313
13 dicembre 2019

Istituto Bruno Leoni
idee per il libero mercato

IBL Focus

Chi ha paura della libertà di internet?

Di Vitalba Azzollini

Introduzione

Le piattaforme *online* costituiscono il principale punto di accesso a informazioni e ad altri contenuti su internet, tramite motori di ricerca, *social network*, siti di *microblogging* e molto altro. Internet non solo ha aumentato il volume e la varietà di notizie a disposizione dei cittadini, ma ha anche trasformato le modalità in cui questi ultimi si relazionano ad esse. I *social network*, in particolare, da passatempo per lo svago, la socializzazione e la condivisione di materiale tra "amici", sono divenuti un canale di informazione e, dunque, strumenti essenziali per operare valutazioni e pervenire a convincimenti personali. Inoltre, sul *web* ogni utente può diventare un attore della comunicazione, a differenza dei media tradizionali.

> Internet rompe gli schemi e consente, per la prima volta, a chiunque di dire la propria opinione, addirittura di dirla nel modo che preferisce.[1]

Questo è il motivo per cui può affermarsi che tramite la rete si attua in modo pieno e concreto la libertà di informazione prevista dall'art. 21 Cost.: sia dal punto di vista attivo (informare, divulgare notizie, esprimere commenti), sia dal punto di vista passivo (essere informati, scegliendo tra una pluralità di fonti, espressione di posizioni diverse).[2] Sotto questo profilo, va anche riconosciuto al *web* di aver consentito un maggiore partecipazione alla vita politica del Paese: la facilità con cui informazioni di vario tipo sono messe a disposizione di chiunque rende il processo democratico più partecipativo e inclusivo.

Tuttavia, questa evoluzione positiva della rete si è accompagnata a fenomeni di degenerazione del suo utilizzo, mediante la divulgazione di manifestazioni di odio mirate e di propagazione di disinformazione su vasta scala. La progressiva crescita di questi fenomeni ha portato a una sempre maggiore attenzione al ruolo degli intermediari digitali – soprattutto *social network* – come "moltiplicatori" dei

Vitalba Azzollini, giurista, lavora in un'autorità di vigilanza (esprime opinioni a titolo esclusivamente personale). È autrice di paper e articoli in materia giuridica.

1 B. Saetta, "Hate speech: l'accordo UE – social network mette a rischio la libertà d'espressione", Valigia Blu, 3 giugno 2016.

2 La libertà di manifestazione del pensiero trova altresì espresso riconoscimento nell'art. 19 della Dichiarazione universale dei diritti dell'uomo, ai sensi del quale "Ogni individuo ha diritto alla libertà di opinione e di espressione", nonché nell'art. 11 della Carta dei diritti fondamentali dell'uomo dell'Unione Europea. secondo cui "Ogni individuo ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee".

discorsi di odio (*hate speech*), che minano le basi della convivenza civile, e di notizie false (*fake news*), che influenzano dinamiche decisionali e distorcono eventi elettorali. Ciò ha determinato nel tempo iniziative politiche d'intervento anche normativo.[3] Da ultimo, è stata avanzata la proposta dell'identificazione certa per l'accesso ai *social network*, al fine di «garantire che ad un account corrisponda un nome ed un cognome di una persona reale, eventualmente rintracciabile in caso di violazioni di legge», nel presupposto che altrimenti non sia possibile individuarne l'autore.[4] Inoltre, il 29 ottobre 2019, è stata istituita presso il Senato una "Commissione straordinaria per il contrasto dei fenomeni di intolleranza, razzismo, antisemitismo, anticristianesimo e istigazione all'odio e alla violenza", data la "crescente spirale" favorita da "una capillare diffusione attraverso vari mezzi di comunicazione e in particolare sul web".[5]

Se è indubbio che condotte lesive della dignità di persone e gruppi sociali rappresentino un ostacolo alla convivenza civile nella collettività, tuttavia azioni volte a contenere le comunicazioni che avvengono in internet possono tradursi in una limitazione del principio della libera manifestazione del pensiero. Parimenti, un intervento in via normativa sul fenomeno delle *fake news*, pur essendo mirato a tutelare le dinamiche della democrazia, potrebbe di fatto ledere l'espressione libera della politica sulle piattaforme *social*.[6] Ci si chiede, pertanto, se servano nuove norme per arginare i fenomeni descritti o se quelle già esistenti possano essere sufficienti a contrastare le condotte che, *on line* così come *off line*, violano prescrizioni dell'ordinamento; se una legge statuale – limitata per definizione all'ambito nazionale – non sia comunque uno strumento inadatto a regolare manifestazioni che travalicano confini di spazio e tempo; se si vogliano creare *social network* "italiani", disciplinati e controllati mediante norme italiane, in una società digitale che non prevede il concetto di confini; se sia preferibile e quali limiti incontri un approccio basato sulla *self-regulation*, più idonea ad adattarsi con sufficiente flessibilità ai rapidi mutamenti del contesto e all'evoluzione delle tecnologie; se il tentativo, comunque realizzato, di regolamentare il *web*, i *social* in particolare, ove si esercita la libertà di opinione e di informazione, nonché ove avviene in condizioni di parità una discussione civica resa possibile anche dall'anonimato, non rappresenti una forma di illiberalismo che espone i cittadini a una limitazione dei loro diritti fondamentali.

3 Si tratta di iniziative rimaste senza seguito. Al riguardo, C. Maietta, "Fake news, cosa rischia l'utente: tutte le leggi violate, i reati e gli illeciti", Wired, 27 marzo 2018. V. pure F. Chiusi e C. Frediani, "Giù le mani dal web", Wired, 7 marzo 2014, e F. Chiusi, "Perché diciamo no a una Commissione parlamentare d'inchiesta sulle 'fake news'", Valigia Blu, 18 novembre 2019.

4 Si tratta della petizione "Basta fake: stop ai profili falsi sui social network" proposta dall'onorevole Luigi Marattin.

5 Già nel 2009 era stata istituita una Commissione per lo svolgimento di un'indagine conoscitiva sull'antisemitismo, data la diffusione di quest'ultimo attraverso il *web*, in particolare i *social network*; successivamente, un'altra Commissione, istituita nel 2016 e intitolata alla parlamentare del Regno Unito, Jo Cox, uccisa per motivi di odio e intolleranza, aveva esaminato i fenomeni di odio, intolleranza, xenofobia e razzismo.

6 È il motivo per cui, mentre "Twitter ha scelto di eliminare la propaganda politica a pagamento perché in contrasto con la libertà di parola, Facebook ha deciso di continuare per questa via". L. Mastrodonato, "Twitter che rimuove la pubblicità politica a pagamento è una buona notizia", Wired, 31 ottobre 2019.

La responsabilità dei gestori di piattaforme tecnologiche.

