Geopolitica.info

CYBER E TECH

Il trolling politico al servizio degli Stati

I casi di Russia, Cina e Turchia

A cura di *Alessia Bevilacqua*
Coordinamento di *Lorenzo Riggi*

11 GENNAIO 2022

Negli ultimi anni, il termine trolling è diventato molto popolare nell'uso, per riferirsi alla pubblicazione online di contenuti provocatori o offensivi. Oggi, però, il trolling non riguarda solo la pubblicazione di messaggi di odio da parte dei singoli utenti, ma è entrato a far parte della strategia politica di governi e candidati politici in tutto il mondo per orientare le emozioni politiche in rete e manipolare l'opinione pubblica. L'obiettivo di questo report è quello di analizzare questo fenomeno e il modo in cui gli Stati lo utilizzano concretamente, delineando le sue implicazioni.

Geopolitical Brief n. 33/ Gennaio 2022
Centro Studi Geopolitica.info | www.geopolitica.info | centrostudi@geopolitica.info
Direttore responsabile: Lorenzo Riggi

Introduzione

Internet e le nuove applicazioni del web sono diventate oggi strumenti essenziali nel contesto politico. In particolare, i social media hanno assunto un ruolo importante, non solo divenendo uno dei principali canali di informazione, ma ricoprendo anche una funzione politica cruciale in diversi eventi internazionali che hanno segnato il campo delle scienze politiche e sociali: si pensi per esempio alla campagna elettorale di Barack Obama nel 2008, alle sollevazioni popolari della Primavera Araba nel corso del 2011 o alla campagna elettorale su WhatsApp di Jair Bolsonaro per le elezioni presidenziali brasiliane nell'ottobre 2018.

La rilevanza assunta da queste piattaforme informative[1] dipende in larga misura dalle enormi quantità di dati personali che sono in grado di catturare mediando le interazioni degli utenti e dagli effetti di questa mediazione sullo stato emotivo della popolazione e sulle opinioni pubbliche nazionali.[2] Infatti, l'elevata quantità di informazioni personali custodite nei server delle *Internet companies* consente a queste ultime di elaborare, attraverso software e algoritmi di *data mining*, profili molto dettagliati dei propri utenti e, talvolta, accurati modelli di comportamento. Attraverso operazioni di profila-

[1] Oggi Internet è dominata da un numero molto limitato di attori, i cosiddetti GAFAM (Google, Apple, Facebook, Amazon e Microsoft), che detengono il dominio del mercato digitale, formando un oligopolio globale che gestisce la totalità delle infrastrutture software e hardware necessarie per la distribuzione di contenuti e servizi agli utenti di Internet. (Smyrnaios, N., 2016, "The GAFAM effect: Strategies and logics of the internet oligopoly", in *Communication & Languages*, vol. 188, issue 2, p. 61).

[2] Santaniello, M., 2018, *Internet Public Policy. Politiche pubbliche e governance delle reti digitali*, Aracne editrice, Roma, p. 22.

zione, targhettizzazione e personalizzazione dei messaggi, queste piattaforme sono in grado di creare contenuti ad hoc da distribuire ai singoli utenti, influenzandone il comportamento. Come sottolineato da Mauro Santaniello: «Internet è rapidamente diventata un'infrastruttura indispensabile per le attività politiche, economiche e sociali del sistema-mondo contemporaneo. Il controllo dei meccanismi di funzionamento della rete, a livello internazionale, nazionale e locale, si traduce in una notevole capacità di condizionamento sull'agire individuale e collettivo, e rappresenta una fonte di potere pervasivo e trasversale».[3]

La rete e le tecnologie a essa collegate diventano «il terreno privilegiato delle lotte per il controllo dell'informazione e dei dati, ovvero della *conoscenza digitale* alla quale si lega ormai indissolubilmente qualsiasi forma di egemonia geopolitica – tanto locale che globale».[4]

Sebbene queste tecnologie abbiano creato nuove opportunità, hanno anche introdotto nuove sfide: operazioni di influenza straniera, campagne di disinformazione, trolling politico, ecc. minano non solo la sicurezza dell'ambiente digitale, ma hanno anche ripercussioni e conseguenze reali nello scenario politico nazionale e internazionale degli Stati.

L'obiettivo di questo report è far luce su questi fenomeni, soprattutto sul *trolling* politico e le sue implicazioni, e sul modo in cui gli Stati e i vari attori politici lo utilizzano concretamente.

---

3 Ibidem, pp. 22-23.

4 Sordi, P., e Fiormonte, D., 2019, "Geopolitica della conoscenza digitale. Dal web aperto all'impero di GAFAM", in *DigitCult, Scientific Journal on Digital Cultures*, vol. 4, issue 1, p. 22.

I troll e il trolling online

Si definiscono *troll* gli utenti di Internet che nelle comunità online, perlopiù in maniera anonima, lasciano deliberatamente commenti crudeli e offensivi, pubblicando contenuti provocatori con l'obiettivo di ingannare, scioccare, offendere e generare controversie.

I primi riferimenti all'uso del termine *troll* sono presenti nell'archivio Usenet[5] e risalgono agli anni Ottanta: i primi "esemplari" di *troll* nascono come *flamer*[6] nei newsgroup di Usenet, aumentando man mano in intensità e organizzazione. Se inizialmente le azioni di disturbo erano legate a discussioni o argomenti specifici, successivamente i messaggi – e gli insulti – diventano fini a sé stessi e hanno il solo scopo di disturbare e gettare scompiglio nella comunità di Usenet.[7] Gli utenti dei newsgroup pensavano di avere il diritto di postare qualsiasi cosa: attraverso commenti sessisti, omofobi, razzisti e altro materiale offensivo, gli utenti/*troll* postavano principalmente per disturbare, per divertimento e per cerca-

[5] Nata negli Stati Uniti all'inizio degli anni '80, Usenet è una rete mondiale composta da migliaia di server interconnessi, che partecipano allo scambio di messaggi contenuti nei cosiddetti newsgroup o gruppi di discussione, accessibili pubblicamente, in cui gli utenti possono discutere dei più svariati argomenti.

[6] Nel gergo delle comunità virtuali di Internet, il *flaming* – letteralmente "in fiamme" – si riferisce all'atto di inviare e postare, su piattaforme che prevedono un confronto diretto, messaggi deliberatamente ostili e offensivi tra utenti.

[7] Come riportato dall'Oxford English Dictionary, è nel 1992 che il termine *trolling* viene usato per la prima con un significato affine a quello attuale: un utente pubblica all'interno del gruppo *alt.folklore.urban* il messaggio «Magari dopo che l'ho postato, possiamo continuare a *trollare* ancora un po' e vedere che succede.» (https://www.oed.com/view/Entry/206615?rskey=7NtmDl&result=3#eid, consultato il 20/04/2021).

re di controllare i "loro" spazi virtuali.[8] Era quindi fondamentale mantenere l'anonimato per interagire con gli altri e proteggersi da eventuali accuse e condanne: chiunque poteva essere un *troll*. E il *trolling* dell'Usenet non era esclusivamente un'attività in solitaria, ma poteva organizzarsi in gruppi attraverso cui attaccare insieme altri utenti.

Con il Web 2.0 c'è stata un'ulteriore evoluzione del fenomeno: l'accesso alle molteplici applicazioni online ha permesso un'elevata reciprocità tra rete e utente, facilitando la creazione, la pubblicazione e la condivisione di contenuti e consentendo anche agli utenti con scarse conoscenze tecniche di poter costruire e condividere i propri prodotti multimediali e informativi, ad esempio sui siti web di social network, anche in tempo reale.[9]

4Chan: origini e diffusione del trolling

È soprattutto dal 2003, quando Christopher Poole crea *4chan* –[10] una *imageboard*, ovvero una piattaforma online basata sulla pubblicazione da parte degli utenti di contenuti, soprattutto immagini, su cui discutere – che il fenomeno del *trolling* cresce sia in termini di dimensioni che di complessità. In questi luoghi virtuali, gli utenti, comportandosi volutamente da *troll*, possono postare e commentare in forma del tutto anonima qualsiasi tipo di materiale, principalmente di natura molto offensiva. Nel tempo si sono sviluppate diverse *board* all'interno della piattaforma, ognuna incentrata su un

[8] Dynel, M., 2016, ""Trolling is not stupid": Internet trolling as the art of deception serving entertainment", in *Intercultural Pragmatics*, De Gruyter Mouton, vol. 13, n. 3, pp. 353-381.

[9] Harrison, T. M., e Barthel, B., 2009, "Wielding new media in Web 2.0: exploring the history of engagement with the collaborative construction of media products", in *New Media and Society*, vol. 11, n. 1-2, pp. 155-178.

[10] https://4chan.org/

argomento specifico: dai videogames al fitness, dalla politica ai contenuti più dissacranti. Se inizialmente *meme*, immagini, ecc., prodotti all'interno delle *imageboard* erano esclusiva di *4chan* e simili, con lo sviluppo dei social network tutti questi materiali hanno iniziato ad essere condivisi da chiunque su altre piattaforme più note, come Facebook e Twitter, crescendo in popolarità.

All'inizio, quindi, il *trolling* era un'attività che veniva svolta *for the lulz*, ovvero per divertimento, oggi invece non coinvolge più solo i singoli cittadini ma è entrato a far parte della strategia politica di governi e candidati politici in tutto il mondo, e riguarda non solo la pubblicazione di messaggi di odio online, ma fa riferimento a una pratica più ampia, centrale per articolare e orientare le emozioni politiche in rete e manipolare l'opinione pubblica.

Propaganda computazionale e cyber troop

L'avvento di Internet e il cambiamento radicale della natura stessa dell'informazione – in termini di velocità, volume e diversità – hanno posto sfide inedite agli Stati e al modo in cui esercitare il controllo sulle informazioni: dall'adozione di approcci offensivi con l'obiettivo di limitare l'accesso non solo a determinate informazioni online ma anche, in alcuni casi, a Internet stesso, alla consapevolezza che le informazioni diffuse online rappresentano una forma di potere da cui trarre profitto.[11] Gli Stati possono utilizzare le nuove tecnologie

[11] Monaco, N., e Nyst, C., 2018, *STATE-SPONSORED TROLLING. How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns*, Institute for the Future, IFTF Digital Intelligence Lab, p. 8.

dell'informazione per il consolidamento del potere e del controllo sociale, per alimentare operazioni di disinformazione e diffondere la propaganda di governo su una scala molto più ampia.

