Aspettando
La buona battaglia

L'educazione civica

Il molteplice della rete

Nel 2017 la rivista "Il Mulino" ha pubblicato una serie di contributi di studiosi di varia formazione sulle possibilità e i problemi della rete, soprattutto in relazione all'istruzione e all'acculturazione. Questo è quello del giurista Giovanni Ziccardi.

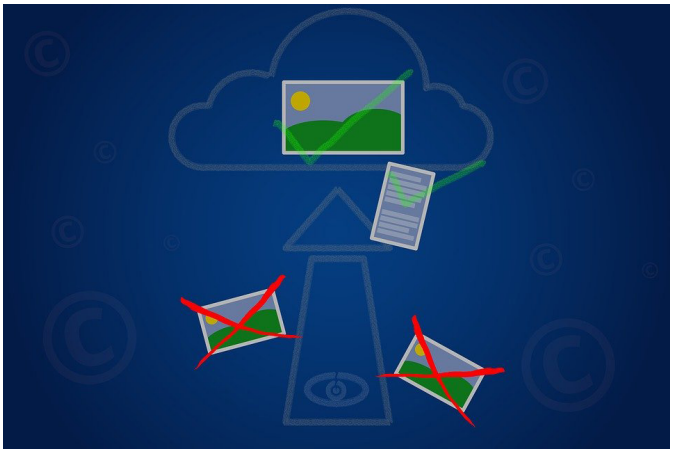
Giovanni Ziccardi

La soluzione c'è: si chiama censura

Giovanni Ziccardi insegna Informatica giuridica all'Università di Milano. Avvocato, pubblicista e scrittore, ha pubblicato *L'odio online* (Cortina, 2016), *Il libro digitale dei morti. Fine della vita, immortalità e oblio all'epoca di Internet* (Utet, 2017) e *Tecnologie per il potere. Come utilizzare i Social Network in politica* (Cortina, 2019).

«Internet interpreta la censura come un qualcosa di dannoso, e ruota attorno ad essa senza problemi». La Rete è geneticamente *impermeabile* a ogni tentativo di controllo. Lo aggira, lo evita, e gioca con la censura stessa per poi liberarsene senza particolari sforzi. Questo è il senso della celebre – e storica – frase citata in esordio, e attribuita all'imprenditore tecnologico **John Gilmore** (richiamata in P. Elmer-Dewitt, *First Nation in Cyberspace, «Time Magazine»*, n. 49, 6.12.1993), uno degli attivisti più influenti nel mondo digitale: ha contribuito a fondare la Electronic Frontier Foundation, la più importante associazione per la tutela dei diritti civili nel cyberspazio.

Si tratta di una sintesi efficace di come i tecnici più preparati, quelli che hanno visto nascere Internet e hanno disegnato la sua architettura e i protocolli di trasmissione dei pacchetti di dati, interpretino la possibilità di una censura in Rete e di un controllo capillare e pervasivo dei contenuti che circolano online come *impossibile*. In teoria, quindi, questo primo ostacolo tecnico oggettivamente insormontabile dovrebbe soffocare immediatamente qualsiasi discussione sul punto: non sarebbe realistico parlare di censura in senso stretto nell'attuale ambiente tecnologico per il semplice motivo che, anche se vi fosse l'intenzione di censurare, ciò non sarebbe tecnicamente possibile. Ciò nonostante, sono ormai



sempre più frequenti le istanze provenienti dal mondo della politica che domandano un maggior controllo sui contenuti presenti in Rete: dal filtraggio degli stessi alla possibilità di una loro cancellazione definitiva, da una maggiore responsabilizzazione (e, quindi, condizionamento) dei provider sino al blocco di determinati tipi d'informazione. Tutte forme, in sostanza, di *censura indiretta*.