Serve innanzitutto fare cenno alla disciplina riguardante soggetti che rendono possibili le attività sul *web*, vale a dire i gestori di piattaforme tecnologiche. La normativa di riferimento è contenuta nel d.lgs. n. 70/2003, emanato in attuazione della direttiva europea sul commercio elettronico 2000/31/CE, adottata al fine di agevolare la libera circolazione e la promozione dei servizi della società dell'informazione. La direttiva esenta gli "internet service providers" (ISP), in quanto fornitori di un servizio di *hosting* neutrale, da obblighi di sorveglianza sulle informazioni che trasmettono o memorizzano e di ricerca di fatti o circostanze che configurino attività illegali: ciò rappresenterebbe per essi un onere spropositato. A favore degli ISP opera, pertanto, una presunzione di non-conoscenza di eventuali illiceità dei contenuti *user-generated*, così che essi non sono gravati da responsabilità derivanti da questi ultimi. La direttiva citata, tuttavia, stabilisce a loro carico l'obbligo di informare senza indugio l'autorità giudiziaria o quella amministrativa qualora vengano a conoscenza di presunte attività o informazioni illecite riguardanti un utente; nonché a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in loro possesso che consentano l'identificazione dell'utente stesso, al fine di individuare e prevenire attività illecite. L'ISP **è civilmente responsabile dei contenuti pubblicati** solo nel caso in cui, richiesto dall'autorità giudiziaria o amministrativa, non abbia agito prontamente per impedire l'accesso a tali contenuti ovvero se, avendo avuto conoscenza del loro carattere illecito o pregiudizievole per un terzo, non abbia provveduto ad informarne l'autorità competente.

L'evoluzione del ruolo dei *social network* sta inducendo a porsi problemi circa la suddetta esenzione da responsabilità.[7] I gestori di tali piattaforme traggono profitto dalla raccolta dei dati degli utenti (il cosiddetto *user data profiting*), poiché di tali dati gli inserzionisti si servono al fine di individuare i profili cui destinare pubblicità mirata in base a gusti, preferenze, attitudini (*behavioural advertising*). Inoltre, attraverso l'utilizzo di algoritmi, i gestori sono in grado di evidenziare alcuni contenuti (*trending feeds*) rispetto ai quali le interazioni fra utenti sono più frequenti, sempre al fine di consentire agli inserzionisti una pubblicità mirata.

> Dunque, i social network provider **non si limitano a svolgere un'attività di** hosting neutrale, ma intervengono direttamente nell'organizzazione, nella gestione e talvolta anche nell'editing **dei contenuti, al fine di aumentare i ricavi derivanti dalla raccolta pubblicitaria**.[8]

Oltre a ciò, i *social network* stanno sviluppando sinergie con editori tradizionali i quali, considerati il volume di traffico e la raccolta pubblicitaria sui *social media*, stringono con i gestori di questi ultimi alleanze per raggiungere un pubblico più ampio e meglio profilato.

> 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». La giurisprudenza italiana, tuttavia, ha finora escluso che i social network possano essere considerati come "publisher", alla stregua di un mezzo di informazione tradizionale.[9]

7 M.R. Allegri, "Contenuti illeciti, responsabilità di social network e provider: tutto ciò che c'è da sapere", Agenda Digitale, 25 gennaio 2018.

8 Ibidem.

9 Corte di Cassazione n. 35511/2010, n. 31022/2015, n. 12536/2016, citata da M.R. Allegri, op.cit..

Hate speech

Non esiste una precisa definizione normativa di *hate speech*, cioè di discorso d'odio.[10] A livello europeo, una prima enunciazione si trova nella Raccomandazione del Comitato dei Ministri n. 20 del 1997 del Consiglio d'Europa, ove si dice che

> il termine "discorso d'odio (hate speech)" deve essere inteso come l'insieme di tutte le forme di espressione che si diffondono, incitano, sviluppano o giustificano l'odio razziale, la xenofobia, l'antisemitismo ed altre forme di odio basate sull'intolleranza e che comprendono l'intolleranza espressa attraverso un aggressivo nazionalismo ed etnocentrismo, la discriminazione l'ostilità contro le minoranze, i migranti ed i popoli che traggono origine dai flussi migratori.

Successivamente, la Decisione quadro dell'Unione europea sulla lotta contro il razzismo e la xenofobia (2008/913/GAI del 28 novembre 2008) ha qualificato come reato

> 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.

Più recentemente, la Raccomandazione di politica generale n. 15 della Commissione europea contro il razzismo e l'intolleranza del Consiglio d'Europa (ECRI) del 21 marzo 2016, ha definito il discorso d'odio come

> l'istigazione, la promozione o l'incitamento alla denigrazione, all'odio o alla diffamazione nei confronti di una persona o di un gruppo di persone, o il fatto di sottoporre a soprusi, molestie, insulti, stereotipi negativi, stigmatizzazione o minacce tale persona o gruppo, e comprende la giustificazione di queste varie forme di espressione, fondata su una serie di motivi, quali la "razza", il colore, la lingua, la religione o le convinzioni, la nazionalità o l'origine nazionale o etnica, nonché l'ascendenza, l'età, la disabilità, il sesso, l'identità di genere, l'orientamento sessuale e ogni altra caratteristica o situazione personale.[11]

In Italia esiste un ampio ventaglio di norme tese a contrastare fenomeni qualificabili come *hate speech*. In materia di discriminazione razziale, il complesso di disposizioni di maggiore organicità è costituito dalla l. n. 654/1975, di ratifica ed esecuzione della Convenzione contro il razzismo, adottata dalle Nazioni Unite a New York nel 1966, che punisce chi propaganda idee fondate sulla superiorità **o sull'odio razziale o etnico;** o istiga a commettere o commette atti di discriminazione per motivi razziali, etnici, nazionali o religiosi; ovvero, in qualsiasi modo, istiga a commettere o commette violenza o atti di provocazione alla

10 Da un punto di vista sostanziale, si può parlare di *hate speech* quando ricorrono i seguenti elementi: i) una chiara volontà e intenzione di incitare all'odio con la parola o altri mezzi di comunicazione; ii) un incitamento vero e proprio, idoneo a causare atti d'odio e di violenza nei confronti di soggetti presi di mira; iii) il verificarsi o il rischio imminente del verificarsi di atti di violenza o di discriminazione. Pertanto affermazioni, per quanto esecrabili, che non incitano terzi all'odio, non rientrano nell'ambito dell'*hate speech*. In questo senso, G. Ziccardi, "Il contrasto dell'odio online: possibili rimedi", in eticapubblica.it., luglio 2018.

11 Si segnala pure che nel dicembre del 2015 la Commissione ha istituito l'Internet Forum UE, ove ministri degli Interni degli Stati, rappresentanti delle principali società del *web*, Europol e altri soggetti valutano come proteggere dalla diffusione di materiale terroristico *on line* e fare un migliore uso della rete per contrastare discorsi d'odio e propaganda terroristica.

violenza per motivi razziali, etnici, nazionali o religiosi.[12] La l. n. 115/2016 - in applicazione della citata decisione quadro del Consiglio dell'Unione europea (2008/913 GAI) sulla armonizzazione delle legislazioni nazionali europee in tema di razzismo e xenofobia - ha aggiunto alla l. n. 654/1975 una norma che prevede una sanzione aggravata nei casi in cui la propaganda razzista, l'istigazione e l'incitamento ad atti di discriminazione razziale, etnica, nazionale o religiosa 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 penale internazionale» e siano commessi in modo che ne derivi «concreto pericolo di diffusione».[13] Va pure menzionata l. n. 205/1993 (cosiddetta legge Mancino) in materia di discriminazione razziale, etnica e religiosa, che sanziona chi, in pubbliche riunioni, compia manifestazioni esteriori od ostenti emblemi o simboli propri o usuali delle organizzazioni, associazioni, movimenti o gruppi aventi tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi. Anche il Testo unico sull'immigrazione (d.lgs. n. 286/1998) definisce condotte discriminatorie per motivi razziali, etnici, nazionali o religiosi, prevedendo l'azione civile. Il Testo unico della Radiotelevisione (d.lgs. n. 177/2005) e il Codice del consumo (d.lgs. n. 206/2005) vietano le trasmissioni che contengano incitamenti all'odio comunque motivato o che inducano ad atteggiamenti di intolleranza basati su differenze di razza, sesso, religione o nazionalità, nonché le trasmissioni pubblicitarie e le televendite che comportino discriminazioni di razza, sesso o nazionalità.[14] Va ricordata anche la l. n. 71/2017 volta a contrastare il fenomeno del cyberbullismo, cioè

> 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.

