



LA DISINFORMAZIONE ONLINE
24 APRILE 2020

Fake news, guerra dell'informazione ed equilibri democratici

di Gabriele Suffia

Assegnista di Ricerca in Informatica Giuridica
Università degli Studi di Milano

e Giovanni Ziccardi

Professore associato di Informatica Giuridica
Università degli Studi di Milano

Fake news, guerra dell'informazione ed equilibri democratici *

di Gabriele Suffia

Assegnista di Ricerca in Informatica Giuridica
Università degli Studi di Milano

e Giovanni Ziccardi

Professore associato di Informatica Giuridica
Università degli Studi di Milano

Abstract [It]: Il contributo analizza l'evoluzione della disinformazione online in un'ottica multidisciplinare: quale strumento di azione di alcuni attori geopolitici ma anche quale fenomeno connotato da diversi elementi, fra cui quelli psicologici. Se nella prima parte del contributo si esplorano le fake news nel quadro dell'informazione, dei social network e del diritto, nella seconda si dà conto di come le fake news circolino e di come esse si inseriscano in un ambito più ampio di propaganda e profilazione dell'utente. Nelle conclusioni gli autori individuano dieci rischi per la democrazia nella dimensione tecnologica dei social networks, auspicando che lo studioso che si voglia occupare di questi temi adotti una prospettiva multidisciplinare e interdisciplinare.

Abstract [En]: The paper aims at analysing the evolution of online disinformation from a multidisciplinary perspective, considering it as an action tool of some geopolitical actors but also as a phenomenon characterized by several aspects, including psychological ones. The first part of the paper looks at fake news in the contexts of information, social networks and law. The second part of the contribution focuses on how fake news are disseminated and how they are linked to other Internet phenomena, such as political propaganda and user profiling. In the final remarks, the authors identify ten risks for democracy in the new technological dimension of social networks, suggesting that the scholar who intends to deal with these issues should adopt a multidisciplinary and interdisciplinary perspective.

Sommario: **Parte I** – L'evoluzione delle *fake news* nella società digitale. **1.** La *fake news* nel quadro dell'informazione. **2.** Esempi di disinformazione e casi di studio. **3.** Disinformazione e *social network*. **4.** Disinformazione e diritto. **Parte II** – Disinformazione, *social network* e propaganda politica. **5.** Alcune considerazioni pratiche. **6.** Gli aspetti informatico-giuridici. **7.** I meccanismi di funzionamento delle *fake news*. **8.** La connessione tra *fake news*, psicologia e test di personalità. **9.** Ulteriori fattori critici. **10.** Le regole delle piattaforme. **11.** Il delicato rapporto tra *fake news*, politica ed equilibri democratici. **12.** *Fictio*, propaganda e profilazione estrema dell'utente. **13.** Alcune conclusioni: un'alterazione degli equilibri democratici?

Parte I – L'evoluzione delle *fake news* nella società digitale

1. La *fake news* nel quadro dell'informazione

Nel corso degli ultimi anni la comunità scientifica ha iniziato a interrogarsi su quello che viene definito, comunemente, come il fenomeno della “disinformazione”, e che viene ricompreso, dagli studiosi più attenti, all'interno del più ampio tema, in generale, della cosiddetta “guerra dell'informazione”.

La locuzione “guerra dell'informazione” è solita indicare, nella dottrina prevalente, aspetti molto diversi tra loro: può evidenziare, *in primis*, una metodologia di interferenza posta in essere da alcuni Stati nei confronti di altri, con modalità specifiche e originali che vengono attuate da singoli settori o apparati dello

* Articolo sottoposto a referaggio. La Parte I è stata redatta da Gabriele Suffia; la Parte II è stata redatta da Giovanni Ziccardi.

Stato. Può, al contempo, sottolineare la condizione generale di un sistema-Paese all'esito di queste interferenze e assumere, quindi, un significato molto simile a concetti quali sotto-educazione, diseducazione o sotto-sviluppo. In questo quadro, le *fake news* sono solamente uno strumento, tra i tanti, che può essere utilizzato per esercitare questa interferenza o per generare questa condizione.

Per inquadrare correttamente il problema occorre, fin da subito, precisare che non tutte le *fake news* sono parte di una campagna di disinformazione.

Anche notizie imprecise, incomplete, smentite successivamente, ove continuassero a circolare in rete o sui *social network*, potrebbero diventare vere e proprie *fake news* e influire sulla percezione da parte di un gruppo o di una totalità di persone. Non per questo, però, andrebbero definite come “disinformazione”. Per questo tipo di notizie si suggerisce sovente il termine, utilizzato in dottrina, di “misinformazione”, o disinformazione accidentale¹.

Si può parlare di disinformazione, invece, nel momento in cui più dati, lanci di agenzia e notizie, anche apparentemente riferibili a temi distanti tra loro, possono essere correlati all'interno di un unico disegno coordinato e assumere la veste di vere e proprie operazioni disinformative.

Per questo motivo possiamo parlare della disinformazione non come una condizione, ma come uno strumento utilizzato per ottenere risultati, facendone derivare il termine dalla “dezinformatzija” sovietica². Una definizione suggestiva, nel suo estremo minimalismo, può essere quindi la seguente: «la manipolazione del sistema di intelligence di una nazione attraverso la somministrazione di dati credibili ma fuorvianti»³.

Un'altra possibile definizione potrebbe evidenziare, invece, la falsificazione intenzionale di dati e notizie al fine di manipolare le percezioni del bersaglio, influenzare le decisioni e indurlo ad agire nel modo desiderato dal disinformatore. Talvolta, anche per indebolire le capacità cognitive e decisionali del *target*, ciò avviene diffondendo notizie che generano in esso confusione e incertezza.

La riflessione sulla disinformazione non origina propriamente dal mondo occidentale ma si presenta, oggi, come una risposta alle iniziative e alle dottrine operative poste in essere da parte di altri attori del panorama geopolitico.

In particolare, ci si riferisce, come prevedibile, alla Russia che, dal 2013, ha abbracciato una serie di principi della guerra asimmetrica, e della guerra evoluta nelle sue forme del XXI secolo, genericamente riassunti nella formula “dottrina Gerasimov”. È curioso, tuttavia, notare come il Generale Valeriy Gerasimov, all'epoca Capo di Stato Maggiore russo, nell'espore la propria visione delle trasformazioni

¹ Su cui si veda in questo numero speciale M. CAVINO, *Il triceratopo di Spielberg. Fake news, diritto e politica*, in questo fascicolo.

² Cfr. F. RUGGE, “*Mind backing*”: la guerra informativa nell'era cyber, in *Notizie di Politeia*, n. 132/2018.

³ Come riportata in W. SAFIRE, *Quoth the Maven*, New York, 1993 (traduzione degli autori).

della guerra ne attribuisse la responsabilità alle campagne non-convenzionali condotte dall'Occidente e finalizzate a orientare e manipolare i media nei Paesi in cui erano scoppiate le cosiddette “Primavere arabe”. Alludendo alle responsabilità di americani ed europei, infatti, auspicava che anche la Russia si evolvesse verso una simile metodologia di conduzione di una sorta di guerra non-guerreggiata.

In realtà, quale che sia la ricostruzione proposta, e che rientra in un più ampio gioco di posizionamenti internazionale, lo spionaggio e la raccolta di informazioni non sono attività nuove nella storia del mondo. L'uso di queste informazioni per operazioni di *deception*, ovvero di “inganno” ai danni di un bersaglio precedentemente individuato, registra però una decisa evoluzione a partire dalla Seconda Guerra Mondiale e, poi, durante la Guerra Fredda.