La democrazia e la crisi dei media tradizionali

Favoriti dal calo della fiducia nei media tradizionali e dalla proliferazione di nuove piattaforme mediatiche, i governi sono sempre più coinvolti nella generazione e nel controllo dell'informazione: «il nuovo panorama politico digitale è quello in cui lo Stato stesso pianta i semi della sfiducia verso i media, fertilizza teorie cospirazioniste e falsità, e raccoglie la disinformazione derivante per servire i propri fini».[12] Fini che sono principalmente politici: Freedom House – un'organizzazione internazionale indipendente che monitora l'espansione della libertà nel mondo e conduce attività di ricerca e sensibilizzazione su democrazia, diritti umani e libertà politiche – in una serie di report[13] relativi al periodo compreso tra il 2016 e il 2019 ha evidenziato come i governi di tutto il mondo abbiano notevolmente aumentato gli sforzi per manipolare le informazioni sui social media; come queste pratiche abbiano svolto un ruolo importante durante i processi elettorali per distorcere il panorama dei media e costruire il consenso popolare a favore delle politiche di governo; e come le tattiche di manipolazione e disinformazione siano diventate tecnicamente più sofisticate grazie all'impiego di nuove tecnologie digitali.

12 Ibidem.

13 Kelly, S. et al., 2017, *Freedom on the Net: Manipulating Social Media to Undermine Democracy*, Freedom House; Shahbaz, A., 2018, *Freedom on the Net: The Rise of Digital Authoritarianism*, Freedom House; Shahbaz, A., e Funk, A., 2019, *Freedom on the Net: The Crisis of Social Media*, Freedom House.

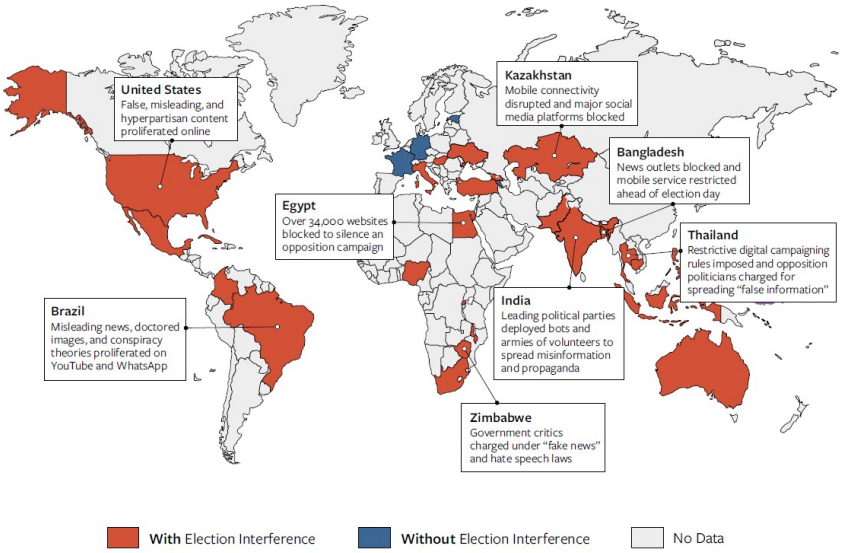

Fig. 1: Il fenomeno globale dell'interferenza e della manipolazione digitale durante elezioni o referendum. Dall'analisi condotta da Freedom House, in 26 paesi su 30 sono state adottate tattiche di manipolazione e disinformazione online durante elezioni o referendum nel periodo considerato (2016-2019).

(Fonte: Shahbaz, A., e Funk, A., 2019, *Freedom on the Net: The Crisis of Social Media*, Freedom House)

Attraverso una sorta di strategia dell'abbondanza di informazioni, gli Stati sfruttano l'attuale ecosistema digitale e la "viralità" e la familiarità dei social media per amplificare e diffondere i loro messaggi politici e sociali.

L'influenza dei social media

Sebbene la manipolazione delle informazioni e la propaganda non siano affatto fenomeni nuovi, occorre evidenziare come negli ultimi anni l'avvento dei social media e lo sviluppo di nuove tecnologie digitali sempre più complesse e pervasive li abbiano profondamente cambiati. Gli eventi politici succedutisi dal 2016 (il referendum sulla Brexit, le elezioni presidenziali statunitensi del 2016, le elezioni presidenziali francesi del 2017, ecc.) sono emblematici del fatto che le tat-

tiche di manipolazione e propaganda, grazie all'impiego di nuove tecnologie digitali, diventano sempre più sofisticate tecnicamente, ben organizzate e più in grado di influenzare i processi politici interni o esteri.

A questo proposito, è stato introdotto il concetto di "propaganda computazionale", ovvero l'uso di algoritmi, automazione e big data per apprendere e simulare il comportamento umano, diffondere intenzionalmente informazioni fuorvianti, modellare e manipolare il discorso pubblico.[14]

Gli attori impiegati a questi fini sono stati definiti *cyber troop*, truppe informatiche, e sono agenzie governative, militari o partiti politici che utilizzano la propaganda computazionale per influenzare l'atteggiamento dell'opinione pubblica e diffondere le loro idee politiche.[15] Queste *cyber troop* sono spesso costituite da un assortimento di attori diversi.[16] In alcuni casi, i governi hanno dei team interni: individui, che spesso fanno parte dell'amministrazione governativa, impiegati dallo Stato come dipendenti pubblici. In altri, le *cyber troop* possono essere: privati assunti dal governo per un periodo di tempo limitato e per una missione o una causa specifiche; gruppi di volontari che collaborano attivamente con il governo per diffonderne l'ideologia politica attraverso messaggi fi-

[14] Woolley, S.C., e Howard, P.N., 2016, "Political Communication, Computational Propaganda, and Autonomous Agents. Introduction", in *International Journal of Communication*, vol. 10, p. 4886; Woolley, S.C, e Howard, P.N., 2017, "Computational Propaganda Worldwide: Executive Summary", in *The Computational Propaganda Research Project*, Oxford Internet Institute, University of Oxford, Regno Unito, p. 6.

[15] Bradshaw, S., e Howard, P.N., 2017, "Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation", in *The Computational Propaganda Research Project*, Oxford Internet Institute, University of Oxford, Regno Unito, p. 4.

[16] Ibidem, pp. 15-16.

logovernativi; cittadini reclutati dal governo – di solito scelti perché detengono una posizione di rilievo nella società o online – che vengono pagati per il loro lavoro ma non sono né funzionari pubblici ufficiali, né impiegati di un'azienda privata. Dal momento che questi cittadini non sono ufficialmente affiliati al governo o a un partito politico, la loro voce "indipendente" può essere utilizzata per diffondere messaggi politici da un'apparente prospettiva neutrale.

Le cyber troop e la propaganda computazionale

Tra le strategie e le tecniche delle *cyber troop* vi è l'impiego di algoritmi, ovvero «procedure in operazioni o calcoli computazionali».[17] Piattaforme online come Google, Facebook e Twitter utilizzano gli algoritmi per prevedere ciò a cui gli utenti sono interessati e stimolarne il coinvolgimento: poiché gli utenti tendono ad essere coinvolti maggiormente dai contenuti che generano in loro una reazione emotiva e/o che confermano pregiudizi e idee già esistenti, gli algoritmi filtrano e ordinano – analizzando le abitudini online, la cronologia dei clic, le condivisioni e i "Mi piace" – i contenuti che l'utente riceve, dando priorità a quelli che più rispecchiano le sue preferenze. Questo può spingere gli utenti all'interno di *echo chamber*,[18] contribuendo alla polarizzazione politica.

[17] Bentzen, N., 2018, "Computational propaganda techniques", in *European Parliamentary Research Service (EPRS)*, Parlamento Europeo.

[18] Le echo chamber o "camere dell'eco" sono «degli ambienti virtuali che si creano all'interno di una piattaforma di condivisione online, in cui un utente si trova a visualizzare prevalentemente contenuti coerenti con le sue convinzioni e ideologie, e ad interagire maggiormente con altri utenti che condividono le sue stesse opinioni» (D'Auria, F., marzo 2021, "Echo chambers. Gli algoritmi dei social influenzano la nostra esperienza online", in *Il Bo Live UniPD*, https://ilbolive.unipd.it/it/news/echo-chambers-algoritmi-social-influenzano-nostra (consultato il 20/04/2021). Insieme alla cosiddetta "bolla di filtraggio" relativa alla personalizzazione dei risultati delle ricerche, le echo chamber favorirebbero bias cognitivi di conferma, polarizzazioni ed estremizzazioni.

A questo proposito, risulta emblematico il caso dello scandalo Cambridge Analytica, che tra marzo e aprile del 2018 ha occupato le prime pagine di quotidiani, servizi di telegiornali e articoli online. Cambridge Analytica – azienda di consulenza e marketing online specializzata nella raccolta di dati e informazioni dai social media sulle abitudini e i consumi dei loro utenti attraverso i "Mi piace", i commenti, i tweet, ecc. – non solo avrebbe usato in maniera scorretta un'enorme quantità di dati prelevati da Facebook per creare profili psicologici degli utenti da usare in campagne di marketing super mirate (*micro-targeting*), ma avrebbe avuto anche un ruolo dirimente nel condizionare le elezioni presidenziali statunitensi del 2016 – intrattenendo importanti rapporti con alcuni dei più stretti collaboratori di Donald Trump, soprattutto durante la campagna elettorale – e il referendum sulla Brexit nel Regno Unito, influenzando e mobilitando gli elettori.[19]

Bot, Fake account e Cyborg

Fake account, ovvero profili falsi sui social media, vengono utilizzati per diffondere messaggi pro-governo o pro-partito sia a livello nazionale che all'estero. Questi account possono essere di tre tipologie: *bot*, umani e *cyborg*.[20] I *bot* – abbreviazione di robot – sono account automatici controllati da algoritmi di intelligenza artificiale, progettati e programmati per analizzare, comprendere e imitare il comportamento umano online e interagire come veri utenti. Sono spesso usati per

[19] Manietti, E., marzo 2018, "Il caso Cambridge Analytica, spiegato bene", in *Il Post*, https://www.ilpost.it/2018/03/19/facebook-cambridge-analytica/ (consultato il 15/04/2020).

[20] Bradshaw, S., e Howard, P.N., 2019, "The Global Disinformation Order. 2019 Global Inventory of Organized Social Media Manipulation", in *The Computational Propaganda Research Project*, Oxford Internet Institute, University of Oxford, Regno Unito, p. 11.

diffondere *fake news* e disinformazione online, amplificare messaggi propagandistici e, soprattutto durante elezioni e referendum, produrre un falso senso di popolarità e consenso per una determinata parte politica (il cosiddetto *astroturfing*).[21] Ad esempio, durante le elezioni presidenziali francesi del 2017 sono state trovate prove dell'impiego di *bot* che erano già stati utilizzati nelle elezioni statunitensi per diffondere contenuti pro-Trump nel 2016: questo indicherebbe l'esistenza di un mercato[22] nero di *bot* politici riutilizzabili.[23]

Ci sono poi account gestiti da individui che non utilizzano l'automazione: si tratta di operatori umani, spesso in team coordinati, che gestiscono manualmente un insieme di account falsi attraverso cui interagiscono sui social media, pubblicando commenti, tweet, ecc., per influenzare il dibattito online. Infine, i *cyborg* sono account che combinano l'automazione (per guidare il volume e la velocità delle attività) con l'intervento umano: attraverso elementi di autentica interazione umana si cerca di far sembrare questi account dei profili veri.