Questa 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. Infine, condotte di odio *on line* possono configurare le fattispecie penalmente rilevanti "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.).

Dalla disamina svolta appare palese che le normative in tema di discorsi d'odio coprono un ambito molto esteso e sono tali da colpire condotte illecite sia *off line* che *on line*. Tuttavia, negli anni scorsi, il verificarsi di attacchi terroristici e il contestuale proliferare di manifestazioni di odio razzista e xenofobo *online*, unitamente alla consapevolezza che l'applicazione delle leggi nazionali in materia debba comunque essere integrata da altre azioni, ha indotto

12 Il dettato normativo oggi vigente è il risultato di una modifica ad opera della l. n. 85/ 2006 che, oltre a ridurre i limiti edittali delle pene reclusive (peraltro già ridotti in precedenza con la l. n. 122/1993) 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 ha fatto sì che solo condotte di maggiore gravità integrino ipotesi di reato.

13 Successivamente, la l. n. 167/2017 (Legge europea 2017) ha previsto che - oltre la negazione - può costituire aggravante speciale del reato di cui alla l. n. 654/1975 anche la minimizzazione in modo grave o l'apologia della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra.

14 Con riferimento ai media radiotelevisivi, v. anche la Delibera n. 157/19/cons, 15 maggio 2019, dell'Autorità per le garanzie nelle comunicazioni: "Regolamento recante disposizioni in materia di rispetto della dignità umana e del principio di non discriminazione e di contrasto all'hate speech".

le istituzioni europee a intervenire al riguardo.[15] Così, nel maggio 2016, la Commissione UE e quattro tra le massime società dell'informatica (Facebook, Microsoft, Twitter e YouTube) hanno presentato un "Codice di condotta per contrastare l'illecito incitamento all'odio online".[16] Per garantire che internet rimanga un luogo di espressione libero e democratico, le società si sono impegnate – tra le altre cose - a proseguire gli sforzi per combattere i discorsi di odio *online*, elaborando "regole o orientamenti per la comunità degli utenti volte a precisare che sono vietate la promozione dell'istigazione alla violenza e a comportamenti improntati all'odio"; predisponendo "procedure chiare ed efficaci per esaminare le segnalazioni riguardanti forme illegali di incitamento all'odio nei servizi da loro offerti"; rivedendo le proprie politiche di funzionamento per rimuovere o disabilitare l'accesso ai contenuti vietati in meno di 24 ore. Nel Codice citato si sottolinea, comunque,

> la necessità di tutelare la libertà di espressione, che, come affermato dalla Corte europea dei diritti dell'uomo, si applica non solo alle informazioni o idee accolte favorevolmente o considerate inoffensive o indifferenti, ma anche a tutte quelle che offendono, sconcertano o disturbano lo Stato o una parte della popolazione.[17]

La Commissione europea monitora l'attuazione degli impegni pubblici del Codice a cadenze regolari: la quarta valutazione (4 febbraio 2019) ha rilevato un miglioramento costante nelle azioni previste. Infatti, le società informatiche sono arrivate a verificare entro 24 ore l'89 % dei contenuti segnalati e a rimuovere da Internet il 72 % dei contenuti ritenuti illeciti, contro il 40 % e il 28 %, rispettivamente, nel 2016.

Successivamente al varo del Codice, il 28 settembre 2017, la Commissione ha adottato una comunicazione (n. 555) contenente delle linee guida, destinate alle piattaforme *web*, sulle procedure di segnalazione e azione per contrastare i contenuti illegali *online*.[18] In particolare, la Commissione valorizza la cooperazione fra autorità competenti (giudiziarie e amministrative, nazionali ed europee) e gestori delle piattaforme digitali: le prime devono individuare regole chiare, da indirizzare agli operatori del settore, sulla definizione dei contenuti illeciti e sulle corrette procedure da seguire per eliminarli; i secondi devono approntare soluzioni tecniche idonee a raccogliere efficacemente le segnalazioni riguardanti i contenuti illeciti, in modo da poter provvedere alla loro rapida rimozione. La comunicazione suggerisce che il controllo di segnalazioni di contenuti illeciti non sia affidato solo a strumenti di filtraggio automatico, ma preveda l'intervento umano, e che siano approntate garanzie per limitare il rischio di rimuovere materiale lecito, sostenute da una serie di obblighi di trasparenza volti ad aumentare la responsabilità dei processi di rimozione.

15 Nella dichiarazione comune rilasciata dal Consiglio straordinario dei ministri della giustizia e degli interni del 24 marzo 2016 sugli attentati terroristici di Bruxelles si sottolinea che «la Commissione intensificherà i lavori presso le aziende informatiche, specie in sede di Forum dell'UE su Internet, per contrastare la propaganda terroristica e sviluppare, entro giugno 2016, un codice di condotta contro l'incitamento all'odio online».

16 Nel 2018 quattro nuove società hanno deciso di aderire al Codice: Google+, Instagram, Snapchat e Dailymotion.

17 Handyside contro Regno Unito, sentenza del 7 dicembre 1976, § 49.

18 La comunicazione, intitolata "Lotta ai contenuti illeciti online Verso una maggiore responsabilizzazione delle piattaforme online", fa seguito a una consultazione pubblica svoltasi fra il settembre 2015 e il gennaio 2016.

Il **1° marzo 2018 è stata pubblicata una raccomandazione della Commissione sulle misure per contrastare efficacemente i contenuti illegali** *on line*, che dispone meccanismi di segnalazione e azione più chiari, strumenti più efficaci, tecnologie proattive e garanzie più solide a tutela dei diritti fondamentali, nonché una più stretta collaborazione con le autorità.[19]

Fake News

Il rischio rappresentato dalle cosiddette *fake news* è stato esaustivamente esposto nella "Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni - Contrastare la disinformazione online: un approccio europeo", del 4 aprile 2018.[20] La comunicazione – che fa seguito alla istituzione da parte della Commissione di un gruppo di esperti incaricati di fornire consulenza e ad una consultazione pubblica - definisce come disinformazione

> un'informazione rivelatasi falsa o fuorviante concepita, presentata e diffusa a scopo di lucro o per ingannare intenzionalmente il pubblico, e che può arrecare un pregiudizio pubblico. Il pregiudizio pubblico include minacce ai processi politici democratici e di elaborazione delle politiche e a beni pubblici quali la tutela della salute dei cittadini, dell'ambiente e della sicurezza dell'UE. La disinformazione non include gli errori di segnalazione, la satira e la parodia, o notizie e commenti chiaramente identificabili come di parte.