In occasione di eventi tragici di cronaca che scuotono le coscienze (come il suicidio di Tiziana Cantone nel settembre del 2016), di attentati terroristici o di fatti che, «semplicemente», sembrano mettere in pericolo equilibri politici (si pensi al recentissimo timore che notizie false e bufale possano condizionare tornate elettorali o influenzare drasticamente l'opinione dei cittadini su temi d'interesse politico) si moltiplicano le proposte bipartisan di nuove leggi che cerchino di risolvere il problema tramite la sanzione penale e altri rimedi correlati più o meno censori. Sempre muovendo dal presupposto errato che manchino le leggi che disciplinano il mondo della Rete e che si sia in presenza di un Far West giuridico quando, in realtà, ormai anche il mondo digitale è iper-regolamentato.

Un'analisi di questa «tendenza alla censura», antica come la Rete stessa e che a cadenza regolare riemerge sui temi tecnologici, si deve basare su tre aspetti cardine, indipendenti tra loro, che permettono di «sezionare» il problema per poi, al termine del ragionamento, riportarlo a unità:

- l'aspetto strettamente tecnico;
- l'aspetto di politica legislativa;
- l'aspetto dei rimedi alternativi, ossia la possibilità che la censura possa essere sostituita da altre azioni meno liberticide e più rispettose dell'ecosistema digitale.

Non è semplice far comprendere al mondo politico come oggi non sia possibile pensare, concretamente, a un sistema tecnologico efficace di censura dei contenuti

in Rete; e come ciò sia dovuto, essenzialmente, all'architettura della Rete stessa, che è rimasta semplice, non molto diversa da quella degli anni Sessanta e dei progetti originari e, per tale motivo, molto poco controllabile. Il cercare di censurare informazioni in una Rete nata appositamente per sventare alcune minacce, tra cui quelle di un attacco/controllo centralizzato e di azioni di censura, è un'impresa assai difficile. Ciò è dimostrato anche dal fatto che, nella storia recente, la censura tecnologica ha riguardato singoli Stati, per periodi limitati, e immediatamente in quegli Stati si è creato un movimento di dissidenti che ha utilizzato le tecnologie – spesso le più semplici – per aggirare blocchi e filtri, singoli provider di Stato o siti web ufficiali e ristabilire una «libertà di navigazione». Di lì a pensare che sia possibile bloccare la circolazione delle informazioni a livello mondiale, in un contesto tecnologicamente avanzato e democratico, è un passaggio molto arduo. Negli ultimi anni, al contempo, la diffusione, anche tra gli utenti comuni e meno competenti, di software per l'anonimizzazione quali Tor e di VPN, ossia programmi pensati appositamente per creare canali cifrati in uscita capaci di aggirare anche blocchi tecnologici di Stato, ha reso estremamente semplice il superamento tecnico di ogni tentativo di blocco o di censura.

Un primo punto che l'interprete dovrebbe quindi riconoscere senza riserve è il fatto che, allo stato tecnologico attuale, il cercare di predisporre strumenti tecnici di censura e di controllo di circolazione delle informazioni in Stati dove non ci sia un unico provider di Stato o un controllo governativo diretto di tutti i mezzi di comunicazione si presenta come una soluzione impraticabile o, se anche fosse praticabile, facilmente aggirabile.

Se, allora, la censura non è un rimedio implementabile tecnicamente, se non si può prevedere, per dirla alla Trump, un «interruttore da premere che spenga Internet» o che cancelli i dati non voluti, se il mezzo non consente modalità profonde di intervento selettivo dei contenuti, come potrebbe procedere il legislatore per cercare di controllare comunque le informazioni?

La prassi rischia di diventare, e in molti casi è già diventata, quella di individuare i soggetti più visibili – e solvibili economicamente – per poi caricarli di responsabilità censorie. Ciò significa, in pratica, che si cerca di costringere per legge i gestori di piccole e grandi piattaforme, siti web, blog e sistemi di messaggistica e chat non solo a intervenire in tempo quasi reale in caso di segnalazioni – noncuranti delle dimensioni che oggi assumono alcune aziende e del numero di reclami che ricevono a ogni ora – ma, anche,

ad agire in via preventiva, ricercando e controllando i contenuti illeciti che circolano e assumendo il ruolo, per così dire, di «sceriffi» del web.

