e diritto*, n. 2, pp. 255-267.

G. Ziccardi (2015b), *Internet e le espressioni d'odio: influenza della tecnologia e strategie di contrasto*, in *Ciberspazio e diritto*, n. 3, pp. 387-401.

Studi di diritto pubblico
diretta da R. Bin, F. Cortese, A. Sandulli

Ultimi volumi pubblicati:

FEDERICO CAPORALE, *I servizi idrici.* Dimensione economica e rilevanza sociale (disponibile anche in e-book).

GIUSEPPINA BARCELLONA, *Votare contro.* Il referendum come opposizione e norma (disponibile anche in e-book).

TOMMASO GAZZOLO, *Essere / dover essere.* Saggio su Hans Kelsen (disponibile anche in e-book).

STEFANO ROSSI, *La salute mentale tra libertà e dignità.* Un dialogo costituzionale (disponibile anche in e-book).

RENATO IBRIDO, *L'interpretazione del diritto parlamentare.* Politica e diritto nel "processo" di risoluzione dei casi regolamentari (disponibile anche in e-book).

PIETRO FARAGUNA, *Ai confini della costituzione.* Principi supremi e identità costituzionale (disponibile anche in e-book).

PIERO PINNA, *La disposizione valida e la norma vera* (disponibile anche in e-book).

MONICA COCCONI, *Poteri pubblici e mercato dell'energia.* Fonti rinnovabili e sostenibilità ambientale.

OMAR CHESSA, *I giudici del diritto.* Problemi teorici della giustizia costituzionale (disponibile anche in e-book).

VINCENZO FERRARO, *L'amministrazione consolare.* Profili di diritto nazionale e ultrastatale (disponibile anche in e-book).

CHIARA BERGONZINI, *Parlamento e decisioni di bilancio* (disponibile anche in e-book).

ANNA LORENZETTI, *Diritti in transito.* La condizione giuridica delle persone transessuali (disponibile anche in e-book).

ANTONELLA SAU, *La proporzionalità nei sistemi amministrativi complessi.* Il caso del governo del territorio (disponibile anche in e-book).

ILENIA RUGGIU, *Il giudice antropologo.* Costituzione e tecniche di composizione dei conflitti multiculturali (disponibile anche in e-book).

MICHELE DELLA MORTE, *Rappresentanza vs. partecipazione?.* L'equilibrio costituzionale e la sua crisi (disponibile anche in e-book).

Minima giuridica

ANDREA GUAZZAROTTI, *Crisi dell'euro e conflitto sociale.* L'illusione della giustizia attraverso il mercato.

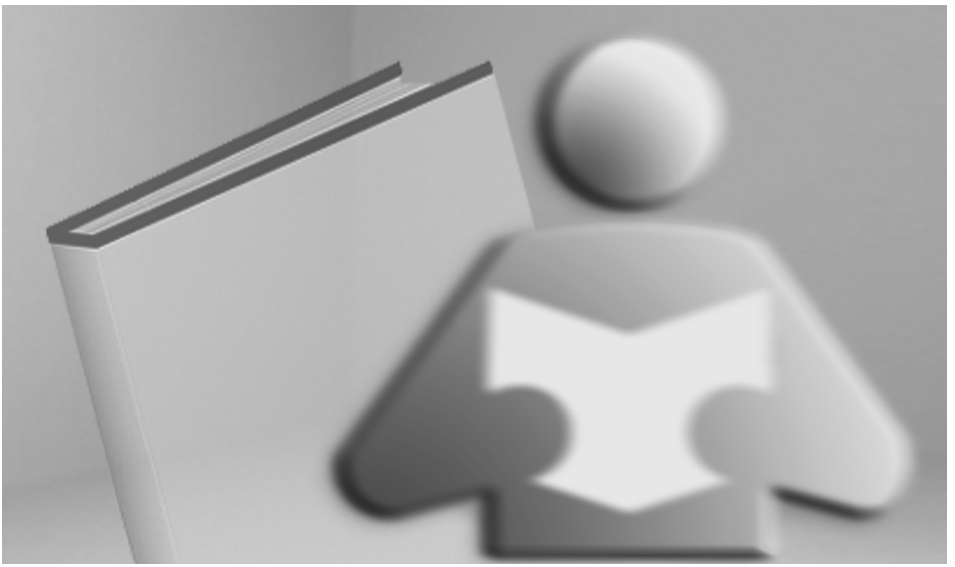
ELISABETTA LAMARQUE, *Prima i bambini.* Il principio dei best interests of the child nella prospettiva costituzionale (disponibile anche in e-book).

DANIELA BIFULCO, *Il disincanto costituzionale.* Profili teorici della laicità.

GIOVANNI DI COSIMO, *Chi comanda in Italia.* Governo e Parlamento negli ultimi vent'anni.

QUESTO LIBRO TI È PIACIUTO?

Comunicaci il tuo giudizio su:
www.francoangeli.it/latuaopinione.asp



VUOI RICEVERE GLI AGGIORNAMENTI SULLE NOSTRE NOVITÀ NELLE AREE CHE TI INTERESSANO?

Seguici in rete | Sottoscrivi i nostri feed RSS | Iscriviti alle nostre newsletter

FrancoAngeli

I *social network* costituiscono un oggetto di studio assai complesso, sia perché la loro stessa definizione assume contorni sfuggenti, sia perché i diversi attori in campo giocano ruoli che tendono a mescolarsi e a sovrapporsi, rendendo rapidamente obsolete le categorie previste nel diritto positivo. Attraverso lo studio di queste forme di comunicazione – e in particolare attraverso il loro inquadramento costituzionale e l'approfondimento del regime di responsabilità previsto per gli intermediari digitali – in questo libro si cerca di capire se e in che modo le norme giuridiche esistenti, o quelle auspicabili in prospettiva *de jure condendo*, possano offrire soluzioni valide per ovviare ai principali problemi che l'enorme diffusione dei *social network* pone con intensità sempre maggiore. Si tratta di comprendere fino a che punto i rimedi esclusivamente tecnici possano risultare efficaci e se e come possa essere composta l'inevitabile tensione fra eteronormazione e *self-regulation*. Il rischio, infatti, è che l'efficacia di nuovi interventi normativi venga vanificata dalla rapidità con cui le innovazioni tecnologiche riconfigurano fisionomia e perimetro, globali e transnazionali, dei fenomeni oggetto di regolamentazione.

Maria Romana Allegri è ricercatrice dal 2001 di Istituzioni di diritto pubblico nel Dipartimento di Comunicazione e Ricerca Sociale della Sapienza Università di Roma e da anni vi insegna, come professoressa aggregata, Diritto pubblico, dell'informazione e della comunicazione.

FrancoAngeli
La passione per le conoscenze