Nella comunicazione si fa presente come *social media*, servizi di condivisione di video, motori di ricerca possano essere impiegati per diffondere disinformazione su vasta scala, rapida e precisa quanto a raggiungimento del gruppo *target*, «creando così bolle di informazione personalizzate e generando potenti camere di risonanza per le campagne di disinformazione». Queste ultime sono sfruttate per instillare sfiducia e produrre tensioni sociali; e, se poste in essere da Paesi terzi, possono minacciare la sicurezza interna e processi elettorali. La diffusione della disinformazione influenza anche i processi di elaborazione delle politiche dei governi, poiché può fuorviare l'opinione pubblica, condizionando il dibattito sociale e riducendo la fiducia nella scienza e nelle prove empiriche.[21] La Commissione rileva parti-

19 La "Raccomandazione della Commissione sulle misure per contrastare efficacemente i contenuti illegali online" si applica «a tutte le forme di contenuti illegali, da quelli di natura terroristica all'incitamento all'odio e alla violenza, dal materiale pedopornografico alle merci contraffatte e alle violazioni del diritto d'autore».

20 Circa le misure adottate da singoli Paesi, v. D. Giribaldi, "Disinformazione e complottismi online, tutte le misure di Governi e social network a contrasto", Agenda Digitale, 22 marzo 2019.

21 Va considerato anche quanto spiega L. Borga, "La disinformatia online non sposta voti", Il Foglio, 5 agosto 2019: l'autorità per le garanzie nelle comunicazioni (Agcom), nel report "News vs. fake nel sistema dell'informazione" del novembre 2018, quantifica i contenuti falsi all'1% del totale nel periodo del referendum costituzionale del 2016 e al 6% in prossimità delle elezioni politiche del marzo 2018; mentre, in un rapporto del maggio 2019 ("Osservatorio sulla disinformazione online"), l'Agcom rileva "un volume di disinformazione online" in occasione delle elezioni europee 2019 "nettamente inferiore a quanto registrato in concomitanza del periodo elettorale delle politiche del 2018". Negli Stati Uniti due ricerche - la prima di Allcott e Gentzkow ("Social Media and Fake News in the 2016 Election", in *Journal of Economic Perspectives*, Volume 31, Number 2, Spring 2017, pp. 211–236), la seconda di Guess, Nyhan e Reifler ("Selective Exposure to Misinformation: Evidence from the consumption of fake news during the 2016 U.S. presidential campaign", in *European Research Council* 9, 9

colari meccanismi che consentono la proliferazione della disinformazione: algoritmi, che favoriscono la condivisione di contenuti personalizzati tra utenti di vedute affini, aumentando la polarizzazione e rafforzando l'effetto della disinformazione; annunci pubblicitari con messaggi sensazionalistici, che incidono sulle emozioni dell'utente, a discapito della veridicità dei contenuti; tecnologie *online*, come servizi automatizzati (denominati "bot") e profili simulati, privi di un utente reale e orchestrati su vasta scala (le cosiddette "fabbriche di troll"), che potenziano artificialmente notizie e informazioni fuorvianti,.[22] Ma a diffondere la disinformazione contribuisce anche la condivisione indiscriminata, cioè senza alcuna verifica, di contenuti da parte degli utenti dei *social*, amplificata dal volume e dalla velocità sempre più elevata del flusso di materiale *online*. Secondo la Commissione, l'azione volta a contrastare la disinformazione dovrebbe essere orientata dai seguenti principi: trasparenza dell'origine dell'informazione e del modo in cui viene prodotta, promossa, diffusa e mirata, al fine di consentire agli utenti di valutare i contenuti cui accedono *online* e smascherare possibili tentativi di manipolare la loro opinione; diversità dell'informazione, per consentire ai cittadini di prendere decisioni informate, fondate su un pensiero critico; credibilità dell'informazione, mediante indicazioni circa la sua affidabilità con l'aiuto di segnalatori attendibili, il miglioramento della sua tracciabilità e l'autenticazione dei fornitori influenti; inclusività delle soluzioni proposte, cioè integrazione fra azioni di sensibilizzazione e alfabetizzazione mediatica, coinvolgimento delle parti interessate e cooperazione tra autorità pubbliche, piattaforme *online*, inserzionisti, segnalatori attendibili, giornalisti e gruppi editoriali.

A seguito di questa Comunicazione, nel settembre 2018, alcuni grandi operatori del settore (tra gli altri, Facebook, Twitter, Google e Mozilla) hanno sottoscritto un "Codice di condotta sulla disinformazione", allo scopo di combattere la disinformazione *on line*.[23] I firmatari del Codice si sono impegnati a:

interrompere le entrate pubblicitarie di determinati account e siti Web che

gennaio 2018) – sono arrivate alla conclusione che l'esposizione a notizie false in rete è in gran parte determinata dalla partigianeria dell'elettorato: cioè chi visita con maggiore frequenza siti di *fake news* sembra essere già convinto sulla propria preferenza politica. Nessuno dei due studi trova evidenza sufficiente per affermare che la disinformazione abbia avuto impatti elettorali. In altri termini, «il ruolo dei social media si limita a fornire agli utenti le informazioni a cui vogliono credere».

22 G. Rancilio, "Come si crea online una campagna di disinformazione", Avvenire, 8 novembre 2019, riporta i risultati della ricerca di J. Donovan e B. Friedberg, "Source hacking: media manipulation in practice", datasociety.net, settembre 2019, sulle tecniche usate in campagne di disinformazione. Il "viral sloganeering" consiste nel prendere i punti centrali di un messaggio politico di un partito o di un individuo e, attraverso l'uso di immagini e contenuti creati ad hoc, distorcerlo a proprio favore. Il "leak forgery" è la falsificazione ad arte di documenti inerenti alla vita privata di un politico che, pubblicati sotto forma di "fuga di notizie", ne screditano l'immagine. L'"evidence collage" opera la costruzione di una teoria del complotto attraverso la mescolanza di verità e bugie, realizzata sovrapponendo articoli di testate vere e riconoscibili a ritagli e articoli falsi. Il "keyword squatting" **è** la creazione di *account* e *hashtag* sui social allo scopo di "bombardare" gli spazi digitali con materiale manipolatorio e screditare l'immagine dei "nemici".

23 L'adozione del Codice, auspicata nella comunicazione dell'aprile 2018, è stata voluta dalla Commissione europea anche in vista delle elezioni europee della primavera 2019, per evitare quanto più possibile l'influenza delle *fake news* sul voto, contribuendo a «una campagna online trasparente, corretta e affidabile (...) nel pieno rispetto dei principi fondamentali della libertà di espressione dell'Europa, della libertà di stampa e del pluralismo».

> **diffondono disinformazione; aumentare la trasparenza della pubblicità politica; affrontare la questione degli account falsi e dei bot online; facilitare l›accesso a diverse fonti d›informazione**, migliorando la visibilità dei contenuti autorevoli, e rendere più facile la segnalazione di notizie false; consentire alla comunità di ricerca di accedere ai dati delle piattaforme per monitorare la disinformazione online attraverso modalità conformi alle norme sulla privacy.

Nel marzo 2019, **è stato implementato** un Sistema d'allerta rapido (Ras) contro le *fake news*, per mettere a disposizione di istituzioni Ue e Stati membri una piattaforma dove far confluire in modo rapido i dati, in formato *open source* (cioè di pubblico accesso), sulle campagne di disinformazione *on line*, oltre che le analisi di studiosi e il lavoro di *fact-checker*.