La censura basata su un'eccessiva responsabilizzazione dei provider e sull'individuazione di una responsabilità che sfiori quella oggettiva entra, però, in aperto conflitto con due principi molto chiari ma, ancora, non sufficientemente compresi nella loro importanza: **il principio di neutralità dei provider**, consolidato nel quadro giuridico europeo sin dagli anni Duemila con la Direttiva n. 31 del 2000 sul commercio elettronico in Europa, **e la non sostenibilità economica di un sistema evoluto di controllo** in contesti che hanno ormai un'estensione senza confini e un numero di utenti elevatissimo.

Il primo tema, il principio di neutralità, non è scolpito sulla pietra, è vero, e molti ne domandano una revisione; ma è chiaro in ciò che dispone e, soprattutto, al momento è ancora in vigore in Europa.

> Il fornitore di servizi di connessione, di comunicazione e di spazi nella società dell'informazione non deve essere considerato responsabile per i contenuti che circolano sui suoi sistemi, a meno che non ometta di attivarsi in tempi ragionevolmente utili a seguito di una segnalazione qualificata di contenuti illeciti da parte dell'autorità.

Un principio di questo tipo – che è stato pensato per provider operanti in un quadro diverso da quello attuale e per fornitori di servizi che erano meno evoluti e con meno potere, dal momento che oggi molti sono in grado di intervenire sui contenuti e prendono sempre di più la forma di *media companies* – è sempre stato considerato un buon compromesso tra reazione al danno e sostenibilità di simili attività commerciali. Il principio è ancora in vigore, anche se forti venti di cambiamento stanno cercando di smussarlo. La sentenza «Google Spain» della Corte di Giustizia dell'Unione europea del 13 maggio 2014, che ha dato vita a un **«diritto all'oblio» e all'obbligo per i provider di rimuovere contenuti in base a determinati parametri**, è stata in tal senso rivoluzionaria, e ha generato un *vulnus* preoccupante. Il secondo argomento di buon senso, si diceva, è quello secondo il quale il costringere una piattaforma ad allestire un «esercito» di dipendenti che analizzino ogni singola richiesta di rimozione dei contenuti, o il prevedere sanzioni elevatissime ed esemplari in caso di omesso controllo, rischia seriamente di condizionare l'ecosistema digitale e di far cessare le attività dell'azienda stessa.

Il conflitto tra provider e mondo della politica è apparso particolarmente evidente in quattro Stati: Francia, Germania, Brasile e Italia.

In Francia il contrasto è nato nel 2000 a causa della presenza di cimeli neonazisti sulla piattaforma di Yahoo! accessibili agli utenti francesi, con la condanna del provider a un'ammenda per ogni giorno di permanenza di tali memorabilia sui server. In Germania, nel 1998, Felix Somm, un dirigente del provider Compuserve, è stato condannato a due anni di reclusione e al pagamento di 100 milioni di euro di ammenda per la presenza sui server del provider d'immagini pedopornografiche. Somm, in quanto direttore del servizio, è stato considerato complice. È stato poi assolto in secondo grado, ma il segnale è stato chiaro.

Anche di recente, in Germania, sono stati resi pubblici «accordi» tra il governo e Facebook per aumentare le reazioni e i controlli nei confronti dei contenuti di odio, soprattutto di stampo neonazista, e di notizie false ed estremismi in vista delle imminenti elezioni. Questi accordi sono stati conclusi sulla base della prospettazione di arresti dei dirigenti del provider e di sanzioni elevatissime: un'azione di *moral suasion* molto particolare.