Con l'accresciuta centralità di questo strumento, compaiono i primi studi volti ad analizzare le casistiche riscontrate e a proporre inquadramenti giuridici e risposte. Dalla *deception* militare si distacca, quindi, una branca, sempre più rilevante, volta a studiare la *deception* politica diretta a ingannare gruppi di cittadini-elettori o intere società. Il contesto internazionale del “dopo Guerra Fredda” presenta alcuni aspetti tali per cui la disinformazione “diffusa” diviene possibile e, anzi, trova un terreno molto fertile su cui innestarsi. Ci riferiamo, in particolare, ai seguenti aspetti:

i) l'avanzamento tecnologico originato dall'informatica, che porta il mondo in una nuova fase (quella definita dell'Industria 4.0) in cui, alla centralità dell'informazione (vedasi, per tutti, il concetto di infosfera⁴), si accompagna una automazione crescente in tutti gli ambiti della vita umana, unita alla presenza di una quantità di dati non più analizzabile dagli esseri umani senza l'ausilio di macchine (*big data*);

ii) la compresenza di Stati, ugualmente legittimati nella comunità internazionale, che adottano regimi illiberali, democrazie “illiberali” e democrazie mature porta a inevitabili discrasie. Per i regimi e le democrazie illiberali (così definite le società formalmente democratiche, ma in cui, ad esempio, la *leadership* è affidata a una figura carismatica e si perpetua immutata per anni, anche eventualmente per successive tornate elettorali), vi è la possibilità di impegnarsi in campagne di influenza e disinformazione sul lungo periodo, ai danni delle democrazie evolute, vincolate ai tempi corti della democrazia.

Alcuni studiosi, da ultimo, si interrogano sulla possibilità che la società attuale sia in una condizione di vero e proprio cambio di paradigma⁵, con le incertezze che ciò comporta.

È dibattuto se, dopo il crollo del mondo bipolare, ci si trovi in un mondo unipolare o multipolare.

Ciò che qui interessa, tuttavia, è proprio il fatto che non si ha una chiara e precisa cognizione dell'ordine globale in cui ci si trova dopo il 1989 e quali siano i concreti rapporti di forza.

⁴ Cfr. L. FLORIDI, *La quarta rivoluzione, Come l'infosfera sta trasformando il mondo*, Milano, 2017.

⁵ Cfr. L. BONANATE, *Anarchia o democrazia. La teoria politica internazionale del XXI secolo*, Roma, 2015.

Questa condizione è, senz'altro, facilitatrice della disinformazione, dal momento che non è più necessario superare grandi ideologie (ad esempio con complesse operazioni di propaganda) ma è sufficiente porre in essere piccole operazioni di influenza per ottenere grandi risultati, essendo la capacità di attrazione e riferimento degli Stati molto più labile anche nei confronti dei propri cittadini.

Non stupisce che sia proprio l'Europa, con la sua struttura ancora in costruzione di libera associazione di piccoli Stati (le cosiddette "Alte parti contraenti" dei Trattati europei), uno dei bersagli principali della disinformazione se non, proprio, la frontiera attorno a cui ci si combatte con questo nuovo tipo di conflittualità ibrida caratterizzata da:

- i) una combinazione di azioni convenzionali e non-convenzionali, militari e non-militari, palesi e occulte;
- ii) il fine di creare ambiguità e confusione circa la natura, l'origine (*attribution*) e l'obiettivo della minaccia;
- iii) la necessità, per arrecare danni, di indagare, individuare e sfruttare le vulnerabilità dell'avversario;
- iv) il generale mantenimento del livello di ostilità al di sotto della soglia della guerra convenzionale.

2. Esempi di disinformazione e casi di studio

A far data dal biennio 2014-2016 si è assistito a un momento di svolta per la disinformazione: il termine *fake news* ha cominciato a circolare nell'opinione pubblica, venendo proposto in primo luogo dal neo-eletto Presidente degli Stati Uniti d'America Donald Trump.

I casi di studio più citati del periodo sono, da una parte, legati alla campagna disinformativa volta a influenzare le elezioni negli Stati Uniti d'America del 2016 e, dall'altra, connessi alle vicende della Guerra in Ucraina orientale.

Nel primo caso, sono diventate celebri le *fake news* che puntavano a deviare o distrarre il voto degli elettori democratici portandoli a dubitare dell'opportunità di sostenere la candidata Hillary Clinton (sostenendo, ad esempio, che avesse una salute precaria e gravi patologie non dichiarate pubblicamente) o, direttamente, a non recarsi neppure a votare (ad esempio millantando, tramite l'attività informativa correlata ad account falsi, una vittoria già ottenuta, e ringraziando per il contributo).

Parallelamente, si puntava a richiamare al voto gli elettori repubblicani, con *fake news* legate in larga misura alla linea che il futuro presidente degli Stati Uniti d'America avrebbe adottato, a differenza di altri candidati.

In entrambi i casi, sia che il bersaglio fossero gli elettori democratici, sia che fossero gli elettori repubblicani, le *fake news* circolavano nella stampa alternativa, o locale, e venivano poi riprese dalla stampa nazionale più schierata e dai mass media, in ragione della loro viralità e dell'interesse che suscitavano. Oppure, parallelamente, venivano proposte come contenuti sponsorizzati all'interno dei social network, con l'aspetto di ordinari *post* generati dagli utenti.

In tutti questi casi, la distribuzione delle *fake news* era favorita dalla preliminare profilazione delle preferenze e delle scelte di migliaia di utenti, come emerso dallo scandalo correlato a *Cambridge Analytica*. Potendo utilizzare questa immensa mole di dati, in modo automatizzato, si riusciva, quindi, a veicolare le *fake news* all'elettorato selezionato, che gli autori sapevano sarebbe stato più incline ad accettare i contenuti come veri e a farne uso (condividendoli nelle reti sociali e orientando le proprie scelte di voto). La possibilità di raggiungere capillarmente tutti gli utenti-bersaglio era poi resa possibile, per la prima volta nella storia, dall'utilizzo di sistemi automatizzati (*bot*).

Dall'esempio citato emerge chiaramente come una efficace campagna di disinformazione miri a influenzare gruppi ben determinati di persone, individuati come bersagli, e non sia diretta, invece, alla totalità degli utenti di un servizio o alla totalità dei cittadini di un Paese.

L'indirizzo di *fake news* a un pubblico generalista potrebbe perfino rivelarsi una mossa azzardata, che potrebbe più facilmente portare a campagne di reazione, di *debunking* e a smascherare l'operazione di disinformazione⁶.

Il secondo esempio citato di utilizzo delle *fake news* e della disinformazione è, invece, relativo al conflitto Russia-Ucraina scoppiato in Europa a partire dal 2014.

In questo caso, la disinformazione si presenta come principalmente proveniente dalla Russia con la finalità di confondere le opinioni pubbliche occidentali sulla reale situazione nel Paese, sulla reale attribuzione delle azioni nel Donbass e in Crimea e, più in generale, con l'intento di rafforzare l'immagine della Russia come potenza internazionale.

L'incertezza internazionale sullo status del Mare di Azov, unita alla marginalità, per gran parte degli europei, dell'Ucraina orientale, non ha fatto altro che favorire il proliferare di notizie false, o parzialmente vere, utilizzate da entrambe le parti per delegittimare l'avversario nel dibattito internazionale.

L'esempio è citato perché, pur presentando tutte le caratteristiche della disinformazione già esposte in precedenza, consente di sottolineare come la distanza geografica e la mancanza di una conoscenza diretta delle fonti siano due delle caratteristiche imprescindibili della disinformazione, nonché due delle ragioni più comuni che consentono alle *fake news* di trovare un fortissimo sostegno nell'immediato.

La notizia che non sia immediatamente, e facilmente, verificabile e confutabile, infatti, ha una maggiore possibilità di essere assunta come vera e di generare un'opinione radicata, eventualmente resistendo anche a un successivo *debunking* (che diventerebbe costoso e non in grado di ricevere lo stesso numero di visualizzazioni della notizia che pretenderebbe di confutare).

⁶ Sull'efficacia del *debunking* e del *fact-checking* si veda: G. RUFFO – M. TAMBUSCIO, *Capire la diffusione della disinformazione e come contrastarla*, in questo fascicolo.

Ulteriormente, tali caratteristiche pongono in luce chiaramente come la disinformazione possa avvalersi sia di notizie completamente false (che alcuni paragonano a una sorta di “diffamazione” su larga scala), sia di notizie parzialmente vere, ma presentate in modo volutamente incompleto o tendenzioso.

La campagna di disinformazione russa si estenderebbe, inoltre, anche a tutto il continente europeo con la finalità di creare un’opinione pubblica favorevole all’eliminazione delle sanzioni poste in essere dopo l’annessione della Crimea; incline a vedere nella figura del Presidente russo Vladimir Putin un uomo forte in grado di risolvere le controversie internazionali, e fare affidamento sulla sua leadership; avversa al processo d’integrazione europea e incline a mantenere, per i più disparati motivi, la situazione di attuale frammentazione degli Stati europei con il risultato, per la Russia, di poter continuare a trattare con essi in una posizione di parità o, addirittura, di forza.