A seguito dell'adozione del suddetto Codice, sono stati previsti rapporti annuali di autovalutazione sulla sua attuazione, presentati dai suoi firmatari. Nei primi rapporti, pubblicati dalla Commissione europea nell'ottobre scorso, gli operatori affermano di aver fatto progressi, soprattutto dal punto di vista dalla trasparenza, e di aver intensificato la collaborazione sia con le autorità nazionali che con alcuni esponenti della società civile, come ricercatori e *fact-checker*.[24] Alcuni dei *report* indicano il numero di *post* pubblicitari rimossi poiché in violazione delle regole d'uso della piattaforma, ad esempio quelle che proibiscono di diffondere dichiarazioni false; il numero degli *account fake* eliminati; le decisioni adottate per evitare la disinformazione e favorire un più ampio accesso ai dati agli esperti. «Facebook, per esempio, ha citato l'introduzione della funzione "Perché vedo questo post" (…) mentre Twitter ha sottolineato il lancio di un nuovo strumento che rimanda gli utenti a fonti autorevoli quando cercano parole chiave associate ai vaccini».[25] Tuttavia, al di là delle affermazioni positive contenute nelle autovalutazioni, dalla applicazione del Codice emergono anche ombre rilevanti. Al riguardo, va premesso che, prima della sua pubblicazione, la Commissione aveva chiesto su tale documento il parere di un gruppo di esperti esterni, i quali erano stati piuttosto critici circa la sua efficacia, evidenziando in particolare che esso non contiene

> né un approccio comune efficace, né impegni significativi, né obiettivi misurabili o indicatori chiave di prestazione (gli indici che monitorano l'andamento di un processo aziendale), né strumenti che permettano di controllare il rispetto o monitorare l'implementazione del processo.[26]

Quanto rilevato *ex ante* dagli esperti si ritrova nelle considerazioni della Commissione a margine della pubblicazione delle suddette relazioni di autovalutazione: essa rileva, tra l'altro, che

> i progressi realizzati variano (…) notevolmente tra i firmatari e le relazioni forniscono scarse informazioni sull'effettiva incidenza delle misure di autoregolamentazione adottate nel corso dell'anno precedente e sui meccanismi di controllo indipendente
>
> …

24 "Annual self-assessment reports of signatories to the Code of Practice on Disinformation 2019", 29 October 2019, in *European Commission*, *Digital Single Market*.

25 Al riguardo, G. Giacobini, "I social network potrebbero fare molto di più per contrastare le fake news", Wired, 29 ottobre 2019.

26 "The sounding board's unanimous final opinion on the so-called code of practice, 24 september 2018" in ec.europa.eu.

i dati e gli strumenti messi a disposizione di ricercatori e società civile per analizzare la materia sono stati sporadici e arbitrari, non rispondendo ad esigenze di ricerca più ampie»; «occorre fare di più in tutti i settori contemplati dal codice.

Circa questo tema, va ancora segnalato che, di recente, l'amministratore delegato di Twitter ha reso nota l'intenzione di bloccare le inserzioni pubblicitarie a sfondo politico sulla sua piattaforma, non volendo porsi come contenitore di *marketing* politico a pagamento. Egli ha motivato la decisione col fatto che la pubblicità sul *web* comporta significativi rischi politici, se usata per spostare voti e influire sulla vita di milioni di persone, e che ciò non ha nulla a che fare con la libertà di espressione.[27] Al contrario, l'amministratore delegato di Facebook ha deciso di continuare a consentire le pubblicità politiche, in quanto esse rappresentano una componente essenziale della predetta libertà, che non va limitata.[28]

Tutela dell'anonimato e identificazione on line

In precedenza si è fatto cenno a un'iniziativa tesa a vietare l'anonimato *online*.[29] Al riguardo, è opportuna una premessa. In un'epoca di iperproduzione normativa, ove le disposizioni si affastellano confusamente e l'attivismo dei governi si misura in numero di regole varate anziché in termini di risultati ottenuti, prima di avanzare qualsivoglia proposta occorre-

27 Al riguardo, è molto critico M. Flora, "Perché bloccare la pubblicità politica su Twitter non serve (ed è dannoso)", in mgpf.it, 3 novembre 2019: «utenti Fake, le dinamiche di brigading, le reti di bot e di inauthentic behaviour e gli state-sponsored attacks sono il vero problema della ingerenza politica della piattaforma, e non passano certamente attraverso operazioni che richiedono alcun tipo di pubblicità a pagamento. E la polarizzazione (o meglio auto-polarizzazione) sulla rete passa non già attraverso i banner pubblicitari (…), ma soprattutto attraverso la creazione di un consenso algoritmico che la piattaforma non tocca in alcun modo con queste sparate sensazionalistiche. Lasciando sul piatto non solo un budget di pubblicità che è praticamente nullo» – 0,5% dei ricavi annuali di Twitter – «ma che diventa comunque sempre più costoso gestire e controllare viste le normative sempre più stringenti di moltissimi stati sullo spending pubblicitario online (…). se dobbiamo capire quali sono le misure da prendere per evitare scandali come quello di Cambridge Analytica la risposta non è vietare la pubblicità politica, ma vietare il micro-targeting». Secondo Openpolis, "La propaganda social e la difficile definizione di politica", 11 novembre 2019, pare «che sia Facebook che Google vogliano eliminare il micro targeting per le inserzioni pubblicitarie politiche».

28 Come esposto da L. Mastrodonato, op. cit., «in molti hanno evidenziato i rischi connessi a questa visione. La candidata democratica americana Elizabeth Warren ha comprato uno spazio sulla piattaforma per diffondere appositamente una bufala, così da dimostrare al Ceo di Facebook la pericolosità del suo discorso. La deputata Alexandria Ocasio-Cortez ha invece pressato Zuckerberg durante un'audizione in Senato, chiedendogli in modo secco se Facebook avesse intenzione di rimuovere le bugie politiche evidenti dalla sua piattaforma. Il patron era in difficoltà, ha sviato alle domande, dimostrando probabilmente una certa consapevolezza sull'assurdità del suo stesso messaggio». L'autore spiega pure come la Lega abbia speso «circa 124mila euro in pubblicità per la sua pagina Facebook. Tra i contenuti sponsorizzati, notizie di cronaca capaci di gonfiare il suo consenso, come quelle relative a stupri, rapine o simili commessi da immigrati. Un modus operandi che rischia di trasformare i social in pannelli pubblicitari a bordo strada, o sui palazzi in ristrutturazione. Spazi da comprare per amplificare l'eco dei propri messaggi. L'idea che basti pagare per pubblicare qualunque tipo di contenuto e renderlo virale è sbagliata, perché rinnega la natura di queste piattaforme e soprattutto può trasformare la libertà di espressione in un diritto (comprato) alla disinformazione».

29 V. nota 4.

rebbe valutarne gli impatti e la fattibilità. Ebbene, vi sono una serie di motivazioni per cui sancire il divieto di anonimato in rete, da un lato, è potenzialmente dannoso per la libertà di espressione; dall'altro lato, è inutile perché gli *hater* sono identificabili già ora e il divieto sarebbe facilmente aggirabile.