Oltre agli account falsi, vi è anche il caso di account compromessi o rubati: alcuni attori statali (tra cui Corea del Nord,

---

21 Ibidem; Bradshaw, S., e Howard, P.N., 2018, "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation", in *The Computational Propaganda Research Project*, Oxford Internet Institute, University of Oxford, pp. 11-12.

22 A questo proposito, uno studio condotto dal Centro di Eccellenza NATO per le Comunicazioni Strategiche (NATO StratCom COE) ha analizzato il mercato online relativo a strumenti e servizi di manipolazione dei social media, evidenziando l'esistenza di un mercato nero fiorente in cui acquirenti e venditori si incontrano per scambiare account, clic, "Mi piace" e condivisioni (NATO StratCom COE Singularex, 2018, *The black market for social media manipulation*, NATO StratCom COE, Riga).

23 Bentzen, N., *Op. cit*.

Russia e Iran) hanno iniziato ad utilizzare account di alto profilo rubati o hackerati nell'ambito delle loro campagne per diffondere propaganda filogovernativa o censurare la libertà di parola, impedendo l'accesso all'account del legittimo proprietario.[24] Ciò evidenzia l'interconnettività della propaganda computazionale con forme più tradizionali di attacchi informatici.

Il ruolo dei troll

Infine, un ruolo significativo è svolto dai *troll*. Questi non solo rappresentano importanti fonti per la creazione di *meme*, *fake news*, teorie cospirazioniste, ecc., per supportare una campagna di manipolazione più ampia, ma possono anche essere utilizzati sistematicamente – sia nel contesto delle elezioni sia come strumento di controllo sociale nei regimi autoritari – per attaccare, perseguitare e prendere di mira individui, comunità o organizzazioni che esprimono opinioni discordanti e dissenso politico, attraverso varie forme di molestie online, incitamento all'odio, ecc.[25] Infatti, «la forma più potente di propaganda computazionale prevede sia una distribuzione algoritmica che l'intervento editoriale umano – bot e troll che lavorano insieme».[26]

Uno studio del 2020 sottolinea come l'impiego di propaganda computazionale e di altre strategie di manipolazione delle informazioni da parte degli Stati sia notevolmente aumentato: da 28 paesi nel 2017 a 70 nel 2019 e 81 nel 2020.[27] Inol-

[24] Bradshaw, S., e Howard, P.N., 2019, "The Global Disinformation Order. 2019 Global Inventory of Organized Social Media Manipulation", *Op. cit.*, pp. 11-12.

[25] Bentzen, N., *Op. cit.*; Bradshaw, S., e Howard, P.N., ibidem, p. 1 e 11.

[26] Woolley, S.C, e Howard, P.N., 2017, "Computational Propaganda Worldwide: Executive Summary", *Op. cit.*, p. 5.

[27] Bradshaw, S., Bailey, H., e Howard, P.N., 2021, "Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipu-

tre: in ogni Paese vi è almeno un partito politico o un'agenzia governativa che utilizza i social media per modellare gli atteggiamenti pubblici a livello nazionale; in 26 Paesi, principalmente regimi autoritari, la propaganda computazionale è strategicamente utilizzata come strumento di controllo delle informazioni insieme a sorveglianza, censura e minacce di violenza; un certo numero di attori statali (tra cui Russia, Cina, India e Arabia Saudita) impiega la propaganda computazionale per influenzare il pubblico globale.[28]

State-sponsored trolling

Si parla così di *state-sponsored trolling*,[29] ovvero *trolling* promosso e finanziato direttamente dagli Stati o da partiti politici che, combinando disinformazione, *fake news*, propaganda computazionale, *bot*, *meme*, ecc., viene impiegato per condizionare il dibattito pubblico, esercitare un'influenza politica e sociale, diffondere la propaganda di governo e condurre campagne mirate di odio e molestie online contro chi è percepito come una minaccia al potere statale. Una pratica divenuta anche uno strumento utile di *information warfare*,[30] at-

lation", in *The Computational Propaganda Research Project*, Oxford Internet Institute, University of Oxford, Regno Unito, Working Paper 2021.

28 Bradshaw, S., e Howard, P.N., 2019, "The Global Disinformation Order. 2019 Global Inventory of Organized Social Media Manipulation", *Op. cit*.

29 Monaco, N., e Nyst, C., 2018, *Op. cit*.

30 Negli ultimi dieci anni, le piattaforme online sono rapidamente diventate uno dei principali canali di comunicazione e informazione e parte integrante delle strategie di guerra, attraverso cui coordinare azioni, raccogliere informazioni e, soprattutto, influenzare le credenze e gli atteggiamenti del pubblico target, mobilitandolo persino all'azione: ciò ha portato ad un ampliamento del concetto di *information warfare*, ovvero "guerra dell'informazione", unitamente all'introduzione del concetto di *psychological warfare*. Inoltre, il settore privato, inclusi i giganti di Internet come Facebook, Twitter e Google, ha agito non solo come sviluppatore e fornitore di tecnologia, ma anche come operatore strategico nella competizione per l'informazione e il potere (NATO Strategic Communications Centre of Excellence, 2016, *Social Media as a Tool of Hybrid Warfare*, NATO StratCom COE, Riga, p. 4.; Nis-

traverso cui gli Stati possono perseguire specifici obiettivi politici e militari anche a livello internazionale, infiltrandosi nelle agende politiche di altri Paesi. Il *trolling* può essere impiegato, infatti, come strategia che non mira a raggiungere vittorie decisive ma a colpire la credibilità e la stabilità dei governi avversari, nonché il sostegno pubblico nei loro confronti.[31] Non è mai uno strumento autonomo e isolato, ma diventa un meccanismo legato a una strategia che combina mezzi e tecniche diverse per raggiungere specifici obiettivi politici e militari. Per esempio, i *bot* possono essere utilizzati per creare in modo computazionale grandi quantità di post con lo scopo di amplificare punti di vista controversi, provocare divisioni e produrre un falso senso di popolarità e consenso su questioni o individui; pagine di *fake news* possono disseminare notizie false, teorie cospirazioniste, ecc., per creare confusione, polemiche e resistenza alla leadership politica; eserciti di *troll* e account falsi possono infiltrarsi nel discorso politico, creare disinformazione, diffondere messaggi propagandistici, produrre divisioni e polarizzazione, condurre campagne mirate di odio e molestie online.[32]

Si possono individuare numerosi esempi di questo fenomeno: uno studio di Freedom House ha evidenziato che almeno

sen, T.E., 2015, *#The Weaponization of Social Media – @Characteristics_of_Contemporary_Conflicts*, Royal Danish Defence College, Copenhagen, p. 84; Sanger D. E., 2018, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, New York: Crown Publishers).

31 NATO StratCom COE, *Internet Trolling as a tool of Hybrid Warfare: the case of Latvia*, NATO StratCom COE, Riga, p. 14.

32 Neudert, L.M., e Marchal, N., 2019, *Polarisation and the use of technology in political campaigns and communication*, Scientific Foresight Unit (STOA), Parlamento Europeo, pp. 26-27.

30 Stati, a livello mondiale, stanno impiegando «eserciti da tastiera» con questi fini.[33]

La Russia

Le fabbriche di troll

Tra i casi più emblematici di *trolling* sponsorizzato a livello statale c'è la Russia e le sue famose "fabbriche di *troll*".

Tra il 2013 e il 2015, dopo fughe di notizie e una serie di inchieste investigative condotte da giornalisti sotto copertura, è stata scoperta a San Pietroburgo l'esistenza di un edificio – soprannominato per l'appunto "fabbrica di *troll*" – in cui personale addestrato veniva impiegato in operazioni di controllo dei social media e di propaganda online a favore del presidente Vladimir Putin e contro i rivali del governo russo, sia in patria che all'estero.[34]

Si ritiene che l'ente, conosciuto con il nome di Internet Research Agency (IRA), sia una delle numerose aziende di *troll* di cui dispone il governo russo: secondo il rapporto *Assessing Russian Activities and Intentions in Recent US Elections* del gennaio 2017, effettuato dall'Intelligence degli Stati Uniti, il finanziatore dell'IRA è Yevgeny Prigozhin, uno stretto alleato di Putin con legami con l'Intelligence russa.[35]

---

33 Kelly, S. et al., 2017, *Op. cit.*, p. 8.

34 Walker, S., aprile 2015, "The Russian troll factory at the heart of the meddling allegations", in *The Guardian*, https://www.theguardian.-com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house (consultato il 09/06/2020); Chen, A., giugno 2015, "The Agency", in *The New York Times Magazine*, https://www.nytimes.com/2015/06/07/magazine/the-agency.html (consultato il 09/06/2020); Aro, J., 2016, "The cyberspace war: propaganda and trolling as warfare tools", in *European View*, vol. 15, p. 122.

35 Intelligence Community Assessment (ICA), 2017, *Assessing Russian Activities and Intentions in Recent US Elections*, Office of the Director of National Intelligence, USA, p. 4.

Secondo documenti interni rilasciati da un gruppo di hacker nel 2013,[36] l'IRA disponeva di un budget annuo di 10 milioni di dollari e impiegava più di 600 persone in tutta la Russia: ogni dipendente doveva pubblicare 50 volte al giorno articoli su notizie pro Cremlino, avere sei account Facebook con cui pubblicare almeno tre post al giorno e almeno 10 account Twitter per twittare 50 volte al giorno, con l'obiettivo di acquisire nuovi follower e aumentarne l'*engagement*.