3. Disinformazione e *social network*

Per comprendere come la disinformazione possa trovare nei *social network* uno dei principali veicoli, occorre considerare la capacità di diffusione di un messaggio al loro interno, dal singolo utente a cerchi sempre più larghi di amici, conoscenti e perfetti sconosciuti.

La capillarità dei *social network* viene generalmente spiegata facendo riferimento alla Legge di Reed⁷.

Le reti hanno specifiche capacità di potenza, ma è con l’avvento di Internet che è stato possibile raggiungere un numero di utenti pari a $n^2 - n$, dove n sta a indicare il numero degli utenti. Ciò è quanto avviene, ad esempio, con riferimento alle comunicazioni via e-mail (legge di Metcalfe). Con i social network, parte della dottrina ritiene invece valida la cosiddetta legge di Reed, tale per cui il valore delle reti è pari a 2^n . Si tratta, come evidente, di una moltiplicazione esponenziale delle potenzialità di comunicazione: ciò è di assoluta rilevanza per parlare di informazione, e disinformazione, nel mondo contemporaneo integrato con il digitale.

La disinformazione e le *fake news* non sono, quindi, elementi del tutto innovativi della nostra epoca, ma si avvalgono del digitale per diventare ancora più virali.

La stessa Internet è cambiata molto nel tempo passando da un Internet con contenuti creati soltanto dalle istituzioni, dagli uffici stampa delle aziende e dalle prime testate giornalistiche online, a uno spazio che fa dell’interazione degli utenti la principale fonte di creazione dei dati e delle notizie.

Sono immediatamente evidenti, in particolare, alcuni problemi:

⁷ Cfr. D.P. REED, *The Law of the Pack*, in *Harvard Business Review*, n. 79/2001.

- i) la quantità di notizie è esponenzialmente superiore a qualsiasi altro periodo storico del passato. Siamo in presenza di un evidente *overloading* informativo, tale per cui abbiamo troppe informazioni e non siamo in grado di analizzarle senza l'ausilio di computer;
- ii) l'autorevolezza di chi crea notizie oggi è difficilmente verificabile, dal momento che tutti, teoricamente, sono in grado di creare notizie degne della pubblica attenzione;
- iii) la veridicità delle notizie così create è di difficile verifica, specialmente prima della loro diffusione/viralizzazione (che può essere estremamente rapida).

4. Disinformazione e diritto

Ancora controversa è la possibilità di definire profili di responsabilità per quanto riguarda la disinformazione, dal momento che le diverse normative, anche se in alcuni punti si sovrappongono tra loro, lasciano ampi margini di incertezza e imprecisione, specialmente riguardo la loro applicazione.

Il problema interessa il mondo del diritto su due fronti: sia il fronte del diritto interno degli Stati, sia il fronte internazionale.

Sul fronte interno, l'utilizzo di *fake news* e di campagne di disinformazione è ancora poco studiato, dal momento che la fattispecie mal si presta a essere ricostruita con precisione. Bisognerebbe, invero, ipotizzare che apparati dello Stato mettano in atto misure volte a disorientare e trarre in inganno altre parti dello stesso, fornendo dati falsi, incompleti o "diffamatori". Ove ciò avvenisse, la fattispecie potrebbe comunque essere ricondotta all'interno dei reati contro la fede pubblica e contro lo Stato.

Sul fronte internazionale, invece, vi è una maggior facilità di individuazione di fenomeni riconducibili alla fattispecie della disinformazione, come negli esempi citati, pur mancando unanimità di vedute sulla possibilità di riposta a questi fenomeni.

Uno degli esempi più rilevanti è dato dalla cosiddetta "fabbrica dei troll", ossia l'*Internet Research Agency* di San Pietroburgo, che è stata accusata di essere alla base delle *fake news* provenienti dalla Russia e dirette contro Stati Uniti d'America e Europa.

Tale agenzia è ricordata, per quanto qui interessa, anche per essere stata "silenziata" in occasione delle elezioni statunitensi di medio-mandato dell'autunno 2018 al fine, proprio, di prevenire interferenze.

In punto di diritto, sia l'operato russo, sia la reazione americana, potrebbero essere configurate come "interferenze" negli affari interni di un altro Stato, così come molte delle campagne disinformative cui abbiamo assistito nel recente passato.

Secondo la dottrina più autorevole, la criticità, a questo punto, non starebbe tanto nell'identificazione della fattispecie, quanto nella definizione dei limiti della risposta e della reazione.

Ciò è reso arduo dalla natura stessa del mondo dell'informazione digitale, così come dall'assenza di un generale consenso intorno alla configurabilità dei dati (e, quindi, delle informazioni) come oggetti di tutela giuridica, o attorno all'uso della forza nel ciber spazio.

A riguardo, la disinformazione viene generalmente ricondotta all'interno delle cosiddette "minacce ibride" che, per loro natura, si avvalgono di elementi leciti utilizzati malevolmente, così come esplorano sovente "zone di grigio" in cui i confini sono labili e poco precisi.

Se, da una parte, la disinformazione è di controversa qualificazione giuridica, non sono nascosti gli effetti che essa produce, o mira a produrre.

L'impovertimento del dialogo e del dibattito pubblico ha effetti diretti sulla qualità della vita democratica dei Paesi occidentali e, sul lungo periodo, può portare a esiti che si stanno ancora studiando.

La crescente polarizzazione dell'elettorato ha comportato il generale declino dei partiti tradizionali in Europa, o la loro radicale riforma, unito all'emersione di forze nuove anche radicali ed extra-sistemiche (come i "gilet gialli" in Francia) che stanno sollecitando dalla radice le categorie, anche giuridiche, dello Stato di diritto occidentale.

Non si tratta di esperienze del tutto nuove al panorama politico europeo ma sono, comunque, espressione di istanze sorte anche attraverso il digitale e gli strumenti di comunicazione informatici, e che devono ancora trovare risposte.

Le democrazie occidentali, come evidenziato, si presentano come il bersaglio più aggredibile da parte della disinformazione che, non a caso, diventa più evidente in occasione delle tornate elettorali per influenzare l'esito delle elezioni⁸.

Un noto esempio di successo della disinformazione è relativo al referendum consultivo sulla Brexit, in cui il dibattito pubblico è stato a tal punto influenzato da notizie e dati non verificabili, veri o falsi che si siano rivelati in seguito, da contribuire a un risultato inaspettato alla vigilia e favorire, seppur di misura, la vittoria del "Leave".

Cercando di trarre, in conclusione, delle ricadute concrete della disinformazione nei confronti dei bersagli contro cui è diretta, possiamo annoverare come obiettivi comuni⁹:

- i) la creazione di un clima di abitudine agli scandali;
- ii) la creazione di un clima di sfiducia nelle istituzioni, al fine di manipolare più facilmente i comportamenti delle persone;

⁸ Cfr. G. ZICCARDI, *Tecnologie per il potere*, Milano, 2019.

⁹ Il presente elenco è mutuato, in parte, da L.S. GERMANI, *La minaccia della disinformazione: panoramica introduttiva*, in L.S. GERMANI (a cura di), *Disinformazione e manipolazione delle percezioni, Una nuova minaccia al Sistema-Paese*, Roma, 2017.

- iii) la creazione di momenti di tensione o attrito tra Stati, crisi diplomatiche o, comunque, di presupposti per cui la cooperazione risulti impraticabile o impossibile;
- iv) l'indebolimento delle difese di uno Stato facendo leva sullo scarso senso critico della sua popolazione e sulla generale impreparazione collettiva;
- v) la conduzione, progressiva, di un Paese ad assumere decisioni di politica interna o estera contrarie all'interesse nazionale;
- vi) il danneggiamento della reputazione dello Stato e/o delle sue imprese, compresa la manipolazione dei mercati finanziari con conseguenze destabilizzanti sul sistema economico;
- vii) il diffondere paura, odio, confusione in determinati settori della popolazione, incoraggiando comportamenti scomposti, irrazionali e violenti;
- viii) lo sviamento delle analisi e delle indagini degli organi dello Stato, comprese magistratura e *intelligence*.
- ix) la creazione di minacce e falsi allarmi, intesi a generare disordine.