Circa il primo profilo, l'idea di introdurre obblighi di identificazione per l'uso dei servizi *on line* è stata criticata nel 2013 dal Relatore speciale per la libertà di espressione per l'ONU Frank La Rue. Considerato che la sorveglianza nelle comunicazioni può costituire una minaccia per la società democratica, il Relatore aveva chiesto agli Stati di garantirne la sicurezza per ogni individuo - in particolare giornalisti, attivisti dei diritti umani e *whistleblowers* - nonché di astenersi «dal forzare l'identificazione degli utenti come condizione preliminare per l'accesso alle comunicazioni…».[30] Ancora, nel 2015 il Relatore speciale David Kaye ha rilevato l'importanza di garantire e proteggere l'anonimato e la crittografia, che consentono agli individui «di esercitare i loro diritti alla libertà di opinione e di espressione nell'era digitale e, come tali, meritano una forte protezione».[31] Inoltre, la Risoluzione del Parlamento europeo dell'8 settembre 2015, intitolata "Diritti umani e tecnologia: impatto dei sistemi di sorveglianza e di individuazione delle intrusioni sui diritti umani nei paesi terzi", invita «a promuovere strumenti che consentono l'utilizzo anonimo e/o pseudonimo di Internet», in quanto garanzia per gli «attivisti dei diritti umani all'interno e all'esterno dell'Ue».[32] Il diritto all'anonimato in rete è tutelato anche attraverso l'art. 8 (Diritto al rispetto della vita privata e familiare) e dall'art. 10 (Libertà di espressione) della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU), le cui previsioni trovano una più piena attuazione mediante il rispetto di tale diritto. Per quanto attiene all'Italia, la Commissione per i diritti e i doveri relativi ad Internet, composta da parlamentari ed esperti, nel 2015 ha elaborato la "Dichiarazione dei diritti di Internet", ove tra l'altro si afferma che

> ogni persona può accedere alla Rete e comunicare elettronicamente usando strumenti anche di natura tecnica che proteggano l'anonimato ed evitino la raccolta di dati personali, in particolare per esercitare le libertà civili e politiche senza subire discriminazioni o censure.

Quanto al secondo profilo, relativo all'inutilità di una sorta di carta d'identità *social*, va innanzitutto osservato che la correlazione tra anonimato e discorsi di odio non è scontata.[33] «Anzi le persone esibiscono in modo trionfante espressioni e posizioni odiose, vogliono che gli sia riconosciuto il coraggio di esprimersi in quel modo, sono in cerca narcisistica-

30 Consiglio delle Nazioni Unite per i diritti umani, "Rapporto del relatore speciale sulla promozione e protezione del diritto alla libertà di opinione e di espressione" , 17 aprile 2013.

31 Consiglio delle Nazioni Unite per i diritti umani, "Rapporto del relatore speciale sulla promozione e protezione del diritto alla libertà di opinione e di espressione", 22 maggio 2015.

32 Negli Stati Uniti, nel 1995, la Corte Suprema (McIntyre v. Ohio Elections Commission, 514 U.S. 334) ha definito l'anonimato come «uno scudo dalla tirannia della maggioranza. Ciò, dunque, esemplifica lo scopo alla base del Bill of Rights e del Primo Emendamento, in particolare: proteggere gli individui impopolari dalle rappresaglie e le loro idee dalla soppressione, per mano di una società intollerante».

33 Al riguardo, v. K. Rost, L. Stahel, B.S. Frey (2016), "Digital Social Norm Enforcement: Online Firestorms in Social Media", in journals.plos.org. Inoltre, A. Antoci, L. Bonelli, F. Paglieri, T. Reggiani, F. Sabatini, F. (2019), "Civility and trust in social media. Journal of Economic Behavior & Organization", 160 83-99.

mente di like, condivisioni, approvazione».[34] Pertanto, il divieto normativo di anonimato non migliorerebbe il clima sui *social media*. Detto ciò, usare un *nickname* non è anonimato: significa soltanto che ci si è registrati con un nome e cognome e poi si è scelto di comparire *on line* con un "soprannome", ma si è identificabili comunque.

> In pochissimi hanno l'abilità di muoversi online dietro anonimato (…). Ognuno di noi quando si collega da un computer o da mobile usa un IP (un indirizzo) che permette facilmente di individuare da quale device ci si è collegati (…). Certo in una indagine per una ipotesi di reato si dovrà anche dimostrare che quel device appartenente a X sia stato poi usato proprio da X per commettere il reato su cui si indaga. Vale lo stesso però se decidiamo di rendere obbligatoria la registrazione con un documento di identità. Bisognerà dimostrare che quell'account è stato usato proprio da quella persona nel momento in cui è stato compiuto un reato o un illecito civile (diffamazione, insulto...).[35]

Pertanto, anche qualificandosi o*n line* con un documento - come vorrebbe la proposta da ultimo avanzata - la procedura di accertamento rimarrebbe esattamente la stessa.[36] In conclusione,

> nel web non esiste una zona franca. Non c'è l'anarchia. Ma vigono le stesse leggi che vigono offline. Se commetti un reato, ci sarà una indagine per stabilire le responsabilità e poi un eventuale processo. In caso di colpevolezza le leggi si applicano anche per i comportamenti online. Diffamare o insultare online è considerato addirittura una circostanza aggravante.[37]

Quindi, il divieto di anonimato è inutile poiché esistono già adesso procedure tecniche e giuridiche che consentono di identificare gli *hater*. E se questi ultimi non vengono perseguiti è perché «non c'è personale inquirente o giudiziario sufficiente per applicare le procedure, o perché i costi sono altissimi, non perché non si sa chi sia il colpevole».[38]

A ciò si aggiunga che, se una legge nazionale ponesse a carico di piattaforme *social* un obbligo di identificazione dei propri utenti, essa riguarderebbe solo il territorio italiano e, dunque, non chi si collegasse dall'estero o, mediante artifici realizzabili agevolmente, facesse risultare che sta «"entrando" da un altro Paese per aggirare il controllo».[39] Di fatto, una

34 A. Ciccone, "Odio e disinformazione: il problema non è l'anonimato e schedare 30 milioni di italiani non è la soluzione", Valigia Blu, 6 novembre 2019.

35 Ibidem.

36 M. Canducci, "Di anonimato in rete, libertà e diritti", TechEconomy, 30 ottobre 2019, spiega che «è tecnicamente possibile risalire fino al dispositivo utilizzato e non alla persona che lo ha utilizzato» la quale, «in possesso di adeguate credenziali, potrebbe utilizzare tranquillamente l'account di qualcun altro. Questa situazione si ripresenterebbe identica anche in caso di account social per i quali in qualche modo l'identità del proprietario sia certificata, consentendo nella pratica l'utilizzo di un account social anche da parte di chi non ne sia il legittimo proprietario ed anche in presenza di identità certificate».

37 A. Ciccone, op. cit..

38 P. Attivissimo, "Perché identificare tutti sui social network è una pessima idea?", Il Disinformatico, 1° novembre 2019.

