Come individuare e contrastare operazioni coordinate di disinformazione in Italia

Casi di studio e indicazioni di *policy* per istituzioni pubbliche e private.

MANUALE

Come individuare e contrastare operazioni coordinate di disinformazione in Italia

Casi di studio e indicazioni di *policy* per istituzioni pubbliche e private

Come individuare e contrastare operazioni coordinate di disinformazione in Italia.
Casi di studio e indicazioni di *policy* per istituzioni pubbliche e private.

Realizzazione di:

Antonio Gullo, Direttore della Ricerca per la parte legale e *cybersecurity*, Luiss Guido Carli

Irene Pasquetto, Direttore della Ricerca per la parte di design, media e disinformazione, Harvard Kennedy School/University of Michigan

Gianni Riotta, Direttore della Ricerca per la parte di *media* e disinformazione, Luiss Guido Carli

Costanza Sciubba Caniglia, Direttore del Progetto e della Ricerca per la parte teorica e di relazioni internazionali, Harvard Kennedy School

Con il supporto di:

Emanuele Birritteri
Eugenia Tere Cab Salinas
Emanuele Camarda
Luca D'Agostino
Adriano Umberto Luigi Dossi
Marco Galimberti
Michelangelo Gennaro
Mattia Giusto Zanon
Alberto Olivieri
Giovanni Piccirilli
Elisabetta Pietrocarlo
Silvio Puccio
Tommaso Sensi
Alessandra Spada
Luca Tacchetti
Federica Urzo
Stefano Vacca

Data di pubblicazione
30 Giugno 2021

"Questa ricerca è stata realizzata con un contributo dell'Unità di Analisi, Programmazione e Documentazione Storica del Ministero degli Affari Esteri e della Cooperazione Internazionale ai sensi dell'Art. 23 bis del Decreto del Presidente della Repubblica n. 18 del 5 gennaio 1967"

Ministero degli Affari Esteri
ella Cooperazione Internazionale

Luiss
Dipartimento
di Giurisprudenza

HARVARD KENNEDY SCHOOL
Misinformation Review

SCHOOL OF INFORMATION
UNIVERSITY OF MICHIGAN

LUISS
Data Lab

Luiss
Master di Giornalismo

zeta

IGD

INDICE

Quadro teorico e motivazione della ricerca

I. Sintesi della ricerca, di Costanza Sciubba Caniglia

Negli ultimi anni, le *campagne di informazione*[1] e la *disinformazione* hanno continuato a rappresentare un pericolo crescente per la democrazia.

Dal 2016, anno in cui le campagne di influenza hanno iniziato a essere analizzate in maniera sistematica, l'incremento e la progressiva sofisticazione di campagne di *disinformazione* condotte sia sui *social media* che sui media tradizionali, e spesso nell'ambito di più complesse

1 C'è qui da fare una prima osservazione di tipo lessicale: con operazioni di informazione intendiamo operazioni complesse che comprendono l'uso integrato di guerra elettronica, computer network operations, operazioni psicologiche, inganno militare e operazioni di sicurezza usate allo scopo di influenzare, distruggere, corrompere od usurpare il potere decisionale tanto di avversari umani che artificiali, secondo la definizione data in questa comunicazione dell'Unione dei Capi di Gabinetto delle forze armate USA: https://web.archive.org/web/20150208100916/http://www.fas.org/irp/doddir/dod/jp3_13.pdf

1

operazioni di informazione, ha destato crescente preoccupazione e interesse sia a livello istituzionale che fra le compagnie di *social media* e la ricerca universitaria.

Vi è ora una più diffusa consapevolezza che le *disinformation operations* rappresentino un pericolo per il mantenimento di sistemi di governo democratici, e possano contribuire a corrompere l'integrità della deliberazione politica. Tuttavia, permane ancora, al momento, una molteplicità di strutture di analisi e di differenze nella definizione del problema e delle sue componenti che rende difficile l'elaborazione di risposte comuni, tanto a livello istituzionale e di pubblica amministrazione, quanto a livello di *piattaforme digitali*[2] o di partnerships pubblico/privato non solo a livello nazionale, ma internazionale.

Questo lavoro di ricerca – portato avanti tramite una collaborazione *ad hoc* fra la Harvard Kennedy School Misinformation Review, il Luiss Data Lab, il Dipartimento di Giurisprudenza dell'Università Luiss Guido Carli, il Master in Giornalismo e Comunicazione multimediale dell'Università Luiss Guido Carli, l'University of Michigan e l'Istituto di Geopolitica Digitale – è partito da questa osservazione per investigare aree di ricerca separate ma in relazione allo scopo di promuovere l'utilizzo tanto di termini quanto di strutture di analisi e di metodologie di ricerca comuni a diversi ambiti di studio per l'analisi di operazioni di informazione (con un focus particolare sulle campagne di disinformazione, che ne sono una componente) e l'elaborazione di contromisure adeguate.

Prima di entrare nel vivo della ricerca etnografica, che si è concentrata su alcune campagne di disinformazione in Italia, e della ricerca giuridica, che ha messo a confronto ordinamenti diversi sul tema in esame, sarà opportuno fare delle necessarie premesse di elaborazione del tema, che illuminano anche la definizione dell'analisi ad ampio raggio e sul lungo periodo.

Seppure questo tipo di operazioni non siano nuove da un punto di vista strategico (basti pensare alle cosiddette "misure attive" portate avanti dall'Unione Sovietica durante il periodo della Guerra Fredda), le innovazioni tecnologiche e le modifiche all'ecosistema dell'informazione degli ultimi anni, hanno aggiunto ulteriori livelli di complessità, portando allo sviluppo di nuove e più sofisticate tattiche e strategie, che rendono

2 Con piattaforme digitali (o piattaforme online), si intendono, secondo la definizione dell'Unione Europea, "strutture di software che offrono mercati in cui i providers e gli user di contenuto e di beni possono incontrarsi". In questa definizione, ricadono sia le piattaforme di social media, che piattaforme digitali che vendono beni e servizi, come ad esempio Amazon. Sebbene in questa ricerca ci riferiamo principalmente alle piattaforme di social media, abbiamo preferito mantenere il termine più ampio di piattaforme digitali, in quanto in maniera crescente si è osservato come molte delle considerazioni relative alla disinformazione ed all'uso di algoritmi di manipolazione del contenuto si possano estendere anche a questo altro tipo di piattaforme. Si pensi, ad esempio al ruolo dell'algoritmo di Amazon nella diffusione di contenuti cospirazionisti e anti vax: https://www.theguardian.com/commentisfree/2020/aug/08/amazon-algorithm-curated-misinformation-books-data

queste campagne più rapide ed efficaci e permettono a diversi gruppi di attori, tanto pubblici quanto privati, tanto domestici quanto stranieri, di intervenire in maniera ingannevole nel dibattito democratico.

Data la natura relativamente recente e in continua evoluzione di queste minacce, non vi è ancora una politica univoca di risposta, né a livello nazionale né multilaterale. Per questo si ritiene sia urgente e di particolare rilevanza studiare metodologie e analizzare casi, allo scopo di elaborare un *framework* utile alla predisposizione di soluzioni adeguate, che assicurino il mantenimento di un elevato standard di qualità del discorso pubblico e dell'informazione in Italia e che possano rivelarsi altresì funzionali a rafforzare meccanismi di coordinamento e cooperazione a livello multilaterale, europeo e internazionale.

Per raggiungere quest'obiettivo, abbiamo redatto sia il presente rapporto, che descrive in dettaglio il lavoro fin qui svolto, la sua impostazione teorica e le raccomandazioni per lo sviluppo della ricerca nei prossimi mesi e anni, che un breve "manuale pratico" riassuntivo che comprende linee guida e indicazioni di *policy* per prevenire o contenere gli effetti delle operazioni di informazione nel contesto italiano, siano esse portate avanti da attori statuali o privati.

Questa ricerca si è svolta in tre parti:

- Una prima parte, che segue, si è concentrata sulla **definizione teorica dell'ambito di studio delle operazioni di informazione**;
- Una seconda parte di **ricerca empirica** ha analizzato due casi di studio relativi a *network* di informazione in Italia e uso di tecniche e strategie per la diffusione di informazioni ingannevoli:
  - ◊ Un caso di studio ha riguardato gruppi vicini alla teoria della cospirazione legata a QAnon;
  - ◊ Un altro caso di studio ha riguardato gruppi legati alle cospirazioni anti-vacciniste durante il *roll-out* vaccinale;

- Una terza parte si è invece concentrata sullo **studio comparato della legislazione relativa alla disinformazione ed alle operazioni di informazione** tramite uno studio delle *policy* esistenti (literature review) e la comparazione delle misure introdotte in diversi ordinamenti. In particolare, Unione Europea, Italia, Francia, Germania, e Stati Uniti.

Dalla ricerca empirica svolta, questo gruppo di ricerca ha riscontrato che:

Sintesi di ***Irene Pasquetto***

- I gruppi che organizzano e diffondono campagne di disinformazione in Italia sono estremamente organizzati dal punto di vista tecnico e infrastrutturale. Questi mettono insieme vere e proprie infrastrutture della disinformazione digitale che si poggiano solo in fase iniziale di espansione su pagine e *account social*, per poi andare a comprendere tutta una serie di siti internet, aggregatori di *news*, banche dati, canali di (dis)informazione alternativa, *blog*, forum, etc. Tali infrastrutture sono gestite da figure chiave quali i *disinfluencers* (vedere definizione in glossario), i quali vengono aiutati da un esercito di follower fedeli e interessati alla causa. La collaborazione e partecipazione attiva dei *follower* è indispensabile alla diffusione e mantenimento delle infrastrutture di disinformazione nel tempo.
- Da questo primo dato sorge l'importanza del tener conto dell'aspetto temporale quando vengono organizzati interventi contro la disinformazione *online* come il *deplatforming* di questi gruppi dai principali *social media*. Come mostreremo, se il *deplatforming* non avviene in modo tempestivo, avrà un effetto limitato nello sradicare tali gruppi e limitare l'efficacia delle campagne. Se il *deplatforming* viene messo in atto dopo che l'infrastruttura ha passato la fase critica iniziale di espansione e stabilizzazione, i gruppi avranno altresì avuto modo di costruire vie di fuga e canali alternativi sui quali dirottare il traffico e coltivarne di nuove in caso di deplatforming. Si noti il ruolo centrale di Telegram, e delle app di messaggistica in generale, nel costituire un rifugio sicuro per i *disinfluencers* e le loro audience in caso di *deplatforming*. Va infine notato che il *deplatforming* non è mai una soluzione definitiva, ma deve invece essere effettuato in maniera iterativa in quanto i gruppi di disinformazione sviluppano tattiche e strategie precise che consentono loro di adattarsi volta per volta a nuove condizione tecniche;
- Lo studio antropologico dei *disinfluencers* responsabili per l'attivazione e diffusione di tali infrastrutture ha rivelato che questi appartengono a categorie di professionisti quali avvocati, medici, liberi professionisti, giornalisti e politici. Tale ritrovamento è in netta contrapposizione con la tendenza a caratterizzare i "disinformati" con persone con bassi livelli di educazione o appartenenti a classi meno abbienti. Le campagne di disinformazione sono costruire da "professionisti della disinformazione" e il fenomeno della disinformazione assume quindi le caratteristiche di una pratica professionale più che di un gioco di ruolo, culto religioso o passatempo (come e' stata caratterizzata in passato). Va inoltre notato come spesso questi *disinfluencers* derivano dei guadagni monetari dalle loro attività *on* e *offline*, per esempio vendendo prodotti,

tessere associative o richiedendo offerte e donazioni;