Parte II - Il rapporto tra fake news, profilazione e politica

5. Alcune considerazioni pratiche

Il tema delle *fake news* è un fenomeno, oggi, assai interessante non solo per gli aspetti di geopolitica e di relazioni internazionali esposti nella Prima Parte di questo Articolo ma, anche, per i suoi risvolti spiccatamente interdisciplinari: coinvolge, infatti, temi politici, sociali, tecnologici, psicologici e caratteriali (degli “autori” e delle “vittime”) e, soprattutto, con l'avvento degli smartphone e dei social network, è mutato radicalmente nelle modalità attraverso le quali si manifesta.

Da un lato, quindi, non è possibile per l'interprete comprendere compiutamente il fenomeno se non mantenendo un approccio trasversale come quello, ad esempio, tradizionalmente adottato dall'informatica giuridica.

Dall'altro, diventa fondamentale cercare di valutare e “pesare”, se possibile, l'impatto concreto che hanno avuto le tecnologie e i *social network* nell'alterazione radicale del panorama. In altre parole: un tema classico quale quello delle notizie false, vecchio come l'uomo, è stato riscritto in forme nuove dalla società digitale. Lo studioso Giuseppe Riva, di recente, ha descritto con molta cura, in una sua opera, questi innumerevoli punti di contatto, e di frizione, tra le varie discipline¹⁰.

Il fenomeno della “produzione” di *fake news* è da considerarsi, secondo Riva, una vera e propria emergenza dei tempi moderni. Esistono, oggi, migliaia di siti, in tutto il mondo, che hanno come obiettivo editoriale (e, spesso, come unica ragione di esistenza) proprio quello di creare *fake news*. Sono, in altre parole, vere

¹⁰ Si veda G. RIVA, *Fake news*, Bologna, 2018.

e proprie “fabbriche” di fake news. L’Autore si riferisce, in questo caso, non solo a *news* palesemente false ma, anche, a *news* che presentano dei fatti reali ma in modo distorto, orientato esplicitamente al supporto di tesi pregiudiziali e, soprattutto, con l’intenzione di generare nel lettore (meglio se utente/elettore) odio e disgusto.

Spesso questa diffusione di false notizie ha ordini di grandezza enormi che ci risulta difficile immaginare e quantificare (superiori ai numeri, ad esempio, che registrano oggi i grandi quotidiani *online*); vantano, quindi, la capacità potenziale di raggiungere tutti i soggetti che sono connessi in rete.

Secondo l’Autore, le *fake news* sono prodotte essenzialmente per due motivi: i) per guadagnare soldi, ossia per generare profitto o ii) per generare consenso (che, nell’ambiente dei *social network*, è da tempo considerato una valuta ben spendibile).

Il consenso generato è, di solito finalizzato, a portare instabilità politica o sociale. A generare caos, insomma.

Circa i soldi, invece, le *news* sono pensate come vere e proprie “esche da click” (“clickbait”) affinché, grazie ai proventi della pubblicità, possano arricchire i creatori delle notizie stesse. Spesso non si comprende, quindi, che alla base del fenomeno che si sta illustrando vi è un vero e proprio commercio e, in particolare, vi è un nuovo mercato che permette profitti assai rilevanti.

Riva nota come le *fake news* (ma, soprattutto, il loro processo di creazione) siano per alcuni aspetti diverse dai processi di disinformazione che sono da sempre presenti in società e (soprattutto) nei regimi politici anche se, spesso, si tende a sostenere che nulla è cambiato nella diffusione di notizie false (e che, in fondo, “ci sono sempre state”).

Secondo Riva, la differenza radicale è che queste *news* sono, oggi, in grado di influenzare i soggetti con un coinvolgimento mai visto prima e, al contempo, con una velocità nuova. Per di più, non solo sono capaci di modificare la percezione della realtà del soggetto che viene “colpito” dalle *fake news* stesse, ma sono anche in grado di influenzarlo fino al punto di spingerlo a condividerle in maniera spontanea e partecipata.

Questa osservazione di Riva è interessante e molto puntuale perché, come si nota chiaramente, non si concentra sul contenuto delle news (che, a volte, non cambia rispetto alla disinformazione “tradizionale”) ma sul contesto (“viralità”, “condivisione”, “engagement”) e sulla vittima (che viene addirittura convinta, in molti casi, a condividere le notizie false, a farle circolare e, in definitiva, ad alimentare il mercato e, sia consentito il termine, diventa così “complice”).

6. Gli aspetti informatico-giuridici

La storia delle moderne *fake news* appare legata a doppio filo alla storia della tecnologia, e non si può scindere l'evoluzione di questo fenomeno da ciò che è successo negli ultimi quindici anni, soprattutto con l'avvento dello *smartphone* e delle reti sociali.

Il loro legame con l'uso dei *social network* è probabilmente la parte più interessante da analizzare, e ha ancora molti lati oscuri.

Se analizziamo il tema delle *fake news* dal punto di vista appena esposto poco sopra, nota correttamente ancora Riva, potremmo azzardare tranquillamente nel paragonarle, nel loro utilizzo politico, a una vera e propria forma di “guerra non convenzionale” in corso. È una guerra che mescola le teorie della scienza della comunicazione con quelle psicologiche, con lo scopo finale ben preciso di convincere le persone. Vi è in corso, in sintesi, una vera e propria “guerra psicologica dell’informazione”.

L'azione, nota sempre l'Autore citato, consiste quasi sempre nell'occupare in maniera massiccia lo spazio informativo per veicolare notizie false nella lingua del Paese individuato come *target* e all'interno di quel territorio. Si cercano, così, di sabotare e influenzare i processi di comunicazione e di trasmissione delle informazioni anche allestendo agenzie, o realtà commerciali, deputate *ad hoc*. Si agisce, poi, sulla coscienza dei cittadini degli Stati che sono gli obiettivi dell'aggressione e, in pochi giorni, con simili tecniche, si può destabilizzare un Paese.

Il tutto avviene sovente in maniera completamente invisibile, senza che le istituzioni e, spesso, anche le piattaforme si accorgano di quello che sta succedendo e, soprattutto, della capacità che hanno simili strategie di avvelenare il dibattito in corso. La stessa società Facebook è stata accusata di non “essersi accorta” di ciò che stava capitando sulla sua piattaforma, prima con il caso di *Cambridge Analytica* e, poi, con il caso di Trump e delle attività dei *bot* russi.

Un secondo punto, non marginale, è l'economicità di un simile sistema: con un budget abbastanza limitato si raggiungono centinaia di milioni di persone, spesso potenziali elettori, e questo aspetto lo rende, ovviamente, ancora più pericoloso.

La caratteristica più visibile è sicuramente questa incredibile capacità di impattare sui soggetti (e sui gruppi sociali) con una velocità, e un coinvolgimento, mai visti prima nella storia della disinformazione.

7. I meccanismi di funzionamento delle *fake news*

Entrando più nel dettaglio, secondo Riva i meccanismi *ad hoc* che fanno “funzionare” le *fake news* sono, nella società odierna, almeno cinque:

- i) le *fake news*, nota l'Autore, sono costruite in modo da riflettere gli obiettivi, gli interessi e le personalità dei membri della comunità. Si tratta di un obiettivo facile da raggiungere grazie alla potenza che hanno, oggi, i sistemi di profilazione degli utenti;
- ii) le *fake news* vengono viste da un numero sufficientemente elevato di membri della comunità. Anche questo obiettivo è facile da raggiungere, dal momento che oggi gruppi su Facebook (ma, anche, su WhatsApp) possono convogliare migliaia, se non milioni, di soggetti;
- iii) i membri della comunità non si accorgono del fatto che le notizie siano false. Ciò è comune anche a causa di un generale calo di attenzione nei confronti della reale natura dei contenuti;
- iv) le altre notizie presenti nella comunità non sono significativamente in contrasto con i contenuti delle *fake news*. Detto in altri termini, le *fake news* si inseriscono perfettamente in un contesto informativo che apparentemente, come tematiche e conclusioni, sembra in linea con i contenuti delle *fake news*;
- v) un numero molto basso di membri della comunità si impegna a informarsi al di fuori di esse. Non vi è, quindi, una verifica delle fonti “al di là del messaggio sullo smartphone”.