39 G. Ziccardi, "Profili sui social network e carta d'identità: perché non è possibile", 2 novembre 2019, in ziccardi.ghost.io.

legge che sancisse il divieto di anonimato sui *social* usati in Italia potrebbe preludere alla creazione di *social* "sovranisti", con frontiere chiuse per chi, collegandosi dall'estero, non si registri: tuttavia, «il solo pensiero di poter individuare un social network nazionale, o "italiano", da poter controllare, quando la società digitale ha da tempo eliminato l'idea di confini, è un errore marchiano».[40]

> Possiamo noi italiani creare un cyber-wall, come la Cina, e imporre solo ai nostri utenti una identificazione certa per tutti i servizi digitali, e imporre alle piattaforme digitali di far accedere ai loro servizi solo utenti che abbiano fornito un documento di identità in modo certo? (…) vogliamo davvero creare un cyber-wall italiano? Dopo i porti fisici, vogliamo chiudere anche quelli digitali? Ci rendiamo conto che in quel caso i "profughi", gli esclusi saremmo noi? Che i più bravi userebbero una VPN per continuare a navigare come prima - in qualche caso, insultare come prima - e che tutti gli altri avrebbero una vita molto più povera?.[41]

In altri termini, se si considera la facilità con cui oggi «si può entrare in rete e creare profili aggirando i limiti nazionali, collegandosi con VPN o siti all'estero, in una rete che è nata geneticamente per aggirare simili tipi di controllo», appare chiaro come una normativa di divieto dell'anonimato in rete sia tecnicamente inattuabile o, al limite, attuabile con costi e rischi altissimi.[42] A quest'ultimo riguardo, si consideri che

> gestire i documenti d'identità di milioni di persone costa ed è complicato. Gli utenti italiani di Facebook, per esempio, sono circa 29 milioni. Ciascuno di loro dovrebbe depositare un documento. Chi paga? Chi organizza? Chi verifica che i dati siano validi? Chi custodisce questi dati, vista la facilità con la quale vengono spesso rubati? Cosa si fa per gli account esistenti? Li sospendiamo in massa? (…) Cosa succede a un turista che arriva in Italia e vuole usare il suo account social? Deve prima depositare un documento? Chi controlla se lo fa o no? E come fa a controllare? (…) La procedura andrebbe ripetuta per ogni singolo social network e per ogni spazio digitale pubblico (…) più tutti gli spazi di commento delle testate giornalistiche e dei blog. A quante aziende dovremmo dare i nostri documenti? E a quale titolo un blogger dovrebbe gestire i dati personali dei propri commentatori?.[43]

E comunque non va dimenticato che i *social network*, ad esempio, sono aziende il cui mestiere è vendere i dati degli utenti.

> Non è come dare la carta d'identità a un operatore telefonico per aprire un'utenza cellulare: l'operatore (…) non ha come scopo commerciale la vendita dei fatti nostri. Non è come lasciare un documento alla reception dell'albergo: in realtà non lo si lascia, ma si viene identificati dal portiere tramite il documento, e i dati vengono raccolti dalla polizia quotidianamente, non finiscono in un gigantesco database gestito da privati (…). Siamo sicuri che per esempio Facebook, quella di Cambridge Analytica, sia un'azienda alla quale affidare la garanzia di

40 Ibidem.

41 R. Luna, "Caro Marattin, la carta d'identità per i social ci rende profughi digitali", Repubblica, 30 ottobre 2019.

42 G. Ziccardi, op. cit..

43 P. Attivissimo, op.cit..

> chi siamo? (…) Equivale a una schedatura di massa. Creerebbe insomma un immenso database centralizzato di dati personali di decine di milioni di italiani, messo in mano non a un'autorità governativa ma una società commerciale o, peggio ancora, a regimi non tolleranti delle opinioni altrui.[44]

In alternativa, si potrebbe incaricare un ente certificatore di raccogliere i documenti di riconoscimento degli utenti e di comunicare alle piattaforme che il soggetto è stato identificato e può quindi accedervi, rilasciando un codice di autenticazione. Ma, in questo modo, non si eliminerebbero i problemi sopra elencati e, comunque, si centralizzerebbe la raccolta di documenti personali presso un soggetto privato, con conseguente pericolo di *data breach*, cioè con un rischio ancora maggiore di quello che si vorrebbe contrastare vietando l'anonimato. Peraltro, servirebbe «il necessario parere del Garante Privacy che, per tradizione, è sempre stato contrario alla raccolta di simili documenti».

Circa l'(in)utilità di un obbligo di identificazione prima di accedere a *social network*, occorre porsi una domanda ulteriore: «in che modo abolire l'anonimato porterebbe i politici o attori maligni a smettere di manipolare l'opinione pubblica»?[45] Cioè può sostenersi che la disinformazione sia favorita dall'anonimato? Nei fatti, si riscontra che essa è prodotta da politici che scientemente manipolano le opinioni dei cittadini, dal cattivo giornalismo, da istituzioni che diffondono informazioni distorte o selezionate per inquinare il dibattito pubblico: quindi, da persone precise. Peraltro, la disinformazione - finalizzata ad attaccare gli avversari politici, a fare propaganda pro-governo o pro-partito, a diffondere notizie tese a creare divisione - è realizzata non solo mediante *account* bot, *account* "cyborg" e *follower* falsi, ma attraverso tattiche come *micro-targeting*, *meme*, *fake news*, nonché altri tipi di condizionamento più subdoli e difficili da intercettare. Tra le altre tecniche, si usano «strumenti di segnalazione sui social per censurare post, sperando nel processo automatizzato di rimozione di contenuti anche se questi non violavano le regole della piattaforma» oppure «hashtag per diffondere il più possibile un messaggio».[46] Quanto esposto rende palese come la disinformazione non sia connessa all'anonimato: non a caso, tra le iniziative – sopra indicate - adottate in sede europea in collaborazione con le piattaforme informatiche, per contrastare manipolazione e propaganda *on line*, non è prevista la schedatura di milioni di utenti del *web*.

Conclusioni

Come sopra esposto, le soluzioni elaborate al fine di arginare fenomeni di *hate speech* e *fake news* al momento si sostanziano per lo più in codici di autoregolamentazione, "regole

44 Ibidem.

45 A. Ciccone, op. cit., fa un lungo elenco di esempi di disinformazione e aggiunge che «l›ultimo rapporto 2019 sulla disinformazione attraverso i social media, firmato dall›Università di Oxford, ha trovato evidenze di attività di manipolazione da parte di agenzie governative o di partiti politici in 70 paesi. La maggior parte della propaganda è creata da persone vere e proprie: l›87% dei paesi usa account umani, non solo bot. Alcuni paesi assumono studenti o gruppi di giovani per la propaganda computazionale, inclusi Russia e Israele. L›aumento riscontrato di questa tipologia di propaganda è dovuto all›incremento dei paesi che vedono i social media come strumento di potere geopolitico». Il rapporto cui si fa riferimento è: "The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation", S. Bradshow e P.N. Howard, *Oxford Internet Institute*, 26 settembre 2019.