La cyberwar nelle relazioni tra Russia e Stati Uniti

L'IRA risulterebbe inoltre al centro di ampie operazioni di influenza e campagne di manipolazione e disinformazione condotte nei confronti di altri Stati. Il già citato rapporto dell'Intelligence Statunitense ha sottolineato che questa "fabbrica di *troll*" nel 2014 è stata usata nelle operazioni a sostegno delle azioni russe durante l'occupazione della Crimea per plasmare l'opinione internazionale sull'invasione dell'Ucraina e, successivamente, a sostegno di Donald Trump durante le elezioni presidenziali del 2016, impiegando una strategia che univa operazioni segrete di intelligence – come le attività informatiche – con sforzi espliciti di agenzie governative russe, media finanziati dallo Stato, *bot* e *troll* per diffondere propaganda in favore di Trump su temi come immigrazione, religione e questioni razziali, e colpire e polarizzare gli elettori statunitensi.[37] Infatti, le attività dell'IRA sono state progettate per polarizzare il pubblico statuniten-

[36] Seddon, M., giugno 2014, "Documents Show How Russia's Troll Army Hit America", in *BuzzFeed News*, https://www.buzzfeednews.com/article/maxseddon/documents-show-how-russias-troll-army-hit-america#.jnn07ep33 (consultato il 09/06/2020).

[37] Howard, P.N., et al., "The IRA, Social Media and Political Polarization in the United States, 2012-2018", in *The Computational Propaganda Research Project*, Oxford Internet Institute, University of Oxford, Regno Unito, pp. 32-34.

se, lanciando molteplici campagne destinate a diversi segmenti di utenti: attraverso il *targeting* per interesse e posizione, ogni annuncio cercava di attirare gli utenti sulle pagine Facebook o Instagram corrispondenti, gestite dallo staff dell'IRA e contenenti slogan, *fake news*, *meme*, notizie sensazionalistiche e teorie cospirazioniste sugli argomenti più disparati.[38] Questi messaggi personalizzati hanno esposto gli utenti statunitensi a una vasta gamma di notizie di disinformazione, progettate per suscitare indignazione e cinismo.

L'influenza russa in Europa

La Russia avrebbe intrapreso misure simili per influenzare le campagne politiche di una vasta gamma di Paesi europei: il referendum sulla Brexit in Gran Bretagna nel 2016, sostenendo il "Leave";[39] le elezioni presidenziali francesi del 2017, supportando la candidata di estrema destra Marine Le Pen;[40] il referendum sull'indipendenza della Catalogna in Spagna nel 2017, a sostegno della secessione catalana;[41] le

38 Shane, S., settembre 2017, "The Fake Americans Russia Created to Influence the Election", in *The NewYork Times*, https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html (consultato il 10/06/2020).

39 "Disinformation and 'Fake News': Interim Report", in *UK Parliament*, luglio 2018, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36308.htm#_idTextAnchor033 (consultato il 13/06/2020); Quinn, B., febbraio 2018, "Social media firms must tell users exposed to Brexit propaganda, MP says", in *The Guardian*, https://www.theguardian.com/uk-news/2018/feb/10/social-media-firms-must-tell-users-impacted-by-propaganda-mp-says?CMP=share_btn_tw (consultato il 13/06/2020).

40 Willsher, K., e Henley, J., maggio 2017, "Emmanuel Macron's campaign hacked on eve of French election", in *The Guardian*, https://www.theguardian.com/world/2017/may/06/emmanuel-macron-targeted-by-hackers-on-eve-of-french-election (consultato il 13/06/2020); Gatehouse, G., aprile 2017, "Marine Le Pen: Who's funding France's far right?", in *BBC News*, https://www.bbc.com/news/world-europe-39478066 (consultato il 13/06/2020).

41 Alandete, D., ottobre 2017, "Pro-Russian networks see 2,000% increase in activity in favor of Catalan referendum", in *EL PAÍS*, https://english.elpais.com/elpais/2017/10/01/inenglish/1506854868_900501.html (consultato il 13/06/2020).

elezioni parlamentari in Germania del 2017, dando il proprio supporto al partito di estrema destra Alternativa per la Germania per fargli ottenere più voti, e probabilmente le elezioni parlamentari in Italia del 2018.[42]

Le campagne di influenza russe non riguardano solo l'Occidente: recentemente si è scoperto che la Russia avrebbe dato vita ad almeno tre campagne di disinformazione in Africa, diffondendo *fake news* in otto Paesi africani, tra i quali Libia e Sudan.[43] Secondo alcuni esperti, la Russia avrebbe scelto l'Africa per sperimentare nuove tecniche di disinformazione con l'obiettivo di rendere queste operazioni di manipolazione ancora più difficili da scoprire.

Da parte sua la Russia ha sempre negato qualsiasi tentativo di influenzare e manipolare gli affari interni americani e degli altri Stati.[44] Dopo le accuse di ingerenza nelle elezioni

---

42 Biden, J.R., e Carpenter, M., gennaio/febbraio 2018, "How to Stand Up to the Kremlin. Defending Democracy Against Its Enemies", in *Foreign Affairs*, https://www.foreignaffairs.com/articles/russia-fsu/2017-12-05/how-stand-kremlin?cid=int-fls&pgtype=hpg (consultato il 13/06/2020).

43 Alba, D., e Frenkel, S., ottobre 2019, "Russia Tests New Disinformation Tactics in Africa to Expand Influence", in *The New York Times*, https://www.nytimes.com/2019/10/30/technology/russia-facebook-disinformation-africa.amp.html (consultato il 13/06/2020); Ilyushina, M., novembre 2019, "Russia's 'troll factory' is alive and well in Africa", in *CNN*, https://edition.cnn.com/2019/10/31/europe/russia-africa-propaganda-intl/index.html (consultato il 13/06/2020).

44 Micalessin, G., marzo 2019, "Russiagate, una bufala che ha messo a rischio la pace", in *Sputnik Italia*, https://it.sputniknews.com/20190325/Russiagate-una-bufala-che-ha-messo-a-rischio-la-pace-7455795.html (consultato il 26/07/2021); Osborn, A., e Stubbs, J., febbraio 2018, "Kremlin says charges over U.S. election tampering prove nothing", in *Reuters*, https://www.reuters.com/article/usa-trump-russia-kremlin-idINKCN1G30Y1 (consultato il 26/07/2021); Geydarova, A., marzo 2021, "Russian Embassy Slams US Intel Accusations Against Moscow of Election Meddling as Groundless", in *Sputnik International*, https://sputniknews.com/20210317/russian-embassy-in-washington-us-intel-accusations-against-russia-of-election-meddling-groundless-1082364742.html (consultato il 26/07/2021).

americane del 2016, il Ministro degli Esteri russo Sergei Lavrov aveva bollato come "chiacchiere" queste insinuazioni, mentre il portavoce del Cremlino Dmitrij Peskov, commentando i risultati dell'indagine del consigliere speciale americano Robert Mueller sulla questione, affermava che «le accuse che continuano a essere mosse contro la Russia sono assolutamente infondate», e che «la parte pubblicata del rapporto di Mueller non contiene nulla di nuovo a sostegno delle accuse di ingerenza russa nelle elezioni statunitensi, solo il riconoscimento dell'assenza di qualsiasi collusione», sottolineando come fossero «tentativi assurdi di demonizzare la Russia e distogliere l'attenzione da casi reali di frode e corruzione politica *[interna agli Stati Uniti]*».[45] Per quanto riguarda le accuse di interferenza negli affari di Washington e nelle elezioni europee, il Presidente Putin le ha respinte con forza, sottolineando come fossero una provocazione da parte di poteri esterni e, citandolo, che «Non ci viene nemmeno in mente di immischiarci in nessuna elezione»,[46] e che «non importa quello che dico, alcuni dei nostri partner si aggrapperanno a qualsiasi cosa pur di dimostrare la presunta interferenza della Russia».[47]

---

45 Isachenkov, V., e Charlton, A, gennaio 2018, "Russia dismisses Democratic US Senate report as unfounded", in *AP News*, https://apnews.com/article/moscow-north-america-ap-top-news-elections-international-news-75e990e3de934b86ac8f42c3fdde3ac3 (consultato il 26/07/2021); "Russia dismisses US report as 'unfounded'", in *China Daily*, gennaio 2018, https://global.chinadaily.com.cn/a/201801/13/WS5a596ad2a3102c394518ef75.html (consultato il 26/07/2021).

46 Isachenkov, V., e Charlton, A, *Op. cit*.

47 "Putin on Us Election: No Matter What I Say Partners Will Accuse Us of Meddling", in *Sputnik International*, ottobre 2020, https://sputniknews.com/20201029/putin-on-us-election-no-matter-what-i-say-partners-will-accuse-us-of-meddling-1080914854.html (consultato il 26/07/2021).

La Cina

L'esercito dei 50 centesimi

Si ritiene che anche il governo cinese gestisca un esercito da tastiera conosciuto con il nome di "esercito dei 50 centesimi" che impiegherebbe oltre 2 milioni di persone – per lo più già dipendenti del governo – per sostenere il regime online, diffondere propaganda filogovernativa e manipolare l'opinione pubblica.[48]

Il primo riferimento a questi "impiegati" è apparso nell'ottobre 2004, in un rapporto ufficiale relativo all'assunzione, da parte del Partito Comunista Cinese (PCC) di Changsha, nella provincia dell'Hunan, di una squadra di commentatori di Internet, i quali avrebbero ricevuto uno stipendio mensile di base di 600 CNY, ovvero poco più di 50 centesimi per ogni post pubblicato (da qui il soprannome).[49]

Secondo uno studio condotto da Gary King, Jennifer Pan e Margaret Roberts,[50] i commentatori ingaggiati dal PCC diffondono all'anno circa 448 milioni di commenti, pubblicati sia su siti controllati dal governo, mascherandoli da commenti di normali cittadini, che su siti commerciali, nascondendoli tra notizie dedicate alle famiglie, foto di animali e altro. Stando ai ricercatori, la strategia adottata dal regime ci-

[48] Weiwei, A., ottobre 2012, "China's Paid Trolls: Meet the 50-Cent Party", in *NewStatesman*, https://www.newstatesman.com/politics/politics/2012/10/china%E2%80%99s-paid-trolls-meet-50-cent-party, (consultato il 20/10/2020).

[49] Han, R., 2015, "Manufacturing Consent in Cyberspace: China's "Fifty-Cent Army", in *Journal of Current Chinese Affairs*, vol. 44, n. 2, pp.105-134.

[50] King, G., Pan, J., e Roberts, M.E., 2017, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument", in *American Political Science Review*, vol. 111, n. 3, pp. 484-501.

nese per il controllo dell'informazione è quella di impiegare questi commentatori per deviare abilmente le conversazioni e inondare i "dubbiosi" con una marea di messaggi positivi sul governo. L'obiettivo di questa massiccia operazione è quello di sviare l'attenzione dell'opinione pubblica con post a sostegno del PCC e del regime, soprattutto durante i periodi di intenso dibattito online e quando proteste, discussioni o altre attività in rete potrebbero trasformarsi in azioni concrete, rappresentando un pericolo per il governo. I post riguardano principalmente la promozione di una visione positiva della Cina e del regime, con slogan ispiratori, forte patriottismo ed elogi ai funzionari del Partito, ai programmi e alle iniziative del governo; la marginalizzazione e demonizzazione di tutte le voci anti-PCC, degli oppositori di governo e di chi ha opinioni filoccidentali; schernire i Paesi stranieri, ridicolizzando soprattutto le democrazie occidentali.

Uno studio di Freedom House[51] sottolinea come negli ultimi dieci anni i funzionari del PCC abbiano incrementato notevolmente gli sforzi per influenzare il dibattito pubblico e la copertura mediatica sulla Cina al di fuori del Paese, in particolare tra le comunità cinesi all'estero, modellando i contenuti e le narrazioni dei media in tutto il mondo anche in altre lingue, e ostacolando i corrispondenti stranieri in Cina.

La continua attuazione della legge sulla sicurezza informatica del 2017, insieme ad altri regolamenti e all'aumento della pressione sulle società tecnologiche private, ha portato a una

[51] Cook, S., gennaio 2020, *Beijing's Global Megaphone: The Expansion of Chinese Communist Party Media Influence since 2017*, Freedom House Special Report.

sorveglianza e a una censura di Internet sempre più ampia e sofisticata.[52]

Infrastrutture tecnologiche e gestione delle informazioni

Il PCC mantiene il controllo sulle notizie tramite la proprietà diretta, l'accreditamento dei giornalisti e severe sanzioni contro i media e i siti che muovono critiche pubbliche al governo. La gestione statale dell'infrastruttura delle telecomunicazioni consente il blocco dei siti web, la rimozione di applicazioni per smartphone dal mercato interno e l'eliminazione di massa di post, messaggi e account utenti che affrontano argomenti politici, sociali, economici e religiosi vietati. Migliaia di siti web sono stati bloccati, comprese importanti testate giornalistiche internazionali e social media come il New York Times, il Washington Post, YouTube, Twitter e Facebook. Inoltre, il controllo è esteso anche a spazi apolitici, come piattaforme per lo streaming musicale, pagine di gossip, ecc.[53]

Pechino, inoltre, sta guadagnando una grande influenza su parti cruciali dell'infrastruttura informatica di alcuni Paesi, poiché le aziende tecnologiche cinesi con stretti legami con il PCC costruiscono o acquisiscono piattaforme di diffusione di contenuti utilizzate da decine di milioni di consumatori stranieri. In questo modo i media statali cinesi, i funzionari governativi e le società affiliate stanno acquisendo una maggiore influenza sui nodi chiave del flusso dell'informazione globale, sfruttando un ambiente tecnologico sempre più sofisticato e mostrando la propensione a prendere parte ai di-

[52] Attraverso il sistema di censura online conosciuto come *Great Firewall*, le autorità cinesi controllano, limitano e bloccano i contenuti a cui gli utenti cinesi possono accedere quando sono online.

[53] Tutte le informazioni e i dati possono essere consultati alla pagina https://freedomhouse.org/country/china/freedom-world/2020.

battiti politici interni e alle competizioni elettorali di altri Paesi.

Dal 2017, il governo cinese ha accelerato le sue campagne di influenza mediatica globale, implementando nuove tattiche sempre più coordinate, sofisticate e difficili da rilevare. Tra queste, sta acquisendo importanza l'uso di campagne di disinformazione in stile russo su piattaforme internazionali di social media – bloccate in Cina – per promuovere le narrazioni del PCC all'estero e influenzare le agende politiche di altri Paesi.

Ad esempio, il governo cinese ha influenzato le elezioni di Taiwan favorendo il candidato pro-Pechino Han Kuo-Yu, rispettivamente nel 2018 e per la presidenza di Taiwan nel 2020, impiegando i social per aumentarne la popolarità e diffondere notizie false e immagini manipolate contro il rappresentante del partito avversario.[54] Più recentemente, Pechino ha utilizzato frotte di *troll* su Twitter per screditare e mettere in cattiva luce le proteste di Hong Kong.[55] A questo proposito, nell'agosto 2019 Twitter ha annunciato di aver rimosso oltre 900 account provenienti dalla Repubblica Popolare Cinese utilizzati nella campagna di disinformazione dello Stato per minare la credibilità dei manifestanti antigover-

[54] Prasso, S., e Ellis, S., ottobre 2019, "China's Information War on Taiwan Ramps Up as Election Nears", in *Bloomberg Businessweek*, https://www.bloomberg.com/news/articles/2019-10-23/china-s-information-war-on-taiwan-ramps-up-as-election-nears (consultato il 20/10/2020); Aspinwall, N., gennaio 2020, "Taiwan's War on Fake News Is Hitting the Wrong Targets", in *Foreign Policy*, https://foreignpolicy.com/2020/01/10/taiwan-election-tsai-disinformation-china-war-fake-news-hitting-wrong-targets/ (consultato il 20/10/2020).

[55] Zhong, R., Myers, S.L., e Wu, J., settembre 2019, "How China Unleashed Twitter Trolls to Discredit Hong Kong's Protesters", in *The New York Times*, https://www.nytimes.com/interactive/2019/09/18/world/asia/hk-twitter.html (consultato il 07/06/2020).

nativi a Hong Kong, e altri 200.000 account creati successivamente.[56]

Tra le tattiche utilizzate dal regime cinese rientrano: l'uso di incentivi economici per mettere a tacere commenti negativi o opinioni contro il regime; pressioni su società tecnologiche, governi stranieri e organizzazioni internazionali per prevenire o punire la pubblicazione di contenuti contrari al PCC; minacce di azioni legali per diffamazione contro giornalisti e organi di stampa per notizie critiche sulle azioni del governo cinese; attacchi diretti dei *troll*, campagne di intimidazione, minacce, aggressioni, attacchi informatici, *denial of service*[57] e attacchi di *phishing*[58].

La Turchia

L'emergere in Turchia dei cosiddetti AKTrolls – un'organizzazione di 6000 *troll* che prende il nome dal Partito della

[56] Twitter Safety, agosto 2019, "Information operations directed at Hong Kong", in *Twitter Blog*, https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html (consultato il 20/10/2020).

[57] Il *denial of service* o "negazione/interruzione del servizio" indica un malfunzionamento causato da un attacco informatico «il cui obiettivo è ingolfare le risorse di un sistema informatico che fornisce un determinato servizio, [...] prendendo di mira server, reti di distribuzione, o data center che vengono inondati di false richieste di accesso, a cui non riescono a far fronte» (Rijtano, R., maggio 2018, "Attacco DDoS (Distributed Denial of Service): Cos'è, come fare, come difendersi", in *Cyber Security 360*, https://www.cybersecurity360.it/nuove-minacce/ddos-cosa-sono-questi-attacchi-hacker-e-come-stanno-evolvendo/ (consultato il 20/04/2021).

[58] Il *phishing* è un particolare tipo di truffa online il cui obiettivo è indurre gli utenti di Internet a rivelare informazioni personali, dati finanziari o codici di accesso, attraverso l'utilizzo di siti Web fasulli o messaggi e-mail ingannevoli che imitano aziende e marchi affidabili ("Malware Protection Center", in *Microsoft Glossary*, https://web.archive.org/web/20130305114911/http://www.microsoft.com/security/portal/threat/encyclopedia/glossary.aspx#d (consultato il 20/04/2021).

Giustizia e dello Sviluppo (AKP) –[59] si può attribuire alla reazione del partito AK in risposta all'uso massiccio dei social media da parte degli attivisti durante le proteste di Gezi Park[60] del 2013.

Se inizialmente i social media come Twitter e Facebook sono stati considerati una seria minaccia al controllo del governo a causa del libero flusso di informazioni, dopo le proteste di Gezi Park sono diventati una delle principali armi del governo.

Gli AKTrolls

L'AKP ha adottato il *trolling* politico online come una vera e propria strategia politica di controllo e manipolazione per costruire il consenso e attaccare l'opposizione. Questa strategia include anche restrizioni legali e tecniche, la regolamentazione di Internet, il blocco dell'accesso ai siti di social network, la rimozione dei contenuti, procedimenti giudiziari e detenzione per tutti gli utenti accusati di essere terroristi o di criticare e insultare il governo e i funzionari pubblici. Nel

[59] Albayrak, A., e Parkinson, J., settembre 2013, "Turkey's Government forms 6,000-Member Social Media Team", in *The Wall Street Journal*, https://www.wsj.com/articles/SB10001424127887323527004579079151479634742 (consultato il 07/10/2020).

[60] Avvenute all'inizio dell'estate del 2013 nel parco di Gezi a Istanbul, le proteste di Gezi Park sono delle manifestazioni nate inizialmente da un sit-in per contestare la proposta del piano di sviluppo urbano di rimuovere il parco a favore di un centro commerciale e appartamenti di lusso. L'uso sproporzionato della forza da parte della polizia nei riguardi dei manifestanti pacifici portò allo scoppio di manifestazioni antigovernative in tutto il Paese, represse violentemente dal governo. Durante le manifestazioni, i manifestanti hanno utilizzato i social media come strumenti fondamentali per diffondere informazioni sulle proteste, mobilitare, reclutare, coordinare e organizzare le proteste, documentare la brutalità della polizia e attirare l'attenzione della comunità internazionale in assenza del supporto dei media tradizionali (Karatas, D., e Saka, E., 2017, "Online political trolling in the context of post-Gezi social media in Turkey", in *International Journal of Digital Television*, vol. 8, n. 3, pp. 383-401).

2015, ad esempio, migliaia di utenti turchi sono stati perseguiti e detenuti con l'accusa di aver insultato il presidente Erdoğan online, in particolare su Twitter.[61] Nel luglio 2016, dopo il fallito colpo di stato, il governo, dotandosi di poteri straordinari, ha ridotto notevolmente la libertà di parola, attuando una vera e propria epurazione post-golpe: nei mesi successivi, quasi 100.000 accademici, giornalisti e attivisti sono stati licenziati o arrestati.[62] Sia nel 2016 che nel 2017, la Turchia ha incarcerato più giornalisti di qualsiasi altra nazione al mondo, continuando a effettuare nuove ondate di arresti.

Gli AKTrolls, noti solo nei circoli del partito, si organizzano in reti di individui e gruppi, ricevendo premi e pagamenti per la loro attività. Le loro principali funzioni[63] sono la sorveglianza attraverso la navigazione in rete e l'eliminazione di qualsiasi voce critica e forma di opposizione attraverso minacce e un linguaggio offensivo e intimidatorio. I *troll*, infatti, effettuano una sorta di linciaggio sociale: l'enorme volume di insulti, minacce di morte, abusi online, minacce di violenza fisica e abusi sessuali ha lo scopo di scoraggiare e intimidire i cittadini presi di mira.[64]

---

61 Corke, S., et al., 2015, *Democracy in crisis: Corruption, media, and power in Turkey*, Freedom House Special Report.

62 The Economist, settembre 2016, "A Conspiracy So Immense", in *The Economist*, https://www.economist.com/europe/2016/09/10/a-conspiracy-so-immense (consultato il 07/10/2020).

63 Karatas, D., e Saka, E., *Op. cit.*; Bulut, E., e Yörük, E., 2017, "Digital Populism: Trolls and Political Polarization of Twitter in Turkey", in *International Journal of Communication*, vol. 11, pp. 4093-4117; Cosentino, G.; e Berke, A., 2019, "Post-truth politics in the Middle East: the case studies of Syria and Turkey", in *After the post-truth*, Artnodes, n. 24, pp. 1-10.

64 Shearlaw, M., novembre 2016, "Turkish journalists face abuse and threats online as trolls step up attacks", in *The Guardian*, https://www.theguardian.com/world/2016/nov/01/turkish-journalists-face-abuse-

Attraverso l'utilizzo di *bot* automatizzati, tecniche di hacking e *phishing* per scopi politici, gli AKTrolls diffondono la propaganda filogovernativa e cercano di contrastare il discorso anti-AKP, screditando le opposizioni e conducendo grandi campagne diffamatorie.

Inoltre, i *troll* turchi hanno iniziato a mobilitarsi sempre più in altre lingue per attaccare cittadini stranieri, soprattutto politici e giornalisti critici nei confronti delle politiche dell'AKP, accusandoli di essere coinvolti in attività di spionaggio e di sostegno a gruppi terroristici contro la Turchia.

Dal soft power allo sharp power: un dibattito aperto

Il soft power

Secondo alcuni autori,[65] questi nuovi mezzi utilizzati per influenzare, manipolare e modificare l'opinione pubblica rappresentano un nuovo tipo di *soft power*, termine coniato da Joseph S. Nye nel 1990 per indicare «la capacità di convincere gli altri grazie alla legittimità dei valori dello Stato o delle sue politiche»[66], e impiegato per descrivere forme di potere e di influenza di natura non militare e non coercitiva. Secondo Nye, il *soft power* di un Paese si basa principalmente su tre risorse, ovvero la sua cultura, i suoi valori politici e le sue politiche estere, ed è spesso visto come qualcosa che gli Stati

threats-online-trolls-attacks, (consultato il 07/10/2020).

65 Santini, R.M., et al., 2018, "SOFTWARE POWER AS SOFT POWER. A literature review on computational propaganda effects in public opinion and political process", in *Partecipazione e Conflitto – The Open Journal of Sociopolitical Studies*, issue 11, n. 2, pp. 332-360.

66 Mingst, K.A, e Arreguín-Toft, I.M, a cura di Pisciotta, B., 2012, *Relazioni internazionali*, UTET Università, Torino, pg. 115.

perseguono per «conquistare i cuori e le menti» e per ottenere un'immagine pubblica positiva, anche all'estero.[67]

Nel caso specifico di Cina e Russia, i ricercatori del National Endowment for Democracy (NED), una agenzia statunitense senza scopo di lucro dedicata alla crescita e al rafforzamento delle istituzioni democratiche in tutto il mondo, in un report del 2017 parlano, invece, di *sharp power*, un potere più affilato e tagliente «che trafigge, penetra o perfora gli ambienti politici e informativi nei Paesi target», con l'obiettivo di manipolare le informazioni (attraverso *fake news*, verità alternative, ecc.) ed estendere la loro influenza, traendo vantaggio dall'ambiente informativo aperto delle democrazie.[68]

Lo sharp power

Per Christopher Walker, lo *sharp power* ha l'effetto di limitare la libertà di espressione e distorcere l'ambiente politico; può essere utilizzato per degradare l'integrità delle istituzioni indipendenti attraverso la manipolazione, il controllo e la distorsione; può funzionare tramite forme moderne di censura, inducendo i media ad autocensurarsi o impiegando nuovi strumenti digitali, come i *bot*, per diffondere informazioni false e divisive online.[69]

In *L'era dello sharp power. La guerra (cyber) al potere*, Paolo Messa riprende lo studio del NED, ricostruendo il dibattito e le critiche che ne sono seguite, e approfondisce le caratteristiche dello *sharp power*. Lo *sharp power* presenta quattro dimensioni: la prima è la conquista dell'opinione pubblica e delle

[67] Walker, C., 2018, "What Is Sharp Power?", in *Journal of Democracy*, vol. 29, n. 3, pg. 18.

[68] Cardenal, J.P., et al., 2017, *Sharp Power. Rising Authoritarian Influence*, National Endowment for Democracy, International Forum for Democratic Studies, p. 13.

[69] Walker, C., *Op. cit.*, pp. 9-23.

istituzioni (attraverso i social media, le università, i think thank); la seconda è la politica (tramite i partiti, le istituzioni multilaterali, le lobby, ecc.); la terza è la dimensione economica; la quarta, più incisiva e che riunisce in sé le altre, è la dimensione cyber.[70] Infatti, il cyberspazio – come si è visto nei paragrafi precedenti – è «uno degli strumenti più incisivi con cui uno Stato può esercitare il suo sharp power e colpire infrastrutture, dati e sicurezza del nemico».[71]

Inoltre, l'autore sottolinea come la rivoluzione informatica e la globalizzazione abbiano introdotto nuovi strumenti per conquistare l'opinione pubblica di un altro Stato. «Alcuni degli strumenti sono convenzionali: la diplomazia, le istituzioni multilaterali democratiche, il commercio, a patto che sia libero e reciproco, la condivisione di cultura. Altri, se usati con intenzioni ostili, sono altrettanto efficaci: la manipolazione delle notizie, la guerra d'informazione, la supremazia economica, le pressioni sui vertici politici e gli attacchi cyber».[72]

Conclusioni

È evidente che il *trolling* politico e le sue implicazioni, sebbene sembrino legate al mondo virtuale, hanno conseguenze reali. Ormai è certo che attraverso queste nuove tecnologie è possibile far leva su bias cognitivi, manipolare il consenso, usare tecniche di neuromarketing, creare campagne ad hoc

[70] Massa, P., 2018, *L'era dello sharp power. La guerra (cyber) al potere*, EGEA Università Bocconi Editore, Milano, pg. 43.
[71] Ibidem, pg. 70.
[72] Ibidem, pg. 43.

per screditare gli avversari, diffondere deliberatamente notizie false.

All'indomani del referendum sulla Brexit e delle elezioni presidenziali statunitensi del 2016, i governi, il mondo dell'industria e il pubblico in generale hanno espresso crescente preoccupazione per la vulnerabilità degli ecosistemi informativi agli attacchi di pirateria informatica, alle campagne di influenza e manipolazione e alla loro capacità di promuovere contenuti dannosi per i processi democratici. Una preoccupazione accentuata anche dai progressi compiuti nell'utilizzo dell'Intelligenza Artificiale (si pensi ad esempio al caso dei *deepfake*) e nella sorveglianza biometrica nonché dall'emergere di nuovi trend: l'ascesa di *bot*, *troll*, tecniche di *advertising* e *micro-targeting* e una maggiore sorveglianza stanno spingendo i cittadini-utenti verso spazi alternativi, come WhatsApp, WeChat e Telegram, per discutere o cercare notizie politiche. Anche queste piattaforme di messaggistica privata "one-to-one" però stanno diventando terreno fertile per contenuti di parte e disinformazione: infatti, per gli attori politici e le operazioni di messaggistica politica è sempre più facile infiltrarsi in questi servizi privati, difficilmente controllabili, per diffondere propaganda e voci false su oppositori politici o gruppi rivali.[73]

Mentre la politica si è progressivamente spostata nella sfera digitale, le tecnologie emergenti si sono affermate in modi che rappresentano non solo un'enorme opportunità, ma anche un rischio per i sistemi politici e una sfida per i valori

[73] Newman, N., et al., *2018, Reuters Institute Digital News Report 2018*, Reuters Institute, p. 10.

democratici fondamentali. Nell'era digitale, le implicazioni della tecnologia abbracciano questioni relative alla privacy, all'alfabetizzazione e all'accesso alle informazioni, alla sicurezza informatica, all'integrità elettorale, alle divisioni digitali e alla polarizzazione.

Dopo le notizie sulle interferenze elettorali e le campagne di manipolazione, agli Stati è apparso necessario attuare una maggiore regolamentazione dell'ambiente digitale e il controllo dei sistemi tecnologici stessi (inclusi algoritmi, sistemi di Intelligenza Artificiale e meccanismi di elaborazione dei dati) nonché dei dati raccolti ed elaborati, per garantire che gli usi e le applicazioni di questi nuovi strumenti fossero in linea con il bene pubblico, poiché «senza regole e principi specifici, la sfera digitale è un "selvaggio West"».[74]

In Europa, per esempio, i governi hanno adottato una serie di misure (come il Regolamento Generale sulla Protezione dei Dati), di filtri e controlli nazionali per contrastare la disinformazione e l'incitamento all'odio online e proteggere i diritti dei cittadini e i valori democratici.[75] Diversi governi hanno organizzato nei loro eserciti unità di sicurezza informatica e di sicurezza delle informazioni per far fronte alle interferenze straniere e alle minacce di manipolazione: queste unità sono impegnate sia nella difesa delle infrastrutture informative sia nelle operazioni strategiche di guerra informatica. Le contromisure comprendono: l'osservazione sistematica dello spazio online, l'identificazione dei trasgressori,

[74] Neudert, L.M., e Marchal, N., *Op. cit.*, p. 44.

[75] Ibidem, p. 40; Bradshaw, S., et al., 2018, *Government Responses to Malicious Use of Social Media*, NATO Strategic Communications Centre of Excellence (NATO StratCom COE), Riga, pp. 6-10.

l'analisi delle strategie di reato, la segnalazione di informazioni problematiche e il *debunking* delle *fake news*. Altre iniziative si concentrano sul monitoraggio dell'ecosistema delle informazioni e sulla fornitura agli utenti di portali per la segnalazione di notizie false e disinformazione. Inoltre, i governi stanno diventando sempre più consapevoli delle problematiche legate all'*advertising* politico online e cercano di risolverle migliorando la trasparenza tra gli acquirenti di spazi pubblicitari e i destinatari. L'implementazione di queste misure deve andare di pari passo con la creazione e l'applicazione di standard e codici etici.

L'Unione Europea stessa ha compiuto notevoli sforzi per contrastare *fake news* e disinformazione: in seguito alla Risoluzione[76] del 15 giugno 2017 sulle piattaforme online e il mercato unico digitale (2016/2276(INI)) del Parlamento europeo, la Commissione europea ha organizzato un gruppo di esperti e una consultazione[77] pubblica su *fake news* e disinformazione online, arrivando a pubblicare nell'aprile 2018 la *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*.[78] In particolare, gli Stati membri sono invitati a presentare diversi strumenti per affrontare la diffusione e l'impatto della disinformazione online e garantire la protezione dei

[76] European Parliament, giugno 2017, *Resolution on online platforms and the digital single market*, (2016/2276(INI)).

[77] European Commission, aprile 2018, *Synopsis Report of the public consultation on fake news and online disinformation*.

[78] Commissione Europea, aprile 2018, *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*, COM(2018) 236 final, Bruxelles.

valori e dei sistemi democratici dell'UE, assicurando la diversità e la credibilità delle informazioni, nonché la trasparenza sulla loro produzione o sponsorizzazione, e mirando a soluzioni inclusive con un ampio coinvolgimento delle parti interessate. L'obiettivo è creare un ecosistema online più trasparente, affidabile e responsabile.[79] L'UE ha quindi delineato un piano d'azione che comprende «l'elaborazione di un codice di buone pratiche sulla disinformazione in regime di autoregolamentazione per le piattaforme online e l'industria pubblicitaria al fine di accrescere la trasparenza e di migliorare la tutela degli utenti, la creazione di una rete europea indipendente di verificatori di fatti per stabilire metodi di lavoro comuni, scambiare buone pratiche e raggiungere la massima copertura possibile in tutta l'UE, la promozione dell'impiego volontario di sistemi di identificazione online per migliorare la tracciabilità e l'identificazione dei fornitori di informazioni e l'impiego del programma di ricerca e innovazione dell'UE (Orizzonte 2020) per mobilitare nuove tecnologie come l'intelligenza artificiale, la catena dei blocchi (blockchain) e gli algoritmi cognitivi».[80]

Sollecitati dall'invito della Commissione, i rappresentanti delle piattaforme online, gli inserzionisti, l'industria pubblicitaria e gli altri attori chiave del settore hanno concordato un codice di condotta di autoregolamentazione per contrastare la diffusione della disinformazione e migliorare le loro

[79] Commissione Europea, dicembre 2018, *Relazione della Commissione al Parlamento Europeo, al Consiglio Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni sull'attuazione della comunicazione "Contrastare la disinformazione online: un approccio europeo"*, COM(2018) 794 final, Bruxelles.

[80] Ibidem, p. 1.

politiche online.[81] Questo codice di buone pratiche mira a raggiungere gli obiettivi fissati dalla *Comunicazione della Commissione*, fissando un'ampia gamma di impegni, tra cui: garantire la trasparenza per quanto riguarda i messaggi pubblicitari di natura politica; realizzare campagne di sensibilizzazione; impegnarsi a chiudere gli account falsi, stabilendo sistemi e norme chiari per l'uso di *bot* automatizzati; collaborare con la società civile, i governi, gli istituti di istruzione e altre parti interessate per migliorare l'alfabetizzazione mediatica digitale. Nel dicembre 2020 la Commissione europea ha presentato sia una proposta di legge sui servizi digitali (il Digital Services Act e il Digital Markets Act)[82], ovvero un insieme di nuove regole applicabili in tutta l'UE per creare uno spazio digitale più sicuro e più aperto, sia il Piano d'azione per la democrazia europea (European Democracy Action Plan)[83], che comprende azioni volte a migliorare gli strumenti esistenti dell'UE per contrastare le interferenze straniere, quali l'imposizione di ammende e una serie di orientamenti[84] per rafforzare il codice di buone pratiche sulla disinformazione.

---

81 Commissione Europea, 2018, *Codice di buone pratiche dell'UE sulla disinformazione*, Bruxelles.

82 European Commission, dicembre 2020, "Europe fit for the Digital Age: Commission proposes new rules for digital platforms", in *European Commission website,* https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347 (consultato il 26/07/2021).

83 European Commission, dicembre 2020, "European Democracy Action Plan: making EU democracies stronger", in *European Commission website,* https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250 (consultato il 26/07/2021).

84 Commissione Europea, maggio 2021, *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni. Orientamenti della Commissione europea sul rafforzamento del codice di buone pratiche sulla disinformazione*, COM(2021) 262 final, Bruxelles.

Le stesse società di social media hanno progressivamente intensificato gli sforzi per autoregolarsi, implementando misure per contrastare *fake news*, informazioni ingannevoli, disinformazione, *bot* e *troll*, soprattutto durante elezioni o altri processi civici. Per esempio, tra maggio e giugno 2018 Twitter ha sospeso circa 70 milioni di account, adottando nuove regole per combattere il *trolling* ed eliminare commenti estremisti e di odio, mentre Facebook ha rimosso 583 milioni di falsi account nel primo trimestre dello stesso anno, annunciando l'implementazione di una nuova politica contro l'odio organizzato, con l'obiettivo di eliminare tutti i contenuti falsi e suscettibili di causare violenza, e delle partnership con siti di *fact-checking* parallele al reclutamento di personale per controllare e rimuovere pubblicità e contenuti dubbi contrari agli standard.[85] Le piattaforme, poi, hanno migliorato i meccanismi di segnalazione, semplificando le procedure che consentono agli utenti di segnalare post sospetti, e hanno attivato misure basate sull'Intelligenza Artificiale per rile-

[85] Bickert, M., aprile 2018, "Publishing Our Internal Enforcement Guidelines and Expanding Our Appeals Process", in *Facebook*, https://about.fb.com/news/2018/04/comprehensive-community-standards/ (consultato il 19/06/2020); Roth, Y., e Harvey, D., giugno 2018, "How Twitter is fighting spam and malicious automation", in *Blog.Twitter.com*, https://blog.twitter.com/en_us/topics/company/2018/how-twitter-is-fighting-spam-and-malicious-automation.html (consultato il 19/06/2020); Timberg, C., e Dwoskin, E., luglio 2018, "Twitter is sweeping out fake accounts like never before, putting user growth at risk", in *The Washington Post*, https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/ (consultato il 19/06/2020); Frenkel, S., luglio 2018, "Facebook to Remove Misinformation That Leads to Violence", in *The New York Times*, https://www.nytimes.com/2018/07/18/technology/facebook-to-remove-misinformation-that-leads-to-violence.html (consultato il 19/06/2020); "Civic integrity policy", ottobre 2021, in *Twitter Help Center*, https://help.twitter.com/en/rules-and-policies/election-integrity-policy (consultato il 26/07/2021).

vare e sospendere preventivamente account e contenuti, quindi prima che vengano messi online. Basta pensare, ad esempio, alle misure progressivamente adottate da Twitter e Facebook nei confronti di Donald Trump: tra maggio e giugno 2020, le due piattaforme sono intervenute direttamente per la prima volta contro alcuni post dell'ex presidente degli Stati Uniti, segnalando agli utenti il contenuto. Nello specifico, Twitter ha segnalato due suoi tweet in quanto uno (sul voto via posta) conteneva informazioni potenzialmente fuorvianti e l'altro un video manipolato; Facebook ha rimosso uno spot della sua campagna elettorale con simboli nazisti perché in violazione della politica della piattaforma contro l'odio organizzato.[86] Nel gennaio 2021, non solo Twitter e Facebook ma anche tutte le altre piattaforme di social network hanno bloccato o rimosso gli account di Donald Trump, accusandolo di aver incitato i propri sostenitori a portare avanti l'attacco al Campidoglio a Washington del 6 gennaio e di aver violato le linee guida che vietano di condividere contenuti falsi e inneggianti alla violenza.[87]

---

86 Conger, K., e Alba, D., maggio 2020, "Twitter Refutes Inaccuracies in Trump's Tweets About Mail-In Voting", in *The New York Times*, https://www.nytimes.com/2020/05/26/technology/twitter-trump-mail-in-ballots.html (consultato il 19/06/2020); Zakrzewski, C., giugno 2020, "Twitter labels Trump video tweet as manipulated media as it cracks down on misinformation", in *The Washington Post*, https://www.washingtonpost.com/technology/2020/06/18/trump-tweet-label-video/ (consultato il 19/06/2020); Stanley-Becker, I., giugno 2020, "Facebook removes Trump ads with symbol once used by Nazis to designate political prisoners", in *The Washington Post*, https://www.washingtonpost.com/politics/2020/06/18/trump-campaign-runs-ads-with-marking-once-used-by-nazis-designate-political-prisoners/ (consultato il 19/06/2020).

87 "Tutte le piattaforme che hanno bloccato Trump", gennaio 2021, in *Il Post*, https://www.ilpost.it/2021/01/12/piattaforme-social-media-blocco-account-donald-trump/ (consultato il 26/07/2021).

Il coinvolgimento dei responsabili politici e delle aziende tecnologiche nel controllo delle informazioni e nella regolamentazione dei contenuti fa crescere la preoccupazione in merito a un eccesso di regolamentazione e al blocco dei contenuti. In uno studio sugli sforzi normativi per contrastare l'uso dannoso dei social media, Samantha Bradshaw, Lisa-Maria Neudert e Philip N. Howard hanno evidenziato che i regimi di tutto il mondo stanno copiando dai Paesi europei le normative volte a controllare le informazioni online al fine di legittimare la censura e la criminalizzazione dei contenuti.[88] Nei Paesi in cui lo stato di diritto è debole, i governi si appropriano di questi quadri normativi per rafforzare il controllo sui flussi di informazione.

Si pensi poi agli effetti collaterali involontari di queste misure, alle profonde implicazioni relative al diritto alla libertà di espressione, alla privacy e alla protezione dei dati personali. Article19, organizzazione per i diritti umani che difende la libertà di espressione a livello globale, in relazione al Codice di condotta UE sulla disinformazione e alla volontà della Commissione di trasformarlo in uno "strumento più robusto" con "un meccanismo di supervisione appropriato" per la sua attuazione, ha messo in evidenza alcune criticità nel bilanciare i suoi obiettivi con la tutela del diritto alla libertà di espressione. Prima di tutto, secondo l'organizzazione, la definizione di disinformazione del Codice risulterebbe eccessivamente ampia, estendendosi non solo alle informazioni verificabilmente false o fuorvianti, concepite e promosse

[88] Bradshaw, S., et al., 2018, *Government Responses to Malicious Use of Social Media*, *Op. Cit.*, p. 6.

per fini economici o per arrecare un "danno pubblico", ma anche alla cosiddetta "misinformazione", ovvero quelle informazioni totalmente o parzialmente false, non create con l'intenzione di causare danni.[89] Inoltre, non viene fornita una definizione esaustiva del "danno pubblico", facendo solo riferimento a concetti vaghi come sicurezza o minacce ai processi democratici o politici, e includendo anche un riferimento ai "beni pubblici" che tuttavia non risultano elencati in modo approfondito. Secondo Article19, l'obiettivo di qualsiasi regolamento non dovrebbe essere l'eliminazione di ogni "misinformazione", ma quello di «sviluppare maggiori linee guida per gli Stati e le aziende dominanti su come promuovere informazioni di alta qualità e l'alfabetizzazione ai media digitali, nonché diverse fonti di media indipendenti per garantire una pluralità di opinioni politiche o scientifiche. Ciò dovrebbe comportare il sostegno a mezzi di comunicazione di servizio pubblico indipendenti, diversificati e adeguati, nonché l'educazione all'alfabetizzazione mediatica».[90] Inoltre, il Codice dovrebbe affrontare di più il modello di business delle piattaforme online basato sulla raccolta dei dati personali degli utenti e fare esplicito riferimento alla ne-

[89] La disinformazione è la diffusione intenzionale di informazioni totalmente o parzialmente false, inesatte o fuorvianti, concepite, presentate e promosse per danneggiare una persona, un gruppo sociale, un'organizzazione o un Paese, o per scopi di lucro; con il termine misinformazione si fa riferimento, invece, alla diffusione non intenzionale di informazioni totalmente o parzialmente false, non create con l'intenzione di causare danni; il termine malinformazione si riferisce a informazioni che si basano sulla realtà, utilizzate per infliggere danni a una persona, un'organizzazione o un Paese. (Wardle, C., e Derakhshan, H., 2017, "Information disorder: definitions", in *Understanding and addressing the disinformation ecosystem*, Annenberg School for Communication, p. 9).

[90] Article19, aprile 2021, *European Commission Consultation on the Guidance on tackling disinformation. ARTICLE 19's submission*.

cessità di un adeguamento agli strumenti dell'UE in materia di protezione dei dati come il GDPR. Un'ulteriore criticità riguarda lo sviluppo di "indicatori di affidabilità" per promuovere solo fonti autorevoli: il rispetto di questi indicatori potrebbe portare giornalisti e comunicatori indipendenti, piccoli giornali o voci di minoranza a essere meno visibili, e questo potrebbe rappresentare un rischio per la pluralità dei punti di vista. Nei Paesi in cui non vi sono media diversificati, o in cui il controllo statale è maggiore, le informazioni "autorevoli" saranno quasi inevitabilmente quelle del governo. Sempre più spesso gli Stati usano come motivazione quella di prevenire *fake news* e disinformazione per bloccare arbitrariamente l'accesso a Internet e adottare una legislazione repressiva, violando il diritto alla libertà di espressione e opinione e all'accesso alle informazioni.[91] Inoltre, secondo l'organizzazione nessuna misura in questo campo dovrebbe essere resa obbligatoria, per non trasformare le autorità pubbliche «in arbitri della verità e dell'informazione attendibile». Lo sviluppo e l'uso di indicatori potrebbe portare, poi, a una rimozione eccessiva dei contenuti: contenuti considerati "borderline", ovvero leciti ma controversi, o contenuti contrassegnati o etichettati come potenziale disinformazione o che non rispondono all'indicatore di "affidabilità" verrebbero semplicemente eliminati, sopprimendo ad esempio il dibattito su questioni divisive. Article 19 sottolinea anche i limiti dei servizi di *fact-cheking*, incapaci di verificare oggetti-

[91] A questo proposito, è possibile consultare il lavoro dell'organizzazione Access Now e della coalizione #KeepItOn che documenta e indaga gli *shutdown* di internet a livello globale: https://www.accessnow.org/keepiton/

vamente le informazioni e la base fattuale di tutti i contenuti, e la necessità di una maggiore trasparenza nel modo in cui le aziende attuano il Codice, anche fornendo a ricercatori, ONG e altri l'accesso ai dati. In particolare, è fondamentale una maggiore trasparenza riguardo l'impiego degli algoritmi e dei criteri seguiti per amplificare o nascondere determinati tipi di informazione. Sebbene le misure per bloccare *fake news*, *troll*, ecc., risultino legittime, occorre tuttavia sottolineare che l'adozione di filtri negli algoritmi e di misure basate sull'Intelligenza Artificiale potrebbe penalizzare valide fonti di informazione alternative. Secondo Jonathan Albright, «nel decennio a venire, saranno dei potenti filtri controllati da intelligenza artificiale e sviluppati da aziende informatiche a stabilire la legittimità delle informazioni prima che il pubblico abbia la possibilità di farlo da sé».[92] Moderazione e repressione automatiche, rendendo ogni contenuto sempre soggetto a controllo, potrebbero censurare anche contenuti leciti. In contesti non democratici, questi impianti normativi potrebbero aumentare il controllo sull'opinione pubblica e reprimere ulteriormente la libertà di espressione, riducendo al silenzio l'opposizione politica e punendo chiunque manifesti il proprio dissenso.

Nell'ultimo rapporto di Freedom House,[93] si evidenzia come a livello globale sempre più Stati stiano cercando di attuare un controllo maggiore sulle grandi aziende tecnologiche: con

[92] Albright, J., dicembre 2016, "Stop worrying about fake news. What comes next will be much worse", in *The Guardian*, https://www.theguardian.com/commentisfree/2016/dec/09/fake-news-technology-filters (consultato il 19/06/2020).

[93] Baker, G. et al., 2021, *Freedom on the Net 2021. The Global Drive to Control Big Tech*, Freedom House.

poche eccezioni positive, la spinta a regolamentare l'industria tecnologica, che nasce dalla volontà di contrastare problemi reali come la disinformazione, le molestie online, ecc., viene sfruttata per attuare nuove regole sulla sfera digitale, ottenendo un maggiore accesso ai dati privati e limitando fortemente la libertà di espressione online. Infatti, nell'ultimo anno, dei 70 Stati analizzati nello studio, 48 hanno perseguito azioni legislative o amministrative per regolamentare le società tecnologiche: le azioni normative si sono spostate drasticamente verso un maggiore intervento dei governi nella sfera digitale e se alcune misure riflettono tentativi legittimi per affrontare alcune problematiche online, frenare l'uso improprio di dati o porre fine a pratiche manipolative di mercato così da rendere i giganti della tecnologia più responsabili delle loro prestazioni, molte nuove leggi impongono responsabilità statali e persino politiche alle aziende private, costringendole spesso a conformarsi alla censura, alla raccolta di dati e alla sorveglianza online, senza garantire maggiori diritti per gli utenti. Le attività online degli utenti risultano monitorate e moderate in maniera più pervasiva dalle aziende tecnologiche attraverso processi che mancano delle garanzie tipiche della governance democratica, come la trasparenza, il controllo giudiziario e la responsabilità pubblica. In assenza di una visione globale condivisa per un Internet libero e aperto, i governi stanno adottando approcci propri per controllare la sfera digitale. E questa situazione è peggiorata con la pandemia di Covid-19: la crisi sanitaria viene usata come pretesto per giustificare un maggior controllo sulla sfera digitale, reprimere il dissenso, censurare

notizie e discorsi critici, attuare una maggiore sorveglianza, ecc.[94] Per esempio, in Turchia il governo ha utilizzato eserciti di *troll* e imposto restrizioni online, *shutdown* di internet e nuove regole per controllare il flow delle informazioni e ridurre la capacità delle società di social media di resistere alle richieste delle autorità governative, volte a censurare le voci dell'opposizione, il giornalismo indipendente, siti web e account ritenuti scomodi.[95] In Cina, il governo ha inasprito le pene detentive per il dissenso online, attuando una forte censura soprattutto dei contenuti relativi al Covid-19 (l'argomento più censurato del 2021), inondando lo spazio informativo con false affermazioni sul virus e i vaccini statunitensi, introducendo nuove regole per limitare e rimuovere gli account gestiti in modo indipendente che pubblicano notizie di attualità e obbligando le aziende ad archiviare i dati degli utenti su server locali per decriptarli su richiesta delle autorità.[96] Il governo russo, invece, ha stabilito nuove regole per le aziende tecnologiche, tra cui una legge del gennaio 2021 che ha introdotto multe per i siti web e le piattaforme che non riescono a rimuovere i contenuti ritenuti illegali dallo Stato, mentre una legge di febbraio ha rafforzato gli obblighi delle piattaforme di identificare e rimuovere i contenuti vietati, richiedendo loro di coordinarsi con il Roskomnadzor – il Servizio federale per la supervisione nella sfera della con-

94 Ibidem, pg. 9.
95 Ibidem pg. 14; Amnesty International, 2021, *Amnesty International Report 2020/21. The State of the World's Human Rights*, Peter Benson House, Regno Unito, pg. 43.
96 Baker, G. et al., *Op. cit.*, pg. 7.

nessione e comunicazione di massa – per la loro moderazione.[97]

Non esistono soluzioni semplici per affrontare le sfide poste dall'impiego di questi nuovi strumenti e il ritmo accelerato con cui si sviluppano e progrediscono determinerà senza dubbio non solo nuove sfide ma anche nuove opportunità per i governi e i responsabili politici.

[97] Ibidem, pg. 14.

Geopolitica.info

Alessia Bevilacqua

Ha conseguito a pieni voti la Laurea Magistrale in Relazioni Internazionali presso l'Università degli Studi Roma Tre, dopo aver studiato per un anno all' École des Hautes Études en Sciences Sociales di Parigi. Ha svolto un tirocinio presso il Servizio per la Stampa e la Comunicazione Istituzionale del Ministero degli Affari Esteri e della Cooperazione Internazionale e ha da poco concluso un anno di Servizio Civile con UNICEF Italia. È appassionata di geopolitica, questioni di genere, diritti umani, ma anche comunicazione e cybersicurezza.

Il Centro Studi

Il Centro Studi Geopolitica.info nasce nel 2004 con l'obiettivo di offrire un contributo al dibattito sulla politica estera, la geopolitica e le relazioni internazionali dalla prospettiva dell'Italia. Le attività del Centro Studi si articolano in tre filoni principali: la pubblicazione della Rivista online *Geopolitica.info* e la ricerca in materia di politica internazionale e geopolitica; la formazione attraverso i corsi in presenza e i corsi online sulla piattaforma www.onlineducation.it; l'organizzazione di momenti di dibattito pubblico sui temi dell'agenda politica italiana relativi alle relazioni internazionali. Tutte le attività sono consultabili sul sito web www.geopolitica.info.

Centro Studi Geopolitica.info
www.geopolitica.info | centrostudi@geopolitica.info