Le caratteristiche dei *social media*, nota sempre Riva, sembrano proprio essere pensate per facilitare il raggiungimento di tutti questi obiettivi nefasti.

Il primo obiettivo di chi genera e diffonde simili contenuti, ricorda l'Autore, è infatti quello di creare delle *fake news* che ottengano il supporto della comunità in cui si vogliono diffondere. Questo obiettivo si raggiunge (semplicemente) incarnando in termini di comportamento, personalità e identità sociale le aspettative e i valori degli appartenenti a quella rete.

Ecco perché i contenuti delle *fake news*, in una prospettiva di efficacia, devono essere coerenti sia con la conoscenza condivisa dalla comunità, sia con la personalità e le aspettative dei suoi membri.

L'autore di *fake news*, nota l'Autore, terrà allora costantemente sotto controllo i *trend topics*, o gli argomenti principali di cui si discute su un sito web, pagina o profilo, “ascoltando” le reti partecipando alla vita della comunità o usando strumenti automatizzati che analizzano i contenuti e le conversazioni.

Il fine è quello di ottenere, prima di far circolare delle *fake news*, dei dati molto dettagliati sugli argomenti più discussi, sull'orientamento positivo o negativo della rete nei confronti dell'argomento, sulla presenza di opinioni divergenti o di *influencer* che potrebbero aiutare nella diffusione delle notizie false.

Siamo in presenza di una vera e propria opera di comprensione sia degli argomenti di cui si parla, sia della personalità dei soggetti che compongono quella comunità o quel gruppo di discussione, tanto che Riva, nel saggio che abbiamo citato, arriva a parlare di “persuasione psicologica di massa”.

8. La connessione tra *fake news*, psicologia e test di personalità

Un passaggio interessante dello studio di Giuseppe Riva è quello che accenna all'uso, per i fini che abbiamo descritto poco sopra, di test di personalità (tramite domande specifiche, in particolare, si cerca di definire un profilo del soggetto che è in quell'ambiente/comunità dove circoleranno le *fake news*).

Uno dei test più tradizionali, che Riva cita nel suo saggio, fu in origine pensato per valutare la personalità di un soggetto in base a cinque parametri/dimensioni fondamentali:

- i) la prima dimensione dell'individuo che viene "contata" e profilata è l'energia (una sorta di orientamento fiducioso ed entusiasta nei confronti delle circostanze della vita);
- ii) il secondo elemento che gli algoritmi trattano è l'amicalità (che si può intendere come altruismo, il prendersi cura degli altri, il dare supporto emotivo a terzi o, al contrario, manifestazioni chiare di ostilità, indifferenza ed egoismo);
- iii) il terzo aspetto che viene preso in considerazione in simili test è la coscienziosità (ossia la precisione, accuratezza, responsabilità e perseveranza dell'individuo nella sua vita quotidiana);
- iv) il quarto parametro dell'individuo e del suo carattere interessante per questi studi è la stabilità emotiva (per cui si rilevano e analizzano episodi di ansia, depressione, irritabilità e problemi dell'umore);
- v) il quinto aspetto interessante è l'apertura mentale del soggetto (intesa come predisposizione verso nuove idee, verso gli altri e verso i sentimenti positivi).

Se si riflette un attimo, sul punto, al caso che ha coinvolto *Cambridge Analytica*, è noto come la società operasse proprio su questi aspetti e con simili strategie al fine di preparare dei contenuti che fossero già idonei a interessare e influenzare un gruppo di persone che già era stato profilato con cura e con una precisione che non aveva precedenti nella storia del marketing e dell'analisi sociale.

Vi è una possibilità concreta, oggi, di utilizzare i commenti lasciati dagli utenti *online*, i "mi piace" e i comportamenti tenuti in rete proprio come se fossero veri e propri indizi e segnali di specifici aspetti della personalità dell'individuo, soprattutto se l'utente mantiene un livello di privacy personale molto basso ed è portato a condividere gli aspetti suoi più intimi e a "denudarsi" online.

La stessa rete di amici che un soggetto ha online diventa essenziale per costruire, come si diceva poco sopra, il comportamento nella sfera sociale o ambiente "comunitario" nel quale opera quotidianamente. In questo caso, se non è la piattaforma la prima a proteggere gli utenti, diventa veramente elementare effettuare simili operazioni di profilazione.

Un secondo punto importante, nota sempre Riva, è la visibilità della notizia sulla piattaforma, una visibilità che viene condizionata anche dai *like* e dagli apprezzamenti della comunità per tale informazione. Se a ciò si aggiunge il fatto che gran parte degli utenti sono all'interno di una sorta di bolla informativa, ossia tendono a conservare le loro idee e minimizzano il confronto con visioni alternative che le possano

contaminare, si trovano all'interno di un universo di informazioni che è specifico per loro e sono succubi di meccanismi invisibili di selezione dei contenuti che portano ad escludere ciò che non corrisponde esattamente ai loro gusti, il quadro che si genera impedisce, come prima cosa, un confronto leale e il fiorire di uno spirito critico.

Se la *fake news* è costruita esattamente in base al profilo di un singolo individuo, di un “tipo” di utente o di un gruppo, conclude Riva, nessuno la metterà mai in discussione. Anzi, se ne faciliterà la diffusione e si fornirà alle notizie false un'ulteriore, pericolosa cassa di risonanza.

9. Ulteriori fattori critici

Ci sono altri fattori, nota sempre Riva, che riducono ulteriormente la capacità critica degli utenti e che contribuiscono, così, a disegnare un quadro di sfondo ancora più preoccupante.

Un primo fattore, evidente, è la bassa attenzione dedicata comunemente ai contenuti da parte delle persone. Gran parte degli utenti è ormai abituata a un'analisi assai superficiale delle informazioni proposte (Riva parla di 8 secondi di attenzione media per ogni contenuto). Ciò comporta una conseguenza chiara: che le informazioni di bassa qualità si trovano ad avere la stessa, identica probabilità di diventare virali di quelle di alta qualità, dal momento che la rete è la prima a non discriminare tra contenuti di alta e di bassa qualità.

Un secondo elemento preoccupante, nota l'Autore del saggio, è che il soggetto è tipicamente resistente al cambiamento: davanti a una scelta da effettuare, la scarsa attenzione spinge il soggetto a scegliere notizie e contenuti che non siano tali da entrare in conflitto con la propria “visione del mondo”. E questa resistenza, segnala Riva, influenza anche le scelte del gruppo, soprattutto quando la scelta stessa tende a polarizzarsi verso le scelte estreme, che garantiscono il consenso del gruppo, e non verso nuove informazioni che possano emergere dalla discussione. Non ci sono quasi mai, insomma, argomenti che tendano verso la direzione opposta, ma vi è quasi sempre una radicalizzazione delle posizioni esistenti.

Se aggiungiamo il fatto, conclude Riva, che non si esce ormai dai *social media* per leggere, ma che le reti sociali hanno assunto un ruolo centrale nella costruzione della nostra identità, si comprende che il quadro è completamente nuovo.

Senza contare, ultimo ma non ultimo, il costante (e grande) dibattito su cosa sia vero o cosa sia falso, o sul “livello” di verità dei *post*. È sempre possibile individuare un fatto citato in una notizia come qualcosa che abbia consistenza vera e reale, ossia immediatamente evidente, vera e propria esperienza diretta? Purtroppo no. Se a ciò aggiungiamo, nota correttamente l'Autore, che il digitale permette di cambiare i contenuti e di modificarli affinché possano sembrare veri, e che le immagini e i video sono ormai il cuore

delle *fake news*, il timore dei *deep fake* e della facilità di manipolazione dei contenuti che offre il digitale aumentano ulteriormente le preoccupazioni.

Secondo Riva, nel quadro che abbiamo poco sopra descritto, possono intervenire, per cercare di migliorare la situazione, i) delle norme, ii) dei *fact-checker* o iii) può intervenire il singolo utente. Analizziamo velocemente tutti e tre questi aspetti/rimedi.

Il ruolo delle istituzioni, e l'intervento della politica, dei Legislatori, dei Governi, pone problemi enormi. Le idee andrebbero lasciate "libere", secondo la più pura tradizione nordamericana, perché il sistema sarebbe in grado di discriminare ed evidenziare le idee migliori o, al contrario, il quadro attuale è completamente diverso rispetto a quello che era stato immaginato nell'Ottocento e nel Novecento ed occorre con urgenza una regolamentazione del parlato e dell'informazione?