46 Ibidem.

d'uso" delle varie piattaforme, meccanismi di segnalazione di messaggi lesivi da parte degli utenti, individuazione e rimozione di contenuti e *account* falsi da parte dei gestori delle piattaforme stesse. Ma questa soluzione, in forza della quale c'è **«qualcuno che decide per noi cosa dobbiamo leggere, e** quindi che plasma la nostra visione del mondo», non può reputarsi ottimale.[47] Essa rappresenta «una vera e propria delega di funzioni statali» alle aziende tecnologiche; inoltre, in mancanza di definizioni certe delle categorie di contenuti da cancellare e di adeguati strumenti di impugnazione delle decisioni da parte degli utenti che ne sono oggetto, può prodursi una compressione dei loro diritti; infine, il potere di rimozione di determinati contenuti determina il rischio della cancellazione di elementi di indagine.[48]

Per un altro verso, occorre fare attenzione a pretendere forme di censura in rete: «provvedimenti di soppressione dei discordi d'odio (…) possono portare anche ad abusi (…). Paradossalmente le limitazioni alla libertà di espressione, giustificate da esigenze di repressione dell'odio online», potrebbero portare a soffocare espressioni di dissenso, attraverso **«accuse verso le opposizioni politiche di fomentare l'odio sociale».**[49] Soprattutto, l'eliminazione di messaggi di *hate speech* dai *social* rappresenta solo un rimedio palliativo, che non previene né ostacola la formazione nell'opinione pubblica di idee basate su intolleranza e discriminazione, ma semplicemente ne impedisce o tenta di impedirne la diffusione attraverso internet, spostandone la manifestazione altrove, ove forse essa è meno visibile.[50] In altri termini, la cancellazione *on line* non risolve un problema che nasce e si esprime comunque anche *off line*. Il fenomeno dell'odio in rete va, pertanto, affrontato non solo in funzione delle particolarità del mezzo – il *web* – mediante cui viene esternato, ma soprattutto attraverso l'analisi delle cause sottostanti.

Ciò che può proporsi, innanzitutto, è la valorizzazione della

> cultura della legalità, dell'affettività, del rispetto dei soggetti deboli e delle minoranze (…), condannando per primi quei rappresentanti delle istituzioni, della politica, dei media che da anni usano l'odio e la disseminazione di false informazioni per raccogliere consenso (…). È sufficiente andare a scorrere i toni, e i tweet, di molti politici che ora si stanno stracciando le vesti e si lamentano del web che sarebbe diventato ingestibile per comprendere quanta ipocrisia ci sia.[51]

Così come il contrasto allo *hate speech*, anche quello alle *fake news* e, più in generale, alla disinformazione richiede la promozione di politiche volte all'educazione e responsabilizzazione dei cittadini, nonché un'azione tesa ad alimentare il pluralismo informativo. Su queste basi, la presenza *on line* di notizie controverse unitamente ad altre in grado di confutarle può avviare una discussione pubblica in grado di portare a una crescita sociale che renda

47 B. Saetta, "Perché le soluzioni al problema 'fake news' sono a loro volta un problema", Valigia blu, 17 Novembre 2017.

48 B. Saetta, "Per una regolamentazione delle piattaforme digitali", Valigia Blu, 8 Novembre 2019. V. pure B. Saetta, "Contrastare l'hate speech online: questioni aperte e alcune proposte", Valigia Blu, 18 febbraio 2017.

49 B. Saetta, "Contrastare l'hate speech online", cit..

50 In questi termini M.R. Allegri, "Odio online, le norme italiane vs il ruolo delle web company", Agenda Digitale, 23 luglio 2018.

51 Ziccardi, op. cit..

più critici rispetto a ciò che si legge, «più esigenti della prova e della provenienza delle notizie, più autosufficienti nel pensiero».[52] La soluzione non è, pertanto, la limitazione dei contenuti sul *web*, bensì il suo opposto: cioè favorire diverse e credibili fonti di informazione, «promuovere l'alfabetizzazione all'uso dei media e del digitale e diffondere – anche a livello governativo – informazioni affidabili sulle materie di pubblico interesse».[53] Servirebbero, altresì, regole più chiare e maggiore trasparenza dei *social media* sul *marketing* politico realizzato per il loro tramite, specie sulla sua fonte, applicando ad esso gli stessi standard delle altre pubblicità, incluso un trattamento grafico che lo renda più riconoscibile.[54]

Infine, «solo cittadini più maturi e consapevoli saranno in grado di muoversi in un mondo sempre più complesso e articolato». Essi

> hanno bisogno di un percorso educativo nuovo che vada ben oltre il semplice addestramento all'uso delle app o lo studio della tecnologia, in quanto la potenza e la pervasività degli strumenti e dei paradigmi del digitale richiedono un salto di qualità nel livello di maturità, nelle competenze e conoscenze di cultura generale e nei modelli cognitivi e comportamentali.

Ciò significa soprattutto

> **riconoscere gli altri, ancora prima delle loro idee; studiare, capire, ascoltare, costruire posizioni ragionate; non aver paura di confrontarsi; avere il coraggio di riconoscere i propri errori e cambiare idea.**[55]

In conclusione, trasparenza da parte dei gestori delle piattaforme, cultura della legalità, pluralismo, alfabetizzazione all'informazione, educazione alla conoscenza e percorsi di sviluppo delle capacità cognitive, non censure tecniche e normative, possono rappresentare gli strumenti più adeguati per contrastare discorsi d'odio e disinformazione.

52 B. Saetta, "Perché le soluzioni al problema 'fake news' sono a loro volta un problema", cit..

53 G. Scorza, "Fake-news: no ad ogni censura normativa o tecnologica", L'Espresso, 4 marzo 2017.

54 Openpolis, op. cit.. G. Scorza, Micro-targeting, profilazioni, algoritmi: il vero problema etico è l'uso da parte della politica dei dati dei cittadini", Valigia Blu, 22 aprile 2018. Circa l'uso del Regolamento europeo sulla tutela dei dati personali n. 2016/679 (GDPR) per il *microtargeting* e la necessità di una normativa integrativa, v. A. Spedicato, "Microtargeting e profilazione politica: tutti i rischi di un uso senza regole", 12 novembre 2019, Agenda Digitale.

55 A. Fuggetta, "Cittadini ai tempi del web", ed. Franco Angeli, 2018.

Istituto Bruno Leoni
idee per il libero mercato

IBL Focus

Chi Siamo

L'Istituto Bruno Leoni (IBL), intitolato al grande giurista e filosofo torinese, nasce con l'ambizione di stimolare il dibattito pubblico, in Italia, promuovendo in modo puntuale e rigoroso un punto di vista autenticamente liberale. L'IBL intende studiare, promuovere e diffondere gli ideali del mercato, della proprietà privata, e della libertà di scambio. Attraverso la pubblicazione di libri (sia di taglio accademico, sia divulgativi), l'organizzazione di convegni, la diffusione di articoli sulla stampa nazionale e internazionale, l'elaborazione di brevi studi e briefing papers, l'IBL mira ad orientare il processo decisionale, ad informare al meglio la pubblica opinione, a crescere una nuova generazione di intellettuali e studiosi sensibili alle ragioni della libertà.

Cosa Vogliamo

La nostra filosofia è conosciuta sotto molte etichette: "liberale", "liberista", "individualista", "libertaria". I nomi non contano. Ciò che importa è che a orientare la nostra azione è la fedeltà a quello che Lord Acton ha definito "il fine politico supremo": la libertà individuale. In un'epoca nella quale i nemici della libertà sembrano acquistare nuovo vigore, l'IBL vuole promuovere le ragioni della libertà attraverso studi e ricerche puntuali e rigorosi, ma al contempo scevri da ogni tecnicismo.

Istituto Bruno Leoni – Piazza Cavour 3 - 10123 Torino – Italy
T: +39 (011) 1978 1215 – F: +39 (011) 1978 1216 – www.brunoleoni.it – info@brunoleoni.it