In Brasile il bersaglio è stato WhatsApp: il servizio è stato bloccato per 72 ore nel maggio del 2016 su richiesta di un giudice, che ha disposto multe di 150.000 dollari giornalieri a carico delle compagnie telefoniche in caso di mancato adempimento dell'ordine. Al centro dell'indagine c'era il traffico di droga, e lo stesso magistrato aveva fatto arrestare, nel marzo precedente, il vicepresidente di Facebook per l'America Latina: non voleva consegnare messaggi WhatsApp sempre collegati a un'indagine sul narcotraffico.

In Italia, in più occasioni, la commissione di studio parlamentare sull'intolleranza, la xenofobia, il razzismo e i fenomeni di odio, istituita dalla presidente della Camera Laura Boldrini nel maggio del 2016, ha lamentato un palese disinteresse di Facebook in tal senso, domandando una maggior attenzione e presenza anche in Italia, dove ci sono ormai oltre 26 milioni di utenti, per le espressioni d'odio che circolano. Il momento di rottura è avvenuto con una lettera pubblica inviata da Laura Boldrini a Mark Zuckerberg il 13 febbraio 2017 e pubblicata su tutti i quotidiani. I toni ci sembra siano chiari.

Si legga questo passaggio:

> Questo dev'essere quindi per tutti il tempo della responsabilità: tanto maggiore quanto più grande è il potere di cui si dispone. E il suo è notevole. [...] Risulta cancellato appena il 28% dei contenuti segnalati come discriminatori o razzisti. Una media che si ricava dal 50% di Germania e Francia e dal misero 4% italiano. Mi domando se questo dato allarmante lo dobbiamo anche all'assenza di un ufficio operativo di Facebook in Italia. Un'Italia che sconta scarsa collaborazione da parte della sua azienda anche sul fronte della disinformazione, al contrario di quanto avviene in Germania o in Francia [...] Le risposte giunte dopo due mesi sono evasive e generiche.

Si noti, tra gli altri aspetti, il riferimento alla richiesta di un centro d'imputabilità aziendale (un ufficio operativo) in Italia, oltre a una chiara accusa di connivenza, neppure troppo velata, nella circolazione delle espressioni d'odio.

È un esempio chiaro d'individuazione del problema unicamente in capo al provider, ossia a chi fa circolare le informazioni; si tratta di un approccio non solo miope ma, anche, molto pericoloso in un'ottica di conseguenti politiche legislative.

Un simile approccio tecnico errato ha, infatti, come immediata conseguenza leggi che mireranno, da un lato, a criminalizzare la tecnologia, ossia a inquadrare il mezzo tecnologico quale il primo fattore che genera odio, bufale o rende più gravi i reati e che, dall'altro, cercheranno di gestire i problemi di attualità cui si faceva cenno poco sopra – il cyberbullismo, le fake news – con un approccio improvvisato e quasi sempre liberticida. Nel recentissimo **panorama legislativo italiano**, le proposte di legge sul cyberbullismo (proponente Elena Ferrara, approvata in Senato il 6 febbraio 2017 e tornata alla Camera per emendamenti) e sulle cosiddette «fake news» (prima firmataria Adele Gambaro, presentata in Senato il 15 febbraio 2017) hanno entrambe manifestato nuovamente chiare intenzioni di censura e l'evidente proposito di porre al centro dell'apparato sanzionatorio il provider, tralasciando, invece, gli aspetti culturali e sociali dei problemi. I due progetti di legge subiranno, nei prossimi mesi, numerose modifiche, quindi non è utile esaminare i punti in dettaglio. Per di più, la normativa sul cyberbullismo è stata notevolmente smussata, nel suo approccio censorio e sanzionatorio, durante i vari passaggi. Più interessanti sono, a nostro avviso, le disposizioni del recente disegno di legge Gambaro («Disposizioni per prevenire la manipolazione dell'informazione online, garantire la trasparenza sul web e incentivare l'alfabetizzazione mediatica»). Proprio quest'ultimo ha alcuni punti che rendono chiaro un simile approccio. Si veda, ad esempio, questo passaggio contenuto nella relazione introduttiva al disegno di legge:

> La reazione di Francia e Germania è stata quasi immediata: [...] è emersa l'esigenza di intervenire sotto il profilo normativo per ottemperare alla duplice necessità di effettuare un costante monitoraggio dei contenuti presenti in Rete, per poi procedere alla rimozione di quelli considerati falsi. [...] Bisogna avviare un simile percorso anche in Italia attingendo agli strumenti che già ci sono: le leggi contro le informazioni false, illegali e lesive della dignità personale [ripensandole] per il web. Ciò consentirebbe ai colossi della Rete l'uso di selettori software per rimuovere i contenuti falsi, pedopornografici o violenti. Il tutto ridiscutendo i tabù

> dell'anonimato, della trasparenza e della proprietà dei media online, del diritto di replica, di rettifica, del diritto all'oblio, della protezione della privacy e della rimozione dal web dei contenuti lesivi. [...] Si prevede, in particolare, che i gestori dei siti siano tenuti a effettuare un costante monitoraggio di quanto diffuso sulle proprie piattaforme web, compresi i commenti degli utenti, con particolare riguardo a frasi offensive e a informazioni verso le quali viene manifestata un'attenzione diffusa e improvvisa, per valutarne l'attendibilità e la veridicità. Quando i gestori rintracciano simili anomalie o ricevono segnalazioni in questo senso sono tenuti alla rimozione di tali contenuti dalla piattaforma e se non procedono c'è una sanzione penale con ammenda fino a 5.000 euro.

Sono disegni di legge che s'inseriscono perfettamente nel solco di una normativa italiana che, sin dal 1992, quando per la prima volta si occupò di tecnologie, ha avuto un approccio liberticida. La tecnologia è sempre stata vista, dal nostro legislatore, come una minaccia, e anche la disciplina di legge ha seguito quella linea. Sono, quindi, utilizzati anche in questo caso termini come *controllo, responsabilità, monitoraggio e sanzioni*, che rendono ben evidente l'approccio.
In realtà, l'azione del legislatore dovrebbe essere ben modulata, in questo ambito, con processi di educazione e con l'uso avanzato delle tecnologie per risolvere il problema dall'interno delle piattaforme. Affidare unicamente a una legislazione repressiva il controllo dei contenuti d'odio in Rete non è efficace – la tecnologia è in grado di aggirare le disposizioni delle norme – né consigliabile, dal momento che rischia di mettere in pericolo specifici diritti di libertà. *In primis* la libertà di manifestazione del pensiero.

Il quadro attuale nel quale l'interprete e il legislatore si devono muovere, con riferimento alle espressioni d'odio, si fonda su quattro aspetti essenziali:

- l'amplificazione del messaggio;
- la persistenza delle informazioni;
- un alto livello di tolleranza/mancanza di percezione delle azioni tra gli utenti online;
- una sorta di «istituzionalizzazione» diffusa dell'odio.

Per amplificazione s'intende l'incredibile capacità che hanno le tecnologie oggi di amplificare i messaggi d'odio e, quindi, di generare maggior danno. Per persistenza s'intende l'impossibilità concreta di una cancellazione delle informazioni che iniziano a circolare, e la conseguente inapplicabilità di un diritto all'oblio. Il livello alto di tolleranza, unito a un *disinhibition effect*, rende poi normali e asettiche le manifestazioni d'odio (tanto che gran parte degli *haters* declinano ormai senza problemi nome e cognome reali) e fa sì che, davanti a uno schermo, si tengano sovente comportamenti più violenti rispetto a quelli che si terrebbero di persona.