Di certo, nota Riva, nei social media non sta accadendo questo: le idee migliori non "raggiungono la superficie" automaticamente, soprattutto se l'utente si chiude in una bolla e se si "premiano" in visibilità non le idee migliori ma quelle più popolari, magari alterando anche i meccanismi e i risultati grazie a falsi profili.

Nel contesto istituzionale diventa, poi, particolarmente centrale comprendere il punto della protezione dei dati degli utenti e il modo migliore per proteggerli. Se i dati personali che possono servire a profilare gli utenti vengono, alla fonte, protetti il più possibile (con norme quali, ad esempio, il GDPR), il quadro di discrezionalità di chi crea *fake news* potrebbe essere in qualche modo limitato (anche se rimane sempre il problema, assai grave, dei dati che sono auto-esposti dagli utenti in cambio di servizi).

Un secondo rimedio possibile, secondo l'Autore del saggio, è un potenziamento delle attività di gruppi o singoli che si dedicano ad attività di *fact-checking*, ossia verificano la corrispondenza ai fatti delle notizie più diffuse. Si tratta, però, di un lavoro che è costoso, richiede pazienza e tempo e non sempre è, all'interno dei sistemi di informazione (che oggi sono, in molti casi, in crisi) sostenibile economicamente. Terzo, ma non ultimo, è lo spirito critico del singolo individuo. Con un aumento dello spirito critico, dell'attenzione alle notizie che si leggono, aumenterebbe anche la "resistenza" alle *fake news*. Il problema, in questo caso, è che gli utenti vivono in un periodo storico in cui si è diffusa una vera e propria dipendenza dallo smartphone e dagli impulsi informativi che arrivano in ogni secondo e che tendono proprio ad annullare lo spirito critico (che ha bisogno di tempo per svilupparsi e manifestarsi al meglio).

10. Le regole delle piattaforme

Nella parte finale del saggio citato, Giuseppe Riva riporta, come esempio interessante, alcune regole di base che Facebook ha pubblicato sulla propria piattaforma per cercare di orientare gli utenti, soprattutto i più inesperti, nel mondo delle *fake news*. Sono indicazioni semplici ma interessanti: disegnano un

percorso utile non solo sui *social network* ma, in generale, come modalità corretta di affrontare le informazioni oggi. Le regole sono le seguenti (tra parentesi, alcune mie considerazioni):

- i) non fidarsi dei titoli urlati (in molti casi, l'uso del maiuscolo o, comunque, di termini suggestivi, clamorosi, volgari, discriminatori, entusiastici o, in ogni caso, “amplificati”, è il metodo/strategia principe per attirare immediatamente l'attenzione e suggestionare il lettore);
- ii) procedere a un controllo accurato dell'indirizzo web/http del sito (ci sono molti siti web di fake news che sostituiscono singole lettere del titolo, o invertono caratteri, per trarre in inganno il lettore e far credere che il sito sia, in realtà, quello “ufficiale” del concorrente più famoso);
- iii) procedere a ricerche specifiche su chi ha scritto la notizia (sarebbe opportuno, in particolare, investire tempo per verificare l'autore della notizia, valutare se un autore esista, analizzare la sua produzione giornalistica, vagliare quali altre notizie abbia fatto circolare e che precedenti di credibilità manifesti);
- iv) è utile fare attenzione alla formattazione/ortografia del testo (sovente un testo sciatto e ricco di errori è indice di una non corretta traduzione o di una generazione automatizzata del testo stesso o, comunque, indice di una dubbia provenienza);
- v) occorre prestare particolare attenzione ai contenuti digitali, soprattutto immagini e video, che siano stati ritoccati, o immagini che sono reali ma sono proposte fuori contesto (si tratta di un problema oggi delicatissimo, data la facilità non solo di creare immagini, video o materiale multimediale completamente falso ma, anche, di recuperare dalla “memoria” della rete informazioni datate per poi riproporle come nuove o, comunque, collegate a un contesto che non è quello originario);
- vi) sarebbe opportuno procedere a un controllo delle date e dei riferimenti temporali (un check della linea del tempo, quasi giornalistico, può consentire di comprendere immediatamente la verità o meno di una notizia);
- vii) verificare le testimonianze riportate nella notizia o correlate alla notizia “sospetta” (si tratta di un classico processo di controllo delle fonti al fine di individuare elementi che possano corroborare il fatto indicato);
- viii) può essere molto utile controllare se altre fonti hanno riportato la stessa notizia (è chiaro che, nel panorama informativo attuale, se una notizia è presente in un solo luogo può essere indice di falso);
- ix) occorre sempre prendere in considerazione il fatto che la notizia potrebbe essere uno scherzo (in questo caso diventa necessario che l'utente comprenda come distinguere le notizie vere da quelle satiriche o da quelle create appositamente per fare divertire il pubblico appartenente a un sito, a un gruppo o a una comunità online);

x) è utile tenere sempre a mente che alcune notizie possono essere intenzionalmente false (esistono infatti realtà che, sui loro siti web o in pagine da loro gestite, pubblicano volontariamente notizie false; in tal caso l'utente dovrebbe essere in grado di comprendere immediatamente il contesto).

Giuseppe Riva conclude il suo saggio indicando, sinteticamente, le cinque caratteristiche delle *fake news* che dovrebbero interessare non solo gli interpreti che studiano il fenomeno ma anche gli utenti che le osservano quotidianamente sulle piattaforme che frequentano o sugli smartphone che utilizzano:

- i) le *fake news* sono, oggi, ottimizzate per generare una forte risposta emotiva capace di spingere il lettore alla mobilitazione e per generare sdegno e rabbia (questo lo definiremmo come l'aspetto psicologico delle *fake news*, fondamentale e, per così dire, propedeutico per comprendere tutti gli altri aspetti);
- ii) le *fake news* sono, nella società digitale odierna, personalizzate (questo lo definiremmo come l'aspetto della profilazione e del micro-targeting dell'individuo, che è centrale in un'ottica predittiva e di anticipazione della volontà dei soggetti);
- iii) le *fake news* sono, oggi, automatizzate nella loro generazione e diffusione (questo è l'aspetto più tecnico, correlato ai falsi profili, ai *bot* e a sistemi evoluti per generare e diffondere notizie false su larga scala senza l'intervento dell'uomo o con un minimo investimento di risorse uomo/tempo rispetto al risultato ottenuto);
- iv) le *fake news* sono create in forma multimediale e con contenuti pensati per facilitarne la diffusione sui *social network* (e qui occorre porre attenzione, si diceva, ai falsi);
- v) le *fake news* sono create per sembrare vere (e su questo punto diventa essenziale l'aspetto dell'inganno, che è molto importante soprattutto nei confronti di utenti con una preparazione culturale, o una soglia di attenzione, molto bassa).

11. Il delicato rapporto tra *fake news*, politica ed equilibri democratici

Il tema del *falso*, come si diceva poco sopra, è diventato, in pochi anni, di grande attualità anche correlato alle attività politiche svolte sui *social network*.

Il problema di fondo è, in prima battuta, originato dalla semplicità che vi è, oggi, nell'*automatizzare* diverse azioni che si svolgono sui *social network* (anche senza bisogno di conoscenze di elementi di programmazione) e la facilità, al contempo, attraverso la quale è possibile creare falsi profili (o identità) su dette piattaforme.

I controlli all'accesso dei *social network* sono, di solito, mantenuti molto laschi, e i gestori delle piattaforme preferiscono reagire *dopo* – quando segnali inequivocabili evidenziano un'attività sospetta in determinati periodi “caldi” – piuttosto che predisporre verifiche accurate prima. Si pensi, a puro titolo di esempio, che nel novembre del 2018 Twitter ha annunciato di avere eliminato 10.000 falsi *account* in vista delle

elezioni di *mid term* negli Stati Uniti d'America (con l'accusa che tali *account*, al fine di condividere in maniera organizzata informazioni false, esortassero i cittadini a non andare a votare e fossero falsamente attribuiti al partito democratico).

Gli studiosi si sono allora interessati, in primo luogo, al fenomeno dei profili falsi – o finti *account*, che dir si voglia – apparsi su Twitter: sono diventati un vero e proprio problema politico internazionale nel momento in cui tutti gli operatori e gli analisti hanno percepito una crescita smisurata di *bot* su Twitter, veri e propri *account* automatizzati e indipendenti, collegati, direttamente o indirettamente, a politici o a campagne elettorali in corso¹¹.