- Dal nostro studio emerge inoltre il ruolo centrale dei media tradizionali nel dare voce e amplificare le campagne di disinformazione nate nella rete. Va notato che questo processo non sempre avviene in maniera intenzionale. Per esempio, per quanto riguarda la copertura mediatica sulla pandemia Covid-19 e sui vaccini, si è riscontrata una diffusa impreparazione tra i media italiani nel descrivere i processi scientifici in maniera accurata e veritiera. Particolarmente problematica è stata la sensazionalizzazione invece che la normalizzazione di fattori come l'incertezza e la processualità dei processi scientifici, fattori costitutivi della scienza che non andrebbero presentati come problematici o anomali ma spiegati e normalizzati. Tra le possibili risposte se ne consigliano due in particolare. Da un lato, l'adozione di *strategic silence* da parte dei media, una tattica di coordinazione giornalistica che prevede la consapevole presa di coscienza del ruolo dei media nell'amplificare le campagne di disinformazione, e la conseguente decisione di non dare visibilità a tali campagne messe in atto dai gruppi della disinformazione. In secondo luogo, si consiglia lo sviluppo di un curriculum giornalistico svolto a educare nuove generazioni di giornalisti su strategie precise per la copertura di notizie di stampo scientifico e, più in generale, sul funzionamento della disinformazione *online*.

Per una migliore comprensione del fenomeno a lungo termine e per sviluppare adeguate contromisure tecniche e regolamentari, questo gruppo di ricerca consiglia inoltre di promuovere lo scambio e la collaborazione fra l'Università, le Istituzioni pubbliche,[3] e le imprese private[4] tramite lo stanziamento di fondi strutturali per creare e mantenere gruppi di ricerca e discussione a livello nazionale ed internazionale, di natura sia formale che informale.[5]

3 In particolare la Presidenza del Consiglio dei Ministri, il Ministero degli Esteri, il Ministero della Difesa, il Ministero dello Sviluppo Economico, il Ministero dell'Istruzione, il Parlamento e la nascente Agenzia Nazionale per la Cybersecurity, seguiti da e in collaborazione con autorità regionali e locali.

4 In particolare le piattaforme digitali.

5 Per raccomandazioni concrete sulle politiche che la pubblica amministrazione può implementare si vedano le raccomandazioni a pag. 133 del report

I.1. Tra disinformazione e guerra ibrida, le relazioni fra stati e la pubblica informazione in un ecosistema dell'informazione in evoluzione

di Costanza Sciubba Caniglia

Negli ultimi anni, l'incremento di operazioni di disinformazione condotte sia sui *social media* che sui media tradizionali ha continuato a rappresentare un pericolo crescente per la democrazia[6]. Ma mentre queste attività sono in crescita, la nostra capacità di attribuire campagne ad attori precisi rimane problematica, così come la capacità di analizzare l'effettiva influenza che queste campagne hanno nel manipolare le opinioni della popolazione.

Questo tipo di influenze, che avvengono regolarmente, diventano particolarmente pericolose in momenti di eccezionale confusione informativa come, ad esempio, la pandemia di COVID-19, eventi di attualità come attacchi terroristici, o di stress per le istituzioni democratiche, come le elezioni politiche. Sebbene rimanga ancora oggi impossibile una chiara quantificazione dell'influenza che queste campagne hanno nel dibattito pubblico, e difficile attribuirle ad attori precisi, è chiaro che esse sono dannose per il discorso democratico ed esercitano una pressione pericolosa per le istituzioni, particolarmente quando si manifestano in occasione di questi eventi.

Dalle più recenti osservazioni, studiosi, ricercatori, e diversi governi nazionali sono concordi nel ritenere il numero e la sofisticazione di queste campagne come destinato ad aumentare[7]. Per questa ragione, la risposta tanto delle istituzioni quanto dei privati cittadini dev'essere quella di un approccio sistematico e a lungo termine ad un ecosistema dell'informazione modificato. Lo scopo dev'essere dunque quello prima di tutto di comprendere questo nuovo ecosistema dell'informazione e in secondo luogo di metterlo in sicurezza tramite uno studio continuativo di tattiche e strategie utilizzate, così come di tecnologie in evoluzione. A questo scopo, ricercatori e istituzioni stanno lavorando per sviluppare risposte di diverso tipo, sia tecniche (per esempio agendo sulle piattaforme digitali ed i loro algoritmi), che di *policy*, che tese ad incrementare l'alfabetizzazione mediatica della popolazione.

L'analisi delle operazioni di informazione, per sua natura, si sviluppa

6 Nel 2021, l'Oxford Computational Propaganda Research Project ha rilevato prove dell'utilizzo di social media allo scopo di diffondere propaganda e disinformazione in 81 Paesi. Un trend in crescita rispetto all'anno precedente, in cui avevano rilevato solo 70 paesi. Vedi Industrialized Disinformation 2020 Global Inventory of Organized Social Media Manipulation - Samantha Bradshaw . University of Oxford, 2020.

7 Si veda, ad esempio, l'utile sommario fatto dalla Brookings Institution: Goldstein, Josh A., and Shelby Grossman. "How Disinformation Evolved in 2020." Brookings. Brookings, January 4, 2021. https://www.brookings.edu/techstream/how-disinformation-evolved-in-2020/.

all'incrocio di molteplici e diverse discipline, la scienza dei dati, il giornalismo investigativo, la teoria della comunicazione, gli studi strategici, lo studio dell'intelligenza artificiale, lo studio delle relazioni internazionali, lo studio del linguaggio e della propaganda, la storia, l'analisi giuridica delle politiche pubbliche e private, ed altri ambiti di ricerca ad essi collegati. Per questa ragione, i molteplici gruppi di ricerca nati negli ultimi anni, particolarmente negli Stati Uniti e a livello di Unione Europea[8], riflettono la necessità di portare insieme esperti e metodologie di ricerca provenienti da diversi ambiti di studio. Anche in questo studio, abbiamo lavorato per far incontrare competenze diverse e interdisciplinari.

Negli ultimi anni, grazie ad un crescente interesse per questo tema, e la creazione di molteplici gruppi di lavoro, tanto governi nazionali di Paesi democratici, quanto organizzazioni sovranazionali, tra cui l'Unione Europea e la NATO, e le piattaforme digitali hanno acquisito crescente consapevolezza dell'attuale minaccia rappresentata da questo tipo di manipolazione dell'informazione.

Tuttavia, seppur abbiano negli ultimi anni aumentato le proprie capacità di comprensione e analisi del fenomeno, gli stati democratici non sembrano ancora aver compreso appieno il livello di trasformazione dell'ecosistema politico e dell'informazione che le piattaforme digitali hanno causato con conseguenze importanti sulla sovranità nazionale[9].

Ci troviamo, dunque, ancora nel pieno di una crisi di disinformazione generalizzata, con conseguenze concrete sull'economia e la sicurezza della popolazione. Si pensi, ad esempio, alle difficoltà nell'implementare correttamente il piano vaccinale di risposta al COVID-19 dato dalla diffusione di teorie della cospirazione legate ai gruppi AntiVax[10].

Il nuovo ecosistema informativo è composto da due componenti principali, entrambe vettori importanti di comprensione del fenomeno:

- Da una parte, i nuovi sviluppi tecnologici hanno profondamente modificato il modo in cui l'informazione circola ed è fruita dalla popolazione. Questa fase di sviluppo tecnologico è stata accompagnata da un periodo di grande espansione non regolamentata della nuova tecnologia, seguito da una fase di elaborazione di nuove policies e regolamenti. È questa è la fase in cui ci troviamo adesso, da un punto di vista **socio-tecnologico**.

8 Per un'utile literature review dei lavori prodotti recentemente da questi gruppi e per alcune raccomandazioni, si veda Kamya Yadav, "Countering Influence Operations: A Review of Policy Proposals Since 2016," Carnegie Endowment for International Peace, accessed May 23, 2021, https://carnegieendowment.org/2020/11/30/countering-influence-operations-review-of-policy-proposals-since-2016-pub-83333.:

9 Come notato da Luciano Floridi in Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. Philosophy & Technology, 33(3), 369-378. doi:10.1007/s13347-020-00423-6.

10 Questo caso, in particolare, è stato oggetto di uno dei nostri casi di studio, a pag. 33

- Da un punto di vista **politico e geopolitico**, invece, queste nuove tecnologie sono venute a maturazione in un periodo in cui esiste un interesse da parte di alcuni attori, siano essi statali o privati, nel creare sfiducia e spingere verso una polarizzazione della società, specialmente di quella degli stati ad ordinamento democratico. La disinformazione è diventata dunque uno strumento strategico chiave nel più ampio fenomeno di *democratic backsliding* che innumerevoli studiosi hanno rilevato[11].

Queste due componenti, seppur indipendenti, sono entrambe essenziali per una corretta comprensione del fenomeno e vanno analizzate in parallelo. La diffusione di disinformazione, -specialmente alla velocità e volume che abbiamo osservato negli ultimi anni- non è né casuale né inarrestabile, bensì la conseguenza di errori nel design tecnologico delle piattaforme e nei regolamenti legislativi, così come dell'inazione sia da parte delle piattaforme che dei governi, dei partiti, e dei media tradizionali, ma anche conseguenza di interessi politici contingenti. Come tale, può essere risolta tramite soluzioni tecniche e politiche.