Infine, per istituzionalizzazione dell'odio s'intende il fatto che i due soggetti che più dovrebbero fornire il buon esempio, ossia i media e la politica, hanno da tempo scoperto che l'odio genera consenso (e copie vendute o click pubblicitari) e, quindi, sono i primi a veicolarlo, soprattutto sul web e sui social network.
Questi quattro punti critici non disegnano un quadro facile da gestire dal punto di vista legislativo, e la tentazione di ricorrere alla sanzione penale nei confronti dei soggetti più visibili è, si diceva, sempre più diffusa in tutto il mondo. In realtà, la criminalizzazione ex se del mezzo tecnologico, l'uso dell'odio contro l'odio (come può essere, ad esempio, la gogna mediatica o il *blastare* pubblicamente gli *haters*, oggi fenomeno molto di moda), la colpevolizzazione dei soggetti più visibili e il richiamo alla censura e al controllo dei contenuti si stanno rivelando tutti approcci errati e inutili.
L'azione di contrasto dovrebbe essere portata contemporaneamente in tre ambiti, dosando con cura, a seconda del contesto e dei fatti, i seguenti rimedi:

- la cultura/ educazione civica digitale/controparola;
- un uso ragionato del diritto;
- un uso avanzato – si potrebbe dire «intelligente» – delle tecnologie per arginare i fenomeni d'odio dall'interno.

Nel primo rimedio rientrano tutte quelle azioni volte a evidenziare la necessità della conoscenza profonda del mezzo elettronico, della comprensione e della diffusione di una cultura tradizionale e non solo digitale, dell'uso dell'esempio come strumento da fornire soprattutto ai più giovani che usano le tecnologie e che si avvicinano al mondo online. Al contempo, cultura vuol dire anche controparola, dialogo pacato, isolamento dei comportamenti più gravi, creazione di reti spontanee, dal basso, per contrastare l'odio (nell'ambito del cyberbullismo hanno dato ottima prova) e, in generale, il cercare di abbassare i toni con modi di dialogare meno accesi e più mirati a questo scopo.
Il secondo rimedio riguarda l'uso «calibrato» del diritto, soprattutto se si è in presenza di reati di opinione che sono soliti generare un rapporto delicatissimo con la libertà di manifestazione del pensiero. Non si afferma in questa sede, sia chiaro, che il diritto non debba intervenire in tale ambito. È però indispensabile che ogni intervento giuridico presti attenzione al possibile condizionamento dell'ecosistema digitale, eviti aggravanti inutili solo per il fatto che è presente la tecnologia e non utilizzi la sanzione penale a fini esemplari.
Nel terzo rimedio ricadono quegli usi della tecnologia che, tramite algoritmi e analisi semantica delle espressioni, uso dei sistemi di profilazione e studio dei comportamenti a fini di prevenzione e reazione alle parole veicolate dalla Rete, possono combattere dall'interno l'odio e la circolazione di manifestazioni estreme. Ciò comporta, ovviamente, una stretta collaborazione tra utenti e piattaforma e tra le varie piattaforme, con un ripensamento delle policy e delle regole d'intervento e con un'attenzione, anche in questo

caso, ai rischi di censura automatizzata o di canalizzazione di un pensiero unico o di poche, selezionate informazioni.
In un quadro del genere, dove l'approccio censorio non solo non è attuabile ma è in grado di danneggiare profondamente gli aspetti più belli dell'ambiente digitale che si è creato – soprattutto un dialogo ininterrotto che lascia ampia libertà anche al dissenso –, un dosaggio accurato dei tre rimedi poco sopra accennati e un'attenzione costante al lato tecnologico, al Dna della Rete, permetterebbe il raggiungimento di risultati molto più benefici senza intaccare i diritti di libertà dell'individuo. Un approccio modulare, da ultimo ma non ultimo, permette anche di adattare le strategie d'intervento alle rapidissime modifiche che sono tipiche dell'ambiente tecnologico moderno, assai sensibile, nelle sue reazioni, ai mutamenti sociali, economici e giuridici.