Il motivo di questa azione sistematica di falsificazione è chiaro e facilmente intuibile: si può, in questo modo, generare senza sforzo, e senza impiegare risorse umane e di tempo, un'enorme *discussione* che attira attenzione, visibilità, viene condivisa e diventa di tendenza, *nel bene* (evidenziando informazioni utili) o *nel male* (immettendo informazioni false o aggressioni personali) sino a influenzare direttamente il mondo dell'informazione.

Gli studiosi hanno stimato che i profili falsi su Twitter siano tra il 5 e il 10 per cento, e sono in molti casi programmati per alterare il dibattito pubblico mettendo in circolazione false informazioni, per deviare l'attenzione da questioni importanti, per manipolare discorsi, alimentare il gossip, far circolare *spam* e *malware* o aggredire direttamente un altro profilo¹².

Alcuni sostengono che piuttosto che la rimozione sarebbe importante una informazione trasparente che faccia capire se il profilo è falso o vero, etichettando, ad esempio, pagine o profili e potenziando le possibilità di conoscenza degli utenti affinché capiscano se una notizia o un'attività sia vera o falsa.

Le *fake news*, come nota bene Antonello Soro, Garante per la privacy italiano, sembrano unite a doppio filo all'*architettura* stessa dei *social network*, dove paiono aver trovato un terreno ideale per fiorire e moltiplicarsi. Si legga questo breve passaggio:

¹¹ Si vedano, sul punto: C. BARANIUK, *How twitter bots help fuel political feuds*, in Internet all'indirizzo <<https://www.scientificamerican.com/article/how-twitter-bots-help-fuel-political-feuds/>>; R. DIRESTA - J. LITTLE - J. MORGAN - L. M. NEUDERT - B. NIMMO, *The bots that are changing politics*, in Internet all'indirizzo <https://motherboard.vice.com/en_us/article/mb37k4/twitter-facebook-google-bots-misinformation-changing-politics>. In questo numero speciale si vedano i contributi di P. BONINI, *L'autoregolamentazione dei principali Social Network. Una prima ricognizione delle regole sui contenuti politici* e M. MONTI, *La disinformazione online, la crisi del rapporto pubblico-esperti e il rischio della privatizzazione della censura nelle azioni dell'Unione Europea (Code of practice on disinformation)*, entrambi in questo fascicolo.

¹² Si veda, sul punto, C. TIMBERG - E. DWOSKIN, *Twitter is sweeping out fake accounts like never before, putting user growth at risk*, in Internet all'indirizzo <https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/?utm_term=.4417d29b90ca>.

«I social assurgerebbero così a luoghi in cui costruire una verità finalmente indipendente, perché liberata dalla soggezione al potere, e in cui custodire l'autenticità contro l'ipocrisia del mainstream. Nasce qui, essenzialmente, il tema delle fake news, alimentato dal meccanismo su cui si fonda la condivisione virale in Rete, che fa dipendere l'attendibilità della notizia non dalla sua verificabilità, ma dalla quantità di condivisioni ottenute. È la logica dell'audience: le notizie, di qualsiasi origine, finiscono con il plasmare post-verità e conferire autorevolezza alla loro fonte in funzione della quantità di lettori. Il che ha implicazioni importanti non soltanto rispetto al tema del pluralismo e della libertà di informazione ed espressione, ma anche rispetto alla formazione della volontà del corpo elettorale, laddove le false notizie concernono appunto questioni oggetto di voto popolare. La manipolazione del consenso, resa possibile dal condizionamento delle opinioni di cittadini profilati in base al loro comportamento in Rete, costituisce, infatti, un pericolo per la tenuta delle democrazie, che rischiano di regredire verso regimi plutocratici, fondati sul potere informativo»¹³.

Le fake news in ambito politico, in particolare, si caratterizzerebbero per quattro aspetti che le rendono particolarmente insidiose;

- i) si fondano su una condivisione virale. La notizia falsa inizia immediatamente a circolare grazie ai contatti, alle condivisioni, alle reti di siti o profili appartenenti alla stessa “galassia” che, puntualmente, ne danno grande visibilità. Oggi tutti i partiti politici hanno una rete di profili, più o meno visibili e più o meno dichiarati, che sono in grado, in pochi secondi, di inondare i social network di notizie false. La viralità si appoggia sulla capacità di amplificazione e sulla persistenza dell'informazione, e fornisce lo strumento migliore per l'inizio delle operazioni di disinformazione;
- ii) Confidano sulla non verificabilità immediata. La ricerca di comunicazione immediata, poco complessa, elementare e superficiale di gran parte degli utenti sui *social network* fa sì che la maggior parte delle notizie false sfugga a un processo di verifica delle fonti, soprattutto se comporta la ricerca di fonti (investimento di tempo), l'uscita dall'ambiente dove ci si trova (spostarsi dalla pagina aperta di Facebook a un sito web) o se la notizia appare verosimile perché ben falsificata. A ciò si aggiunga il fatto che, se la notizia falsa arriva a una persona di cui già si conosce l'orientamento su quel tema, la verifica molto probabilmente non avviene per auto-convincimento del soggetto stesso;
- iii) Confidano sulla complicità di tante condivisioni che danno autorevolezza. Le notizie false, man mano che sono condivise, acquistano *autorevolezza* nel contesto dei *social network*. Grazie anche a persone che condividono con la classica frase “non so se è vera, ma la condivido”, o senza pensare, o perché in linea con il loro modo di pensare. L'autorevolezza non viene dalla verifica delle fonti ma dal numero di

¹³ Si veda. A. SORO, *Persone in rete*, Roma, 2018, p. 31.

visualizzazioni, condivisioni e *like*. Lo *share* è la moneta nel mercato dei *social network*: una valuta che assume sempre più valore tanto più attira condivisioni;

iv) Sono sempre più mirate al soggetto. Le *fake news* sono sempre più mirate e ritagliate sul soggetto e sulle sue preferenze, saltando così il delicato aspetto della verifica – il *target* non verifica la bontà della notizia perché “sente” quell’affermazione come sua – e domandando al soggetto di far circolare nel *suo ambiente* (dove presumibilmente ci sono molti soggetti che la pensano allo stesso modo) quelle comunicazioni.

12. *Fictio*, propaganda e profilazione estrema dell’utente

Remo Bodei descrive molto chiaramente un quadro connotato dalla cosiddetta “post-verità”, generata da una politica fatta di *annunci* e, in definitiva, di *fictio*. Si prenda in considerazione questo breve ma intenso passaggio:

«La verità è oggi insidiata da quelli che nell’entourage di Trump si chiamano “fatti alternativi”, perché viviamo – è un’espressione che si sta affermando – nell’epoca della post-verità. Esiste ancora un’opinione pubblica, come sfera di dibattito basato su un serio confronto di idee o di posizioni, come “cane da guardia” del potere? O non è anch’essa diventata una fictio, una costruzione capillarmente e scientificamente organizzata di una realtà parallela? E questo non avviene già, a monte, attraverso matrici di idee ed emozioni preconfezionate, e, in seguito, mediante il loro ritocco e aggiornamento continuo, che produce un mutevole “clima di opinione”? E i cittadini non sono orientati anche attraverso una politica di annunci cui non segue alcuna effettiva attuazione, anche perché la politica non è più capace di operare scelte rilevanti e deve continuamente ammansire gli elettori, gestire le frustrazioni e lavorare sul registro dell’immaginario (paura e speranza), visto che i reali decisori sono élite economiche transnazionali, anonime e prive di responsabilità nei confronti dei cittadini?»¹⁴.

Come si diceva poco sopra, il fenomeno della disinformazione è legato a doppio filo con quello di strategie di *propaganda* pre e post-elettorale che cercano di sfruttare al massimo gli aspetti positivi e negativi dei *social network*. I tre obiettivi di comunicazione che sono ormai caratteristica essenziale di tutte le attività sui *social network* dell’era della *fast politics* sono i seguenti:

- i) Occupare subito lo spazio mediatico. Il candidato politico, o chi per lui, interviene *per primo* sulla notizia del giorno. In tal modo, si costringono i media tradizionali, gli avversari e gli alleati a *rincorrere*;
- ii) Polarizzare la discussione. La seconda strategia consiste nel polarizzare tutta la discussione attorno a sole due categorie: pro e contro un determinato candidato o una certa idea;

¹⁴ R. BODEI, *Vivere online*, in *Il Mulino*, n. 2/2017, pp. 208-209.

iii) Alzare i toni. La terza strategia consiste nel lanciare messaggi forti, estraendo dall'opinione pubblica i "sentimenti negativi", soprattutto rabbia, paura e aggressività.