I.2. Fase preliminare: definizione dei termini e del *framework*. Cosa si intende con operazioni di informazione

Come visto in introduzione, la disinformazione è una componente di un fenomeno più ampio che abbiamo definito come operazioni di informazione (o operazioni di influenza), ovvero "l'uso integrato di guerra elettronica, *computer network operations*, operazioni psicologiche, inganno militare e operazioni di sicurezza che, assieme a relative capacità strategiche, vengono utilizzate allo scopo di influenzare, distruggere, corrompere od usurpare il potere decisionale tanto di avversari umani che artificiali."[12] Si può trattare, dunque, di una strategia all'interno di operazioni più ampie e multi-strategiche volte a raggiungere un risultato tramite l'influenza di una parte della popolazione. Questo tipo di strategie è tipico della guerra ibrida, cioè una "strategia militare, caratterizzata da grande flessibilità, che unisce la guerra convenzionale, la guerra irregolare e la guerra fatta di azioni di attacco e sabotaggio cibernetico[13]". Tuttavia,

11 Si veda, ad esempio: Levitsky, Steven and Daniel Ziblatt, How Democracies Die. New York: Crown, 2018.

12 Rimando alla nota 2 in questo capitolo.

13 Definita dall'Enciclopedia Treccani come: Strategia militare, caratterizzata da grande flessibilità, che unisce la guerra convenzionale, la guerra irregolare e la guerra fatta di azioni di attacco e sabotaggio cibernetico. https://www.treccani.it/vocabolario/guerra-ibrida_%28Neologismi%29/

è bene qui ricordare che la disinformazione può essere utilizzata non solo per questo tipo di fini politici e strategici, ma anche per ragioni economiche o di vandalismo. In questi casi, essa può presentarsi isolata e non parte di una più complessa operazione strategica.

In questo studio abbiamo scelto di concentrarci principalmente sulle tattiche e le strategie di manipolazione dell'informazione in due casi esemplificativi nel panorama informativo italiano. Questi due casi di studio, uno legato alle cospirazioni QAnon, provenienti dagli Stati Uniti e, come vedremo, adattate al contesto locale e uno legato agli AntiVax, ci hanno permesso di osservare a livello locale la creazione di consenso all'interno di un ecosistema dell'informazione con diversi modelli di autorità epistemiche e di rilevare alcune tattiche e strategie di disinformazione utilizzate. Tramite l'analisi di questi gruppi di informazione, siamo in grado di anticipare o rilevare nelle sue fasi iniziali eventuali operazioni di informazione e osservarne l'efficacia, come abbiamo fatto nel caso di *#Italiadidit*, una campagna di disinformazione che ha tentato -con limitato successo- di diffondersi utilizzando il *network* di utenti legato a QAnon.[14]

Seppur alcune definizioni qui utilizzate siano mutuate da un contesto militare e di sicurezza, qui non intendiamo analizzare solo operazioni di influenza con scopi geopolitici, ma ogni tipo di operazione di informazione portata avanti da attori tanto statuali quanto privati, volta a manipolare l'informazione e le credenze di un pubblico. Questo tipo di operazioni può includere **sia informazione vera che falsa, purché sia distribuita allo scopo di manipolare la credenza di un gruppo**.

Alle operazioni di disinformazione si affiancano spesso, soprattutto nel contesto di operazioni di influenza, anche attacchi alla sicurezza cibernetica. In questi casi, bisogna dunque tenere presente due vettori predominanti di influenza strategica, separati eppure paralleli: da una parte attacchi cibernetici, volti ad esempio ad infiltrare i sistemi di voto, e dall'altra operazioni di informazione *online* volte ad esempio ad influenzare elettori e media e manipolare l'ambiente dell'informazione, spesso allo scopo di diminuire la fiducia nei processi democratici.[15]

In molti casi, l'esistenza contemporanea tanto di campagne di disinformazione quanto di attacchi cibernetici può essere un segnale che può indicare un'operazione coordinata.

Sebbene, inizialmente, il fenomeno della disinformazione sia stato ricondotto esclusivamente ad attori statuali e spesso stranieri, la realtà è più complessa. Sono, infatti, diversi gli attori che utilizzano campagne di influenza e disinformazione (che di esse rappresenta solo una parte) e diversi gli scopi per cui agiscono.

14 Per un'analisi di questa campagna si veda a pag. 48 del report

15 Sarah O'Connor et al., "Cyber-enabled foreign interference in elections and referendums," ASPI, 28 October 2020.

Questi possono essere sia di natura politica, ad esempio diretti ad alimentare le tensioni sociali su temi chiave per creare confusione e sfiducia nella popolazione, che di natura economica, o talvolta vandalica. Accanto agli attori statuali, ve ne sono molti altri, inclusi gruppi di attivisti, partiti politici, altri gruppi organizzati, in misura sempre crescente agenzie di comunicazione specializzate in queste campagne che offrono servizi di "*disinformation for hire*",[16] e da altri tipi di attori. Una recente ricerca dell'Università di Oxford rileva come, nel 2020, ben 81 Paesi abbiano utilizzato campagne di disinformazione come strumento strategico, un trend in crescita dal 2019, anno in cui questo gruppo di ricerca aveva rilevato questo tipo di attività solo in 70 Paesi.

I.3. La mancanza di definizioni univoche come elemento di criticità

Sia a livello nazionale che internazionale, la mancanza di definizioni univoche così come di strutture analitiche condivise si presenta come una delle principali criticità per lo studio e la risposta operativa a campagne di informazione. Questo non è soltanto un problema limitato alla ricerca accademica, ma anzi diventa ancora più evidente nello scambio fra soggetti privati (come le piattaforme digitali), istituzioni, e ricerca. Anche la Commissione Europea, nel recente report di analisi dei risultati preliminari del *Code of Practice on Disinformation*[17] sottolinea questa mancanza, raccomandando lo sviluppo di un linguaggio comune.

In questo studio abbiamo utilizzato la definizione di *disinformazione* condivisa dall'Unione Europea e originariamente presentata in un report per il Consiglio d'Europa degli studiosi Claire Wardle e Hossein Derakhshan,[18] che definisce la disinformazione come "informazione falsa creata con l'obiettivo causare un danno." Con disinformazione intendiamo dunque informazione che può essere verificata come falsa e che è creata, presentata e diffusa allo scopo di acquisire un vantaggio economico o di indurre il pubblico volontariamente in errore, e che può essere causa di danni pubblici quali ad esempio minacce alla democrazia ed ai processi democratici, ai beni pubblici, e alla protezione della salute, dell'ambiente o della sicurezza dei cittadini. Questa definizione volontariamente non include errori, satira, o parodia, o informazione partigiana chiaramente

16 Con un giro d'affari di almeno 60 Milioni di dollari dal 2009, secondo lo studio dell'Università di Oxford citato sopra. Possiamo ipotizzare che questa cifra sia in realtà molto più elevata, se si considera che la maggior parte di queste campagne non viene scoperta.

17 European Commission, "Code of Practice on Disinformation," February 23, 2021, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

18 Information disorder: Toward an interdisciplinary framework for research and policy making. C Wardle, H Derakhshan. Council of Europe report 27, 2017.

riconoscibile come tale.

Con il termine *misinformazione*, intendiamo, invece, "informazione falsa diffusa inconsapevolmente". Vi è poi un'ulteriore categoria, quella della *malinformazione*, cioè "informazione che, pur essendo vera, è diffusa con l'obiettivo di causare un danno". Questo può includere, ad esempio, dati personali condivisi allo scopo di minacciare un utente nella vita reale.

Le campagne di influenza possono includere tutti questi diversi tipi di informazione manipolata. In questo studio, tuttavia, ci concentriamo specialmente sulla *disinformazione* come strategia di manipolazione dell'informazione all'interno di gruppi di utenti in relazione di scambio di informazione prolungato nel tempo.

I.4. Il ruolo della coordinazione nella definizione di campagne di disinformazione

Nelle analisi delle campagne di informazione, ci si è inizialmente concentrati su un tipo di strategia che Facebook ha in un primo momento definito come "comportamento coordinato ed inautentico" ("CIB", *coordinated inauthentic behavior*).[19] Il comportamento coordinato fra diversi utenti e "inautentico" ovvero che tramite strategie tecniche (come ad esempio *bots* o *sockpuppets*) o di disinformazione rappresenta un determinato utente o un gruppo di utenti come aventi una diversa identità, è certamente un segnale chiaro di una possibile campagna di informazione. Seguendo questa definizione, tuttora in uso, Facebook (e di conseguenza altre piattaforme digitali e istituzioni) si sono concentrati non tanto sul contenuto di verità di *post* e altre comunicazioni, bensì sulla volontà di indurre gli utenti in errore, presentandosi come attori diversi. Il concentrarsi su questo tipo di azioni ha permesso alle piattaforme digitali di evitare di cadere nella trappola di diventare "arbitri della verità[20]" - rifiutando anche la definizione di "editori", che avrebbe avuto conseguenze legali importanti - e allo stesso tempo agire efficacemente su alcune di queste campagne.

Questo tipo di definizione del problema, seppur utile in un primo momento, è però in via di modifica, anche a causa delle nuove forme che le campagne di informazione stanno prendendo.

Più di recente, infatti, esse hanno raggiunto livelli di sofisticazione maggiori e si sono concentrate sempre di più, piuttosto che sul comportamento "inautentico," sull' utilizzo di *networks* di informazione

19 Per la definizione si rimanda al Glossario. Si veda anche https://m.facebook.com/communitystandards/inauthentic_behavior/.

20 Congressional Hearing of Facebook's CEO Mark Zuckerberg, July 29, 2020 https://www.youtube.com/watch?v=uaivHmHYZ8Y.

già presenti allo scopo di aggiungere una componente "organica"[21] alle campagne che permette maggiore diffusione.

Le campagne di influenza, sempre più frequentemente, hanno come scopo quello di entrare in relazione con utenti *reali* (organici) o cercando di far sì che specifiche narrative, sviluppate da gruppi coordinati, vengano riprese e diffuse oppure, al contrario, amplificando e diffondendo materiale prodotto *organicamente*. Questa evoluzione ha delle conseguenze importanti sia per la concettualizzazione del fenomeno, in quanto diventa meno rilevante identificare comportamenti inautentici, sia per la possibilità di limitarne la diffusione, in quanto il limite fra opinione legittima e operazione di influenza diventa più sfocato.

L'utilizzo di opinioni organiche a scopo strategico, che viene definito come "riciclaggio di narrative" (*narrative laundering*), complica la definizione delle operazioni di informazione; se esse sono diffuse o in alcuni casi persino create da utenti che agiscono in buona fede, sono ancora da considerarsi come operazioni di informazione? E qual è il limite per cui lo Stato può monitorare cittadini che esprimono opinioni in linea con i propri diritti costituzionali?[22] Anche l'iniziale focus sulla componente "straniera" delle operazioni coordinate diventa più complessa e va ridimensionata: come definire operazioni miste, che impiegano sia comportamenti organici che inautentici e attori sia nazionali che stranieri? Cosa intendiamo con attori stranieri? Solo governi nazionali? Oppure anche gruppi di cittadini organizzati?

Ognuna di queste domande ha conseguenze importanti sulle risposte, sia di tipo politico che tecnico, che è opportuno sviluppare.

Le operazioni di informazione vanno dunque definite non esclusivamente come un problema di influenza esterna, ma come una **commistione di influenze in un ecosistema informativo complesso che può includere sia influenze esterne che domestiche e sia comportamenti inautentici che organici.**

Se questo ci aiuta a livello di definizione teorica e analisi scientifica, apre anche però questioni più complesse dal punto di vista della necessaria risposta a livello di relazioni fra paesi e a livello tanto di diplomazia quanto di sicurezza nazionale.

Di fronte ad un grave e urgente rischio di indebolimento del processo democratico dato dalla circolazione di informazioni false e tendenziose, volte a manipolare la pubblica informazione, quali risposte sono

21 Con utenti "organici" intendiamo utenti non parte di campagne coordinate di disinformazione. Si tenga presente che utenti organici possono diventare parte involontariamente di campagne di disinformazione, distribuendo inconsapevolmente narrative e materiale disinformativo.

22 "The Intelligence Community's Role in Countering Malign Foreign Influence on Social Media," Lawfare, August 25, 2020, https://www.lawfareblog.com/intelligence-communitys-role-countering-malign-foreign-influence-social-media.

auspicabili, senza che esse vadano ad intaccare la libertà d'opinione e d'espressione?

I.5. La disinformazione nelle relazioni fra stati, strumento legittimo o interferenza sulla sovranità nazionale?

Da un punto di vista di relazioni fra stati, capire a quale livello e in che occasioni le campagne di informazione vadano definite come influenze straniere è necessario, così come è necessario operare una riflessione sulla legittimità di queste tecniche di manipolazione dell'opinione.

Diffondere informazione che avvantaggia uno stato straniero non è di per sé illegittimo e non va visto in ogni caso come un'operazione di influenza. Si pensi, ad esempio, alla diplomazia digitale, ovvero l'uso che istituzioni straniere possono fare di canali digitali per diffondere informazioni direttamente, anche ad un'audience composta da cittadini di altri Stati. Questo tipo di campagne, anche quando diffondano informazione falsa, può essere ritenuto legittimo nel contesto delle relazioni fra Stati. Si pensi, invece, al caso in cui informazione falsa diffusa da *account* che impersonano cittadini di uno Stato e loro *sockpuppets* abbia lo scopo di manipolare i risultati di una votazione. In questo caso la stessa informazione, trasmessa però tramite inganno sulla *fonte* dell'informazione, diventa problematica e, per alcuni, da identificare nel contesto della *guerra ibrida*. È dunque l'elemento di inganno sulla fonte, piuttosto che il contenuto di verità stesso dell'informazione, a risultare spinoso? O è invece ogni tentativo di manipolazione dell'opinione pubblica ad essere contrario alle buone relazioni fra Stati? O, ancora, ci si deve concentrare sul contenuto di verità? Un'informazione falsa diffusa da fonti chiare è più o meno pericolosa, più o meno illegittima di un'informazione vera diffusa da fonti manipolate?

Secondo alcuni studiosi, tra cui James Pamment[23] la proiezione di informazione "può essere definita al meglio come *l'interferenza negli affari interni di un altro stato sovrano*." In questo senso, bisogna domandarsi se "il rispetto per la sovranità" dal punto di vista della diffusione di informazione sia da considerarsi come regola assoluta, al pari della proibizione di intervento (militare) nei confronti di un altro stato. Da un punto di vista di diritto internazionale è legittimo influenzare - o tentare di influenzare - la popolazione di uno stato sovrano?

Oltre alla già citata difficoltà di misurare l'effettiva influenza delle campagne di informazione, c'è anche un'ulteriore problematica teorica

23 Hedvig Ördén Pamment James, "What Is So Foreign About Foreign Influence Operations?," Carnegie Endowment for International Peace, accessed May 26, 2021, https://carnegieendowment.org/2021/01/26/what-is-so-foreign-about-foreign-influence-operations-pub-83706.

legata alla mancanza di linee guida esatte nel diritto internazionale che permettano di definire chiaramente cosa costituisca un chiaro elemento di coercizione nel contesto dell'interferenza straniera durante attività elettorali. Per esempio, possiamo considerare le operazioni di informazione come contrarie al principio di non intervento?[24]

Nel rispondere a queste domande, si ravvisa intanto l'importanza che la trasparenza delle fonti ha per la definizione della legittimità dell'informazione. L'informazione falsa o tendenziosa diffusa da fonti chiare è preferibile ad informazione falsa diffusa da fonti manipolate. Da questo, ne consegue che una prima efficace misura per rispondere alla disinformazione dev'essere quella di assicurare quanto più possibile la trasparenza per quanto riguarda l'informazione, che può essere facilitata da un lato da una maggiore trasparenza richiesta alle piattaforme e al governo in caso di scoperta di operazioni di influenza (con qualche caveat, che vedremo più avanti) e dall'altro ampliando in maniera sistematica i programmi di alfabetizzazione mediatica rivolti alla popolazione. Si tratta di ampliare la robustezza istituzionale e sistemica ai tentativi di influenzare l'opinione pubblica tramite contromisure concentrate sull'ampliare le capacità di comprensione del fenomeno tanto delle istituzioni, quanto della popolazione.

Accanto a queste misure, volte a incrementare la capacità istituzionale e della popolazione, un ruolo importante giocano le piattaforme digitali e le soluzioni che esse possono mettere in campo (ad esempio eliminare *account* inautentici, o limitare la possibilità di pubblicità di natura politica). La maggior parte delle piattaforme ha lavorato, negli ultimi anni, in questo senso, grazie anche alla pressione politica e istituzionale ricevuta tanto da singoli stati quanto a livello multilaterale, ad esempio dal *Code of Practice on Disinformation* dell'Unione Europea[25]. Nonostante questo sia un ottimo inizio, tuttavia, il *Code of Practice* rimane un accordo su base volontaria, non sufficiente, da solo, a porre il giusto tipo di pressione sulle piattaforme. Su questo punto, la Commissione Europea ha recentemente introdotto, il 15 Dicembre 2020, il *Digital Service Act*, un nuovo pacchetto legislativo che introduce una regolazione più stringente per le piattaforme[26].

24 Ibid.

25 Per un'analisi più approfondita del Code of Practice si rimanda alla relativa sezione in questo studio, a pag. 17 del report

26 Per una lettura più accurata del Digital Service Act, si rimanda alla relativa sezione in questo studio

I.6. Costruendo una via futura, suggestioni di ricerca

Per incrementare la comprensione del fenomeno, ed elaborare risposte politiche e legislative adeguate, è necessario lavorare su alcuni aspetti principali:

- Da un lato, i governi dovrebbero lavorare sul comprendere meglio come l'ecosistema dell'informazione nel suo complesso, in particolare analizzando come la disinformazione si crei e diffonda in ambito sia nazionale che internazionale, sia sui *social media* che sui media tradizionali, e sia da parte di gruppi organizzati che di utenti cosiddetti "organici." In una prospettiva di lungo termine, c'è la necessità che queste ricerche si concentrino anche sulla valutazione degli effetti e dell'influenza[27].
- Dall'altro, le istituzioni devono avere una comprensione specifica tanto dei *network* di informazione e disinformazione operanti nel Paese, così come delle tattiche e delle strategie che in esse sono utilizzate allo scopo di manipolare l'informazione.
- Vi è, inoltre, anche un problema di valutazione dell'efficacia delle contromisure alla disinformazione che sono state fin qui sviluppate. Per esempio, quanto sappiamo dei risultati di operazioni di *deplatforming*[28]? La nostra ricerca sui gruppi legati al *network* di QAnon in Italia cerca di analizzare la questione anche da questo tipo di prospettiva.

I.7. Un problema complesso, una soluzione multilaterale. Collaborazioni pubblico privato e ruolo della stampa

Negli ultimi anni, si andata intensificando l'aspettativa da parte del pubblico che le organizzazioni internazionali ed i governi abbiano un maggiore controllo sulle operazioni di informazione che avvengono sulle piattaforme digitali, specialmente sui *social media*. Questa è una tendenza in crescita, che vediamo anche negli Stati Uniti ed in altri paesi europei ed extraeuropei, e che è andata ad intensificarsi durante la pandemia di COVID-19, alla quale si è affiancata ciò che l'Organizzazione Mondiale della Sanità descrive come un'*infodemia*[29], cioè un momento di particolare

27 Anastasia Kapetas et al., "The Case for a 'Disinformation CERN'," The Strategist, May 18, 2021, https://www.aspistrategist.org.au/the-case-for-a-disinformation-cern/?mc_cid=1f4b166eb8&mc_eid=1707f28241.

28 Con questo termine si intendono tutte quelle misure, e in particolare il ban, che impediscono ad un utente l'accesso ad una piattaforma digitale.

29 "Infodemic," World Health Organization (World Health Organization), accessed June 14, 2021, https://www.who.int/health-topics/infodemic.

diffusione di mis- e disinformazione durante la pandemia di COVID-19, con conseguenze importanti anche dal punto di vista sanitario. Questa situazione ha creato una maggiore presa di coscienza del problema da parte della popolazione a livello globale ed ha sortito un effetto di spinta sulle istituzioni per cercare una risposta più proattiva a questo problema.

Anche se c'è un'alta aspettativa da parte della popolazione che i governi e i servizi segreti nazionali monitorino le campagne di informazione sui *social media*, in realtà questo tipo di attività è ancora limitato e per diverse ragioni.

Da un lato, il monitoraggio di attività *online* dei cittadini va in diretto contrasto con la necessità di rispettare il principio costituzionale della libertà di espressione, specialmente dal momento in cui le risorse pubbliche e il tipo di controllo sui cittadini che ne potrebbero derivare sono oggi molto più pervasivi di quanto potessero essere 10 anni fa.

I governi nazionali, così come le organizzazioni internazionali - per esempio l'Unione Europea - sono ora in una fase delicata, in cui hanno riconosciuto l'importanza delle operazioni di informazione per la sicurezza nazionale e per il mantenimento della democrazia, e tuttavia devono ancora elaborare le adeguate risposte politiche, legislative e operazionali per rispondere a questa problematica. Vi sono, infatti, molteplici problemi sia a livello pratico che legislativo riguardo alla possibilità dei governi di lavorare sulle operazioni di informazione e sul come posizionare il lavoro delle agenzie governative e dell'intelligence.

Se da un lato, come osservato in precedenza, le operazioni di informazione possono in alcuni casi essere assimilate a strategie di guerra ibrida, queste utilizzano in molti casi contenuti e attività *legali*. Diversamente da quanto avviene, infatti, per altre tipologie di contenuto "distruttivo" (disruptive) come contenuto di tipo terroristico o di pedofilia, il contenuto di disinformazione spesso ricade al di la di una dimensione di illeceità per l'ordinamento, e dunque dell'area di operazione dei servizi di *intelligence* o governativi.

Vi è poi da chiarire ancora chi sia a dover assicurare una corretta pubblica informazione, specialmente in un momento di crisi, i governi nazionali o le piattaforme digitali? La questione rimane aperta, poiché i bilanciamenti di potere fra queste istituzioni sono in via di evoluzione.

Ci troviamo di fronte ad un nuovo ecosistema dell'informazione, non più controllato dalla stampa professionale, che basava il proprio lavoro su di un accesso ad informazioni riservate ed un lavoro di certosino controllo dell'informazione, ma al contrario in un sistema in parte aperto, in cui il problema non è più avere accesso ad informazione limitata e riservata ma, piuttosto, ordinare una grande quantità di dati e informazioni di pubblico accesso che sono però controllate da compagnie private e - dal punto di vista italiano - straniere, le quali diffondono informazioni estremamente limitate sia sull'utilizzo che esse fanno di questi dati, che sul funzionamento

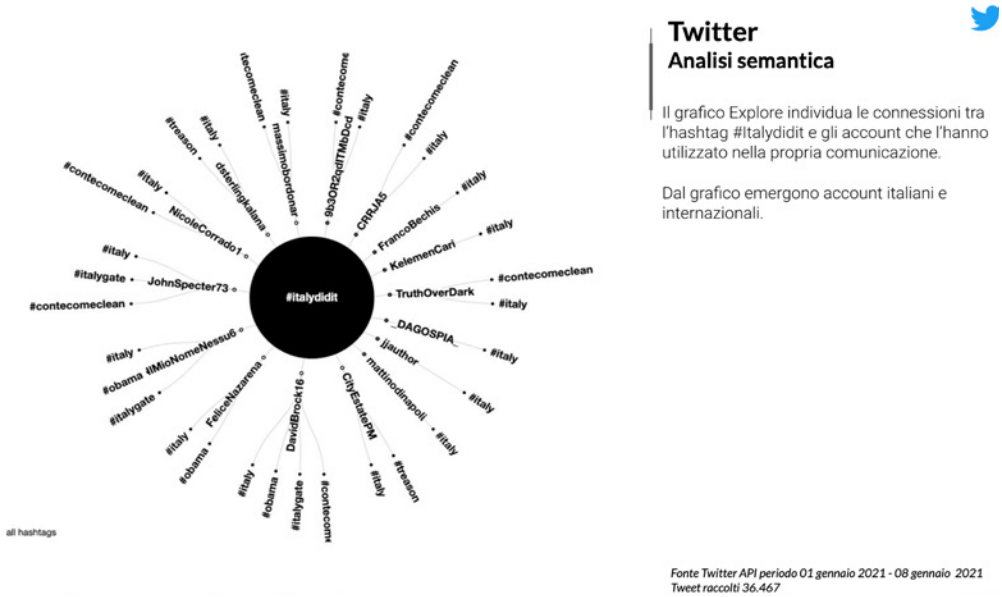
delle piattaforme e della prioritizzazione e il monitoraggio del contenuto, incluso quello fondamentale per le istituzioni a livello strategico. Alcuni segnali incoraggianti vengono dalle piattaforme in termini di cresciuto interesse per la trasparenza e la collaborazione con le istituzioni pubbliche, ma non si è ancora arrivati ad un accordo sui ruoli e le responsabilità che pubblico e privato ricoprono di fronte alla necessità di salvaguardare il discorso pubblico.

Se infatti, da un lato, le istituzioni hanno l'interesse primario e le capacità di intelligence per lavorare sulle campagne di informazione, non hanno però accesso all'enorme quantità di dati di cui le piattaforme digitali dispongono e che permettono un monitoraggio più efficace. Vi sono stati casi episodici di collaborazione e scambio di dati, ma non si è ancora arrivati ad un flusso di lavoro formalizzato, che sarebbe necessario alle istituzioni per un monitoraggio adeguato.

Ne consegue, che da un punto di vista strategico, le istituzioni, ed in particolare le istituzioni italiane, abbiano la necessità di coprire un divario di accesso all'informazione, tramite una collaborazione più stretta con le piattaforme digitali, e con la ricerca accademica.

Non sono però solo le istituzioni ad avere necessità di una maggiore comprensione del fenomeno. L'analisi di queste campagne di informazione è molto spesso difficile da portare avanti anche per redazioni giornalistiche tradizionali, le quali hanno in linea di massima budget e tempi limitati, e spesso non dispongono delle capacità tecniche per portare avanti queste investigazioni. I media tradizionali non possono dunque prendere in carico il necessario lavoro di monitoraggio e analisi di cui queste campagne necessitano, e hanno anch'esse bisogno di lavorare di concerto con piattaforme digitali, università e istituzioni.

Similmente, in un contesto nel quale aziende private sono anch'esse soggette a campagne di disinformazione e ad attacchi *cyber*, è necessario che esse siano in grado di attingere ad un database che le aiuti a comprendere l'ecosistema informativo. Si pensi, ad esempio, al caso della Leonardo SPA, recentemente vittima di un attacco di propaganda secondo il quale avrebbe avuto un ruolo nel truccare le elezioni americane a vantaggio del candidato democratico, Joe Biden. Questo caso è stato analizzato da noi nel contesto del lavoro sul *network* di informazione legato alla cospirazione QAnon. Grazie al nostro lavoro precedente su *influencer* e nodi di informazione, siamo stati in grado di osservare velocemente il nascere ed il diffondersi della campagna, parte di una narrativa più ampia legata agli slogan *"Italy did it"* e *"Conte come clean"*, secondo i quali il sistema Italia sarebbe stato coinvolto nel manipolare le elezioni americane a favore del candidato democratico ai massimi livelli di governo e dello Stato. Secondo questa teoria della cospirazione, diffusa in contemporanea all'assalto al Campidoglio americano del 6 Gennaio 2021, il Presidente della Repubblica Italiana, Sergio Mattarella, sarebbe



stato in realtà un agente dei servizi segreti britannici, mentre l'allora Primo Ministro, Giuseppe Conte, avrebbe operato di concerto con l'ex Presidente americano Barack Obama e il Senatore della Repubblica Matteo Renzi, allo scopo di manipolare le elezioni americane. Questa campagna, che ha avuto fra i proponenti anche figure rilevanti della politica americana, come il Generale Michael Flynn, ex consigliere per la sicurezza nazionale dell'amministrazione Trump ed ora figura rilevante dell'ambiente della cospirazione americano, ha coinvolto anche la Leonardo SPA, all'epoca recentemente vittima anche di un attacco cibernetico.

Seppur questo caso non abbia guadagnato molta trazione, è un chiaro esempio di come l'interesse strategico del Paese, sia pubblico che privato, venga attaccato da simili operazioni, che richiedono una risposta in cooperazione fra istituzioni pubbliche e private, università, società civile, e stampa tradizionale.

Dobbiamo chiederci: quali devono essere le risposte strategiche delle istituzioni? Mentre c'è stata un'evoluzione dal punto di vista della risposta ad operazioni di sicurezza cibernetica, non vi è ancora la necessaria comprensione del rischio da un punto di vista della disinformazione.

I.8. Verso una strategia per analizzare e monitorare operazioni di disinformazione: modelli e problematiche

Dopo aver rilevato l'importanza di contenere le operazioni di informazione per la stabilità democratica e per il governo del Paese, è importante concentrarsi su quali siano i metodi migliori per monitorare campagne e gruppi con un potenziale rischio sociale e per il discorso pubblico.

Per fare questo, è necessario introdurre un modello di comportamento che la ricerca e le istituzioni devono avere riguardo a operazioni di informazione: questo modello deve, a nostro avviso, costituirsi di 3 fasi:

- Comprensione
- Monitoraggio
- Prevenzione

Comprensione: Innanzitutto, la pubblica amministrazione deve investire su di una comprensione maggiore del rischio strategico e del potenziale impatto di queste campagne. In questo senso, è importante che il lavoro di ricerca si concentri sull'identificare *network* e gruppi di utenti particolarmente soggetti ad amplificare contenuti falsi e manipolati e ad identificarne tattiche e strategie.

Monitoraggio: Una volta comprese le dinamiche di trasmissione dell'informazione, così come le tattiche e le strategie di diffusione, c'è necessità di un monitoraggio regolare delle narrative più diffuse e dell'evoluzione delle tattiche utilizzate. Questi studi devono avvenire su base continuativa, poiché se ci si concentra su campagne attive o già esistenti si creano due problemi: 1) da un lato, utilizzare gli stessi schemi di ricerca porta a rinvenire sempre gli stessi modelli, trascurando gli altri 2) dall'altro si dà modo agli attori di modificare le proprie tattiche e strategie per evitare il rilevamento.

Prevenzione: Una volta compreso come le operazioni di informazione possano modificare l'opinione pubblica, quali siano i gruppi maggiormente attivi, e il tipo di tattiche e strategie che impiegano, sarà possibile identificare narrative prima che esse entrino in circolo e si diffondano, in modo tale da reagire con misure preventive. Per esempio, diffondendo informazione accurata durante momenti di incertezza, nei quali è più facile che si diffonda disinformazione.

I.9. Modelli

In questo studio, per quanto riguarda la parte di ricerca etnografica, ci si è affidati al modello del Media Manipulation Cycle, sviluppato del gruppo di ricerca *TASC* dello *Shorenstein Center for Media*, Politics, e *Public Policy* della Harvard Kennedy School.[30] Utilizzando questo metodo di ricerca, che si concentra sull'utilizzo dei manufatti di manipolazione dell'informazione, i nostri ricercatori sono stati in grado di rilevare alcune delle principali tattiche di manipolazione dell'informazione utilizzate da

30 Per una spiegazione dettagliata della ricerca e della metodologia v. https://mediamanipulation.org/. Per una traduzione in italiano delle tecniche di manipolazione dell'informazione, si rimanda al glossario a pag 53

due gruppi domestici: da una parte i teorici della cospirazione legati a QAnon, e dall'altra alcuni gruppi anti vax attivi in Italia.

Accanto a questo modello, è utile portare anche l'attenzione su un framework di analisi che abbiamo utilizzato da un punto di vista teorico e di sviluppo della ricerca. Si tratta del cosiddetto modello ABC[31], sviluppato da Camille François di Graphika, un'agenzia di analisi e mapping di *social media*. Questo modello si concentra sullo studio di **A**ttori manipolativi, Comportamenti (***B**ehaviors*) ingannevoli e **C**ontenuto dannoso come vettori tipici della manipolazione virale e che possono guidare risposte del regolatore e dell'industria e si applica bene sia all'analisi di campagne di disinformazione, che negli ambiti della *cybersecurity*, del monitoraggio del contenuto, ed altri ambiti ad essi collegati.

Secondo questi due modelli, abbiamo costruito il lavoro per rispondere alle seguenti domande di ricerca:

- Chi sono i gruppi che diffondono e, in alcuni casi, producono disinformazione in Italia?
- Quali sono le tattiche e le strategie di manipolazione dell'informazione che utilizzano?
- Quali piattaforme sono maggiormente utilizzate?
- Quali narrative provenienti da gruppi stranieri o italiani sono particolarmente efficaci in Italia?
- Qual è il quadro legislativo esistente in Italia e quali sono le politiche e le misure normative adottate nel contesto internazionale (Unione Europea, Francia, Germania, Stati Uniti)?
- Quali soluzioni operative e/o di *policy* sono adeguate a rispondere a questa minaccia?

I.10. Risposte di *policy*

Alla ricerca sulle tattiche di manipolazione dell'informazione è seguita un'analisi delle risposte politiche e legislative.

Governi nazionali da una parte, e piattaforme digitali dall'altra, negli ultimi anni hanno largamente incrementato la propria capacità di analisi e comprensione del fenomeno, posizionandosi però su posizioni diverse anche se in parte complementari. Queste diverse posture sono causa del diverso accesso ai dati e delle diverse capacità di analisi che piattaforme digitali e stati nazionali hanno. Da un lato, le piattaforme digitali hanno un

31 François, C. (2019). Actors, Behaviors, Content: A Disinformation ABC Highlighting Three Vectors of Viral Deception to Guide Industry & Regulatory Responses (One). Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression.

accesso maggiore ai dati e una comprensione del modo e della misura in cui le infrastrutture digitali influiscono sull'ecosistema informativo, in particolare, il funzionamento dell'algoritmo, ovvero del sistema automatizzato che determina il contenuto mostrato agli utenti. Dall'altro, i governi non hanno accesso a informazioni essenziali per la comprensione dell'ecosistema informativo, ma hanno accesso a dati personali dei cittadini, in molti casi essenziali per un'investigazione accurata delle campagne di informazione.

Le piattaforme digitali stesse hanno inoltre una capacità limitata di comprendere campagne di disinformazione che si svolgono su molteplici piattaforme.

Molti Stati Europei non riconoscono ancora pienamente il problema, allocando solo risorse limitate e insufficienti allo studio del fenomeno e all'elaborazione di risposte adeguate.[32] Mentre alcuni Stati, fin da subito oggetto di campagne di informazione aggressive, hanno sviluppato più rapidamente una consapevolezza della necessità di dotarsi di strumenti di *policy* adeguati, altri, come ad esempio la Spagna, a seguito del referendum in Catalogna hanno sviluppato questa consapevolezza più di recente. Questa divergenza di vedute è riflessa anche nel dibattito interno all'Unione Europea e ha rallentato la creazione di linee guida efficaci.

Negli ultimi anni, l'Unione Europea ha sviluppato una serie di politiche riguardanti la disinformazione che sono complesse e multilivello, nonché articolate in diversi strumenti regolatori e di analisi. Tra questi: la Comunicazione "Contrastare la disinformazione *online*: un approccio europeo[33]", il *Code of Practice on Disinformation*[34] al quale le piattaforme possono aderire su base volontaria (fra gli attuali firmatari: Facebook, Twitter, Google, TikTok, Mozilla), il Piano d'azione contro la disinformazione[35] preparato congiuntamente dalla Commissione e dall'EEAS, la *East StratCom Task Force*,[36] ed il *Rapid Alert System*,[37] che

32 "Democratic Defense against Disinformation 2.0," Atlantic Council, February 4, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/democratic-defense-against-disinformation-2-0/.

33 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling online disinformation: a European Approach, COM/2018/236 final, accessed June 14, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236

34 European Commission, "Code of Practice on Disinformation," February 23, 2021, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

35 EEAS, "Action Plan against Disinformation," May 12, 2018, https://eeas.europa.eu/headquarters/headquarters-homepage/54866/action-plan-against-disinformation_en.

36 Part of the StratCom Task Force work is available here: https://euvsdisinfo.eu/

37 Si veda "The EU's Rapid Alert System against Disinformation and How It Functions," europarl.europa.eu, accessed June 14, 2021, https://www.europarl.europa.eu/doceo/document/E-9-2020-006819_EN.html.

facilita la cooperazione anche con altri gruppi multilaterali come la NATO e il G7, così come con le piattaforme.

Il 26 Maggio 2021, la Commissione Europea ha inoltre presentato una guida su come migliorare il *Code of Practice Anti-Disinformation* che si concentra sul ruolo delle piattaforme. Nel presentare questo nuovo modello di lettura del codice Věra Jourová, Vice Presidente per i Valori e la Trasparenza della Commissione ha osservato come: "Le minacce poste dalla disinformazione *online* sono in rapida evoluzione e dobbiamo intensificare la nostra azione collettiva per responsabilizzare i cittadini e proteggere lo spazio informativo democratico." È necessario un nuovo Codice più forte che responsabilizzi ulteriormente le piattaforme, aumenti il controllo pubblico su di esse e che minimizzi il ritorno economico della disinformazione, allo scopo di preservare la libertà di parola[38].

Oltre a questo, nel 2020–2024 *European Democracy Action Plan*[39] si include linguaggio specifico di impegno a proiettare valori democratici nel mondo e un significativo impegno di *policy* all'intersezione di disinformazione, protezione elettorale, tecnologie digitali e partenariato pubblico-privato. Ma lo strumento più recente, e certamente più interessante per comprendere il potenziale sviluppo dei regolamenti europei relativi alla disinformazione è il *Digital Services Act*[40] che introduce misure di responsabilizzazione delle piattaforme digitali e un rilevante apparato di *enforcement* nazionale ed eurounitario. Anche se alcuni studiosi sono scettici sul fatto che il *DSA* possa sussumere completamente la regolazione relativa alla disinformazione, questo strumento offre qualche motivo di ottimismo.[41]

Dal punto di vista degli stati nazionali, lo scopo primario dev'essere sia quello di identificare, monitorare, e prevenire le azioni distruttive di "*bad actors*" con interessi strategici in Paesi democratici, particolarmente in Paesi *target*, come l'Italia[42] che quello di comprendere i *network* di "disinformazione" presenti nel Paese e le loro tattiche e strategie di

38 "Commission Presents Guidance to Strengthen the Code of Practice on Disinformation," European Commission - European Commission, accessed June 14, 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2585.

39 European Commission, "Action plan against disinformation", retrieved June 6, 2021, from https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250

40 Directorate-General CONNECT of the European Commission. "The Digital Services Act package", 15 December 2020, Retrieved December 29, 2020 from https://ec.europa.eu/digital-single-market/en/digital-services-act-package. The DSA is part of a "regulatory package" that includes also a Digital Markets Act https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

41 Shattock, E. (2021). Self-regulation 2:0? A critical reflection of the European fight against disinformation. Harvard Kennedy School (HKS) Misinformation Review. https://doi.org/10.37016/mr-2020-73

42 Sciubba Caniglia, Costanza. "Signs of a new world order: Italy as the COVID-19 disinformation." The Harvard Kennedy School Misinformation Review 1, no. 3 (2020). DOI: 10.37016/mr-2020-018

diffusione dell'informazione.

Come osservato in precedenza, le operazioni di informazione negli ultimi anni si sono evolute sempre più verso l'utilizzo di *network* organici nei paesi *target*. Dunque, lo studio e il monitoraggio continuo di comunità che promuovono disinformazione, anche organicamente, può permettere di identificare queste operazioni di informazione nei loro stadi iniziali, consentendo così una risposta adeguata in tempi rapidi.

Si pensi ad esempio, come rilevato dalla nostra ricerca sui gruppi anti vax attivi in Italia, ad alcuni gruppi chiusi su Facebook che promuovono cure anti-COVID-19 a domicilio, che comprendono anche l'uso di hydroxy clorochina, farmaco non riconosciuto per la cura anti COVID-19 dalle autorità sanitarie italiane. Seppure le attività del gruppo non rientrino nella fattispecie dell'illegalità, in quanto solo promotori di un tipo di terapia non riconosciuta che però affermano di non mettere in pratica, in realtà l'esistenza (pubblicizzata in questi gruppi) di *networks* di personale sanitario volontario simpatetico con queste proposte, che può essere contattato per cure domiciliari, pone alcuni dubbi sulla diffusione di queste terapie. Bisogna dunque chiedersi quale sia il ruolo delle autorità nel vigilare sulla diffusione e pubblicizzazione di *network* che possono avere conseguenze importanti per la salute pubblica.

Come osservato da Joan Donovan e dal gruppo di ricerca della Harvard Kennedy School TASC in una recente comunicazione allo Special Rapporteur delle Nazioni Unite,[43] limitare la disinformazione non è un limite alla libertà di espressione ma, al contrario è **necessario** per il rispetto del diritto alla libertà di espressione e di opinione, così come previsto dall'Articolo 19 della Dichiarazione Universale dei Diritti Umani.[44]

La questione diventa dunque: posto che c'è una necessità di comprendere le operazioni di informazione attive nel nostro Paese, e gli attori che ne sono promotori, siano essi statuali o non, stranieri o domestici, e che queste operazioni presentano molteplici difficoltà sia in termini di monitoraggio, attribuzione, e controllo incidentale di utenti che partecipano "organicamente" e in maniera involontaria e senza uscire dai limiti dei propri diritti costituzionali, cosa dovrebbero fare i governi e le istituzioni per monitorare e limitare l'incidenza di queste operazioni senza limitare la libertà di espressione e di opinione dei propri cittadini?

Nella sezione seguente, abbiamo raccolto alcune raccomandazioni pratiche, divise per temi, che possono servire per una prima delineazione della questione e per iniziare a disegnare linee di intervento. Si tratta,

43 "Submission to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," Media Manipulation Casebook, accessed June 14, 2021, https://mediamanipulation.org/research/submission-un-special-rapporteur-promotion-and-protection-right-freedom-opinion-and.

44 The United Nations. 1948. Universal Declaration of Human Rights. Accessed June 14, 2021. https://www.ohchr.org/en/udhr/pages/Language.aspx?LangID=itn.

come fin qui osservato, tuttavia, di un ambito nuovo ed in evoluzione. Queste raccomandazioni vanno dunque intese come preliminari, e richiederanno in futuro maggiori risorse di ricerca per evolversi in contemporanea con l'evoluzione delle piattaforme e dell'ambiente dell'informazione che su di esse si sviluppa.

I.11. Raccomandazioni[45]

Lo scopo principale di queste raccomandazioni è di offrire linee guida per comprendere e monitorare operazioni di informazione che mirano a intervenire nel sistema democratico, mantenendo allo stesso tempo fermi i valori della libertà di espressione.

Queste raccomandazioni pratiche sono rivolte in prima battuta al Ministero degli Esteri e all'Amministrazione Pubblica in generale, e in secondo luogo ad organizzazioni pubbliche e private incluse le piattaforme digitali, le aziende, le università e la società civile.

A livello strategico, le priorità devono essere quelle di:

- **Promuovere e diffondere definizioni e *framework* comuni**
  - ◊ Non c'è ancora, a livello sia nazionale che internazionale, un modello condiviso tanto di analisi quanto di rilevamento delle campagne di disinformazione. Questo rende difficile il confronto fra attori diversi e campagne diverse. C'è necessità di sviluppare definizioni e *framework* comuni, da diffondere pubblicamente e rendere disponibili, in particolare, alla stampa tradizionale e alle redazioni.[46]
  - ◊ Stabilire un modello di notifica specifico per le elezioni politiche e promuoverne l'uso tra ricercatori universitari, organizzazioni private, piattaforme e istituzioni pubbliche.

- **Incrementare la capacità di analisi e monitoraggio delle pubbliche istituzioni**
  - ◊ Prevedere l'aumento di capacità di analisi e monitoraggio delle campagne di informazione tramite l'investimento e l'assunzione di figure specializzate che lavorino all'interno della pubblica amministrazione.

45 Per le raccomandazioni relative alle policy giuridiche, rimandiamo alla relativa sezione in questo studio, a pag. 41

46 Jon Bateman and Craig Newmark, "Social Media Disinformation Discussions Are Going in Circles. Here's How to Change That.," Slate Magazine (Slate, March 24, 2021), https://slate.com/technology/2021/03/online-disinformation-congressional-hearing-amazon-google-twitter-ceos.html.

- ◊ Stabilire una *task force* indipendente di monitoraggio e risposta rapida interministeriale attiva su base continuativa, che abbia il compito di informare il governo e - in caso di necessità - alleati e piattaforme digitali riguardo a campagne di disinformazione emergenti.[47] La *task force* avrà inoltre il compito di riferire in Parlamento su base regolare. In vista delle Elezioni politiche, prevedere l'apertura di un'agenzia governativa dedicata, sul modello di quella Francese[48] e Statunitense[49].
- ◊ Lavorare fin da ora per stabilire una collaborazione *ad hoc* tra Università, istituzioni pubbliche, piattaforme digitali, gruppi di monitoraggio dell'informazione privati, e giornalisti per facilitare il lavoro di monitoraggio e analisi della disinformazione durante le Elezioni.
- ◊ In vista delle prossime Elezioni politiche, collaborare fin da ora con le piattaforme perché incrementino le proprie capacità di analisi interne con esperti del contesto italiano, in linea con quanto promosso da altri Paesi Europei.
- ◊ Per lo sviluppo di capacità tecniche e di analisi non esistenti nella pubblica amministrazione, prevedere fondi alla ricerca universitaria da utilizzare anche allo scopo di facilitare la coordinazione con le piattaforme digitali.[50]

- **Creare collaborazioni con istituzioni sia pubbliche che private, tanto a livello nazionale che multilaterale**
  - ◊ Creare una **Coalizione Anti-Disinformazione** a livello di Unione Europea e in collaborazione con altri Stati democratici allo scopo di riunire regolarmente esperti governativi e non-governativi, comprese piattaforme digitali e di *social media*, stampa tradizionale, università, e gruppi della società civile[51].
  - ◊ Promuovere l'adesione ad iniziative di collaborazioni quali sul

47 "Democratic Defense against Disinformation 2.0," Atlantic Council (blog), June 13, 2019, https://www.atlanticcouncil.org/in-depth-research-reports/report/democratic-defense-against-disinformation-2-0/.

48 AFP. "France Creates Agency to Fight Foreign Disinformation." DAWN.COM, June 3, 2021. https://www.dawn.com/news/1627160/france-creates-agency-to-fight-foreign-disinformation.

49 Per un altro esempio di una simile gruppo di lavoro si veda il nuovo gruppo di lavoro creato dall'ODNI Office of the Director of National Intelligence degli Stati Uniti. Martin Matishak, "Intelligence Community Creating Hub to Gird against Foreign Influence," POLITICO, accessed May 26, 2021, https://www.politico.com/news/2021/04/26/intelligence-community-hub-foreign-influence-484604.

50 Jacob N. Shapiro Wanless Natalie Thompson, Alicia and Jacob N. Shapiro Wanless Natalie Thompson, Alicia, "Research Collaboration on Influence Operations Between Industry and Academia: A Way Forward," Carnegie Endowment for International Peace, accessed May 25, 2021, https://carnegieendowment.org/2020/12/03/research-collaboration-on-influence-operations-between-industry-and-academia-way-forward-pub-83332.

51 Per un'elaborazione su questo tema si veda: https://www.atlanticcouncil.org/wp-content/uploads/2018/03/Democratic_Defense_Against_Disinformation_FINAL.pdf

modello **"CERN della disinformazione"**[52] per incrementare lo scambio a livello di ricerca universitaria fra Paesi democratici e aiutare le istituzioni a comprendere meglio l'entità del problema e promuovere l'accesso ai dati delle piattaforme e lo scambio di informazioni.

- **Promuovere un'informazione pubblica puntuale e maggiore alfabetizzazione mediatica nella popolazione**
  - ◊ Aumentare la trasparenza e la velocità dell'informazione pubblica, allo scopo di riempire vuoti di informazione e limitare lo spazio per campagne di disinformazione. Se un'informazione ufficiale, accurata, e accessibile non è disponibile, i cittadini saranno portati a cercare informazione da fonti inattendibili, particolarmente in momenti delicati come un attacco terroristico, la pandemia, o elezioni politiche. Se prima dell'avvento dei *social media*, le istituzioni potevano aspettare di avere notizie confermate prima di rilasciare dichiarazioni, questo non è più sufficiente, poiché un vuoto informativo lascia spazio ad attori che hanno interesse a promuovere narrative false in momenti di crisi. In caso di incertezza, le autorità hanno il compito **riempire questo vuoto, quando necessario annunciando la mancanza di informazioni definitive e stabilendo i canali ufficiali come canali in cui l'informazione sarà disponibile appena verificata**. In questo modo, la popolazione può valutare dove trovare informazione accurata e, per converso, è informata che informazione verificata non è ancora disponibile.
  - ◊ Prevedere fondi strutturali per l'università e la scuola, così come da destinare ad organizzazioni senza scopo di lucro che abbiano la finalità di incrementare e promuovere l'**alfabetizzazione mediatica** della popolazione.
  - ◊ Prevedere **investimenti pubblici o incentivi per le redazioni giornalistiche per la formazione tecnica di giornalisti** volta a incrementare la comprensione delle tattiche di manipolazione dell'informazione e delle moderne tecniche di reporting. I giornalisti devono imparare tanto tecniche quali l'identificazione di siti falsi, di contenuto sintetico, e di campagne coordinate, quanto la teoria dei modi più appropriati di riportare le notizie relative a campagne di disinformazione, per evitare di amplificarne la portata.

52 Anastasia Kapetas et al., "The Case for a 'Disinformation CERN'," The Strategist, May 18, 2021, https://www.aspistrategist.org.au/the-case-for-a-disinformation-cern/?mc_cid=1f4b166eb8&mc_. Secondo calcoli preliminari questo progetto potrebbe costare intorno ai 10 milioni di dollari, un investimento contenuto se si considera l'impatto che la disinformazione ha avuto, per esempio, anche solo durante la pandemia di COVID-19.

- **Incrementare lo scambio di informazione e di capacità fra Istituzioni e soggetti privati**
  - ◊ Le amministrazioni pubbliche soffrono di una mancanza di accesso ai più recenti strumenti di *software* per l'investigazione forense e l'analisi dei dati legati a operazioni di informazione. Bisogna dunque prevedere, così come per l'Agenzia Nazionale di *Cyber Security,* collaborazioni con aziende private che sono provviste di queste capacità sia di conoscenza tecnica che di *software*.
  - ◊ Stabilire un comitato, presieduto da diversi esponenti della comunità di intelligence, esperti legali in materie di diritti civili, così come esperti del settore privato, allo scopo di testare e analizzare nuova strumentazione tecnica e nuovi *software*, inclusi di intelligenza artificiale, prima di approvarne l'utilizzo. Questo comitato dovrebbe essere organizzato a livello di Unione Europea.

Casi di studio

I. QAnon

assistente alla ricerca, Alberto Olivieri

I.1. Metodologia

Nel caso di studio relativo a QAnon, abbiamo utilizzato un metodo basato sull'etnografia investigativa digitale. Questo paradigma combina l'etnografia digitale, che è utilizzata solitamente nello studio di comunità digitali e cultura dell'internet, l'etnografia virtuale e tecniche investigative digitali, provenienti dagli studi sul giornalismo e sulla sicurezza. I dati sono stati raccolti per 11 mesi (dall'inizio del 2020, con la crescita del numero di utenti grazie attirati dalla situazione particolare causata dall'emergenza COVID-19, a metà Novembre 2020, una volta terminate le elezioni americane).

Inizialmente, abbiamo identificato una serie di personaggi chiave che portavano avanti la narrativa di QAnon Italia attraverso vari media digitali. Successivamente, abbiamo ricostruito il lavoro di questi agenti

attraverso diverse piattaforme e abbiamo monitorato le loro interazioni e collaborazioni. Espandendo i nostri studi da queste conoscenze iniziali, abbiamo inoltre raccolto dati utilizzando l'API di Twitter e successivamente abbiamo effettuato su di essi un'analisi quantitativa che ci ha permesso di identificare ulteriori personaggi chiave, *hashtag* popolari e livelli di interazione nel tempo. Questo ci ha permesso di riprendere e continuare il lavoro etnografico includendo queste nuove informazioni nelle nostre osservazioni. Durante l'estate del 2020, una parte del team ha osservato e trascritto su diari settimanali l'attività di QAnon su Facebook, Twitter e Telegram, in aggiornamento costante con gli altri membri del gruppo di ricerca. Ad Ottobre/Novembre 2020 abbiamo scaricato e codificato le conversazioni di alcune chat di Telegram seguendo uno schema di codice sviluppato sulle domande di ricerca. Le immagini e i video sono stati archiviati su *Archive.is* e sulla *The WayBack Machine*, o se non possibile altrimenti, tramite *screenshot*.

I.2. Evoluzione Temporale

Nella fase iniziale pre-pandemia e pre-infrastrutturale del 2018-2019, gli *influencer* promuovevano narrative mutuate da quelle degli *account* di QAnon americani. La narrativa utilizzata si limitava a quella d'oltreoceano, senza alcun tentativo di completarla o arricchirla. La presenza di riferimenti al contesto Italiano era sporadica e non particolarmente significativa. Spicca in questa fase l'*influencer* B. (iniziale di fantasia), il quale ha postato una serie di messaggi su Facebook che si collegavano e sostenevano a vicenda, dove la struttura della sua narrativa si basava su un messaggio centrale, il più vecchio, sul quale si sviluppavano tutti i messaggi successivi. L'approccio di B. era quello di postare dei *link* a del materiale originale americano di QAnon usato come "prova" su cui poi sviluppare il discorso dei suoi *post*. Nel tempo, si è creato fra gli utenti un sentimento di appartenenza alla causa di Q che ha facilitato la diffusione della narrativa. Per dare l'idea di quanto importante sia stato l'impatto di questo influencer in questa fase iniziale basta vedere la quantità di *like,* commenti e condivisioni di ogni suo *post*. Nel 2019, questo influencer ha introdotto un gruppo di auto-proclamati «*Italian QAnon Patriots*», chiamato «Oracolo Quantico».

Nella fase pandemica, da Marzo 2020, il numero di *account* italiani legati a QAnon è aumentato notevolmente. Infatti, dall'inizio della pandemia "Oracolo Quantico" diviene uno degli *account* di Twitter più attivi nel panorama italiano. L'*account* cita e ritwitta vari *influencer* di QAnon. B., inoltre, è apparso su *Border Nights Radio*, dove ha insistito sulla presenza enorme di dati controfattuali a supporto di Q. Ha anche invitato le persone a rimanere critiche e ad effettuare il lavoro di ricerca individualmente, perché «se le persone pensano come individui non

possono essere controllate come le masse». Questa è una narrazione tipica delle teorie della cospirazione, che ha lo scopo di convincere di una narrativa particolare e di creare confusione e sfiducia nell'autorità più in generale.

Durante la primavera del 2020, è avvenuto un grosso cambiamento nelle narrative dei QAnon italiani. In questo periodo le teorie di QAnon americane hanno iniziato ad essere modificate ed adattate al contesto italiano-europeo. Un altro cambiamento radicale osservato è stato il lento ma costante spostarsi delle attività da Twitter e Facebook, verso le chat di Telegram.

La terza fase del movimento è stata caratterizzata da una serie di *deplatforming* e dalla narrativa delle elezioni americane. Il *deplatforming* ha colpito duramente anche svariate pagine e *account* seguite dal team. Nonostante questo "bagno di sangue", sulle chat di Telegram non si è quasi per nulla menzionato l'avvenimento. Con l'avvicinarsi delle elezioni è stato notato come il lavoro infrastrutturale degli *influencer* sia diventato più intenso e sofisticato, con nuovi contenuti e articoli pubblicati quasi giornalmente. Finite le elezioni, i livelli di attività delle chat hanno raggiunto volumi tre volte maggiori rispetto a quelli osservati nel periodo precedente. Il quarto giorno dalle elezioni, gli *influencer* che fino a quel momento non si sono più manifestati sulle chat, hanno cancellato tutti i contenuti passati e utilizzato varie strategie di repressione del dissenso, anche in maniera verbalmente violenta, cosa mai successa prima. Questi hanno inizialmente sviluppato una strategia di narrazione che si basava sulla falsa narrativa del furto delle elezioni. Alla conclusione delle nostre osservazioni nei vari gruppi di QAnon era stata accettata la sconfitta, anche se con la "consapevolezza" che il risultato finale fosse stato causato da frodi e la conversazione si è quindi spostata sul promuovere la futura campagna Trump 2024.

I.3. Tattiche

Le tattiche che sono state prese in considerazione dal team sono solo una parte di quelle utilizzate dai vari *influencer*, ma riteniamo siano le più rappresentative di questa operazione di disinformazione.

La tattica degli ***Evidence Collage***, ovvero file di immagine costituiti da screenshot con testo che rappresentano un particolare evento o attività, viene modificata ed adattata alle esigenze della narrativa di QAnon che la esprime in maniera più metodica, con la condivisione di database che raccolgono argomenti, immagini e slogan di precipua importanza dal punto di vista degli attivisti di QAnon. Questa versione alternativa supporta la narrativa interna che rappresenta i membri del movimento QAnon come un «gruppo di ricerca».

Nel ***Viral Sloganeering***, vengono creati messaggi politici o culturali

divisivi cercando di influenzare chi ne viene a contatto, creando un alto livello di engagement che spesso spinge i media tradizionali a "coprire" la narrativa, in questo modo amplificandola involontariamente. Gli slogan possono essere sia già esistenti e adottati per gli scopi degli agenti della manipolazione, sia completamente nuovi e da questi derivanti. Principalmente, vengono utilizzati meme, *hashtag*, poster e video, per la loro facilità di diffusione e per la difficoltà intrinseca di reperirne l'origine. Una campagna di questo tipo eseguita con successo raggiunge una massa di interesse critica che porta gli stessi mainstream media a parlarne, creando ulteriore amplificazione.

La ***Infrastructuring*** è la tattica che consiste nella creazione di infrastrutture agnostiche, ovvero indipendenti dal messaggio che viene veicolato tramite esse, spesso anche multipiattaforma (YouTube, Facebook, Twitter, Telegram). Questa tattica ha dei vantaggi sia per chi la utilizza, sia per chi cerca di limitare il diffondersi delle campagne di disinformazione. Da una parte gli agenti della disinformazione utilizzano questa struttura aperta e rodata per le nuove campagne di disinformazione, dall'altra ricercatori etnografici possono facilmente controllare se determinate campagne o agenti utilizzino un sistema infrastrutturale e quindi monitorare il progresso e la genesi di determinate narrative, potendo sperare di controllarne l'impatto finale.

Ricordiamo che queste sono solo alcune delle tattiche utilizzate e utilizzabili. Sia gli *Evidence Collage* che il *Viral Sloganeering* e molte altre, sono tattiche che sorgono all'attenzione dei ricercatori solamente quando superano una massa critica di interesse nel pubblico a cui queste campagne sono rivolte.

I.4. Raccomandazioni per contrastare le tecniche osservate

Riportiamo di seguito due metodi utilizzabili per poterne contrastare efficacemente la maggior parte:

Il primo metodo consiste nel portare avanti una narrativa alternativa quanto più possibile fattuale e, al tempo stesso, nel cercare di distanziarsi dalle altre narrative che condividono l'obiettivo di contrastare la tattica di disinformazione, ma che non utilizzano un approccio fattuale. Questo è importante, in quanto un mancato distanziamento da queste narrative non basate sui fatti potrebbe portare ad una sfiducia da parte del pubblico anche verso la propria narrativa, nel caso che qualcuno portasse all'evidenza le eventuali incongruenze presenti tra queste.

Il secondo metodo, che è applicabile solamente a campagne di disinformazione organizzate, ha un'efficacia teorica ampiamente superiore al primo, perché permette di contrastare qualsiasi tipo di tattica prima

che raggiunga la massa critica di interesse nel pubblico. Questo metodo consiste nel mappare e monitorare le infrastrutture che gli agenti della disinformazione utilizzano, in modo che sia possibile osservare la messa in moto delle varie tattiche quando sono ancora in fase molto precoce. In questo modo si ha il tempo di preparare e diffondere tra il pubblico una narrativa fattuale che vada a smentire i punti principali della narrativa degli agenti della disinformazione, prima ancora che questa sia nota al pubblico. Il lato negativo del dover monitorare le infrastrutture, è quello che costringe a limitare l'utilizzo del *deplatforming*; questo, se usato senza cautela, porterebbe a una distruzione solo temporanea dell'infrastruttura che verrebbe ricostruita in altre forme e su altre piattaforme, e ciò renderebbe il monitoraggio più arduo, se non impossibile.

Per quanto riguarda l'*infrastructuring* stesso, ovvero la creazione di infrastrutture, l'unico metodo applicabile per contrastarlo è il *deplatforming*, ma come detto precedentemente sarebbe solamente una soluzione temporanea che potrebbe anche rischiare di rendere meno efficaci gli sforzi per contrastare le altre tattiche.

II. AntiVax

assistenti alla ricerca,
Adriano Dossi e Michelangelo Gennaro

II.1. Metodologia

Nel caso di studio sulla disinformazione sanitaria abbiamo utilizzato un metodo osservativo-descrittivo, che riproduce l'esperienza dell'utente *online* che si avvicini alle *community* AntiVax italiane. Questo approccio è stato poi integrato con il riferimento a una variegata bibliografia specialistica. La raccolta dati si è protratta per circa 6 mesi, da metà gennaio a inizio giugno 2021.

Muovendo i primi passi nella ricerca, abbiamo individuato alcuni tra i principali *disinfluencer*[1] coinvolti nelle campagne antivaccinali. Attraverso la comparazione dei loro *account*, pagine e canali sulle differenti piattaforme, abbiamo identificato Facebook come *social media* di riferimento per

1 Il vocabolario Treccani definisce influencer un "personaggio popolare in Rete, che ha la capacità di influenzare i comportamenti e le scelte di un determinato gruppo di utenti e, in particolare, di potenziali consumatori, e viene utilizzato nell'ambito delle strategie di comunicazione e di marketing". Gianroberto Casaleggio, «Influencer,» Treccani (Neologismi 2017