13. Alcune conclusioni: un'alterazione degli equilibri democratici?

Negli ultimi anni sono sempre di più gli studiosi – nazionali e internazionali – che, analizzando il quadro odierno della politica e delle comunicazioni sui *social network*, denunciano la possibilità di una *alterazione* (o manipolazione, o distorsione che dir si voglia) degli *equilibri democratici*.

Si tratta, questo, di un punto nodale che ci porta ad alcune riflessioni conclusive che diventano centrali per il nostro studio.

La potenza dei social network che abbiamo descritto nelle pagine precedenti si presterebbe, in sostanza, a incidere direttamente sul sistema stesso di governo e di rappresentanza.

Di qui, il "giocare sporco" in rete e sui *social network* da parte di rappresentanti istituzionali o, comunque, di interesse pubblico produrrebbe un *vulnus* costante nella società.

Antonello Soro, Garante per la protezione dei dati personali in Italia, poco tempo dopo il clamoroso caso di *Cambridge Analytica*, ha ben tratteggiato questa attività di alterazione degli equilibri democratici. Si legga, ad esempio, il seguente passaggio:

«La vicenda dell'utilizzo, da parte di Cambridge Analytica, dei dati personali di milioni di utenti di Facebook, al fine di influenzarne le scelte elettorali orientando così nella direzione voluta (o, meglio, commissionata) le consultazioni politiche o referendarie, mette in luce quanto l'estensione del metodo profilativo, dal piano commerciale a quello politico, produca effetti gravemente distorsivi del sistema democratico. Le garanzie volte a salvaguardare il pluralismo, la corretta informazione dei cittadini, la libera formazione del consenso elettorale e la diversificazione dell'offerta politica – in condizione di parità nella competizione – vengono di fatto annientate con un solo click: e a pagarne il prezzo è ciascuno di noi, cittadino prima (e oltre) che consumatore. Ancora una volta, il problema non è la tecnologia in sé (i big data, in questo caso) ma il suo utilizzo, che deve essere volto alla promozione dell'utilità sociale e dei diritti, e non alla concorrenza sleale o all'indebito condizionamento di scelte che, sul piano commerciale e soprattutto su quello politico, devono restare libere e autodeterminate»¹⁵.

Secondo Soro, in sintesi, sono *quattro* i punti di vulnerabilità del sistema democratico che sono attaccati, sino a causare una alterazione degli equilibri.

i) Attacco al *pluralismo*. Vi è il timore, in questo caso, che un algoritmo possa decidere di impedire la *coesistenza* in società di individui, gruppi e partiti con orientamenti diversi che possano avere un'autonomia

¹⁵ Si veda. SORO, *Persone in rete*, cit., p. 144.

ed eguale partecipazione alla vita pubblica. Ciò avverrebbe filtrando, selezionando e censurando determinati contenuti e, al contempo, prediligendone altri;

ii) Attacco alla *corretta informazione* dei cittadini. La paura, in questo caso, è che il sistema dell'informazione sia *viziato*, sia a causa della circolazione di notizie false, sia di notizie mirate al profilo specifico dell'utente, sia creando "bolle" che escludano l'accesso a un gran quantitativo di informazione di diversa natura e orientamento;

iii) Attacco alla libera formazione del *consenso elettorale*. Sistemi quali quello alla base di *Cambridge Analytica* impedirebbero al cittadino/elettore di formarsi completamente (in un'ottica di conoscenza) e liberamente valutando ogni posizione politica. Ciò in quanto l'algoritmo è in grado di recapitare unicamente informazioni connesse allo stato attuale dell'utente e alle sue preferenze manifestate nell'ambiente online;

iv) Attacco alla *diversificazione* dell'offerta politica e alla condizione di *parità* nella competizione. Maggior potere sui *social network*, deciso dall'algoritmo, comporterebbe maggiore visibilità e, quindi, maggiore possibilità di arrivare agli elettori. Ciò vizierebbe la completezza del quadro, penalizzerebbe i movimenti politici meno evidenti o presenti, e fornirebbe informazioni, in molti casi, "a senso unico".

Si comprende, in definitiva, come l'ambiente sia ancora più vulnerabile a causa di comportamenti che sono *suggeriti*, spesso, dai *social network* stessi e dalla loro dinamica discorsiva del tutto particolare.

Il comprendere il livello di influenza dei *social network* sugli equilibri democratici permette un'interpretazione dell'uso delle nuove tecnologie che sia sempre e comunque, si diceva, attento ai diritti.

Se la società è sui *social network*, tecnologie che possano alterare il flusso di comunicazioni sui *social network* possono condizionare direttamente le persone e incidere sui loro percorsi di scelta.

Anche l'attività politica, che ora è sui *social network* e ha cominciato a fare a meno, in molte occasioni, dei *media* tradizionali, ne può essere condizionata. Nel bene o nel male.

Nel quadro attuale, e per portare a unità tutto quanto detto poco sopra, si possono individuare almeno dieci possibili minacce agli equilibri democratici ad esempio, nei seguenti punti che ci permettiamo di rilevare:

i) nella creazione e condivisione di bufale e *fake news*, soprattutto volte a colpire i politici per minare il loro rapporto di fiducia con i cittadini. Il "drogare" le notizie incide direttamente sull'assetto democratico di una società, e se la diffusione avviene con metodi automatizzati – intelligenza artificiale e bot – il potenziale di danno è ancora maggiore;

ii) nell'uso di profili finti e *bot* che inquinano la politica e che possano manipolare (o, addirittura, decidere) le elezioni. Se non si distingue più tra ciò che è falso e ciò che è vero, tra chi è presente di persona a fare una campagna elettorale sui social network e chi, invece, guida un esercito di robot, le libertà democratiche sono a rischio;

- iii) nella diffusione di contenuti aggressivi o d'odio, sia al fine di raccogliere consensi (utilizzando l'odio come una "valuta"), sia al fine di attaccare gli avversari;
- iv) nell'usare la potenza dei *social network* per creare un "effetto gregge", tramite messaggi semplici e immediati, distorcendo la realtà sociale e politica;
- v) nel manipolare il mercato del consenso e nel condizionare la libertà di formazione del voto nel cittadino, anche con un'attività di profilazione psicologica molto invasiva;
- vi) nel filtrare le notizie sino a deformarle;
- vii) nel pensare ogni giorno a un consenso *relativo e immediato*, e non al consenso assoluto in una prospettiva sul lungo periodo;
- viii) nel creare una "democrazia bonsai", dove la regola diventa il relazionarsi solo con chi la pensa come me¹⁶;
- ix) nella brutalizzazione del dissenso;
- x) nel delegare i propri *follower* a prendere le scelte, vagliando in ogni momento il loro *sentiment* e basando le scelte sul pollice dei *like*.

In conclusione, il tema delle *fake news*, nella sua interdisciplinarietà, costringe lo studioso ad approcciare il fenomeno unendo nozioni di geopolitica, informatica, diritto, psicologia, marketing e storia. A nostro modesto ma fermo avviso, l'aspetto tecnologico è centrale, e l'approccio informatico-giuridico consente di unire al meglio la "tradizione", ossia concetti e principi che non sono mutati negli ultimi anni, con la novità di un mezzo e di piattaforme che consentono una diffusione su larga scala, una amplificazione del messaggio e, soprattutto, una viralità nella diffusione che non esistevano anche soltanto dieci anni orsono.

¹⁶ La locuzione "democrazia bonsai" è stata usata da Marco Minniti nel corso di un'intervista ("Liberare la politica dal cappio letale dei social network") nella quale si discuteva dell'impatto dei social network sulle libertà democratiche. In Internet all'indirizzo <<https://www.ilfoglio.it/politica/2017/11/17/news/liberare-la-politica-dal-cappio-letale-dei-social-network-intervista-a-marco-minniti-163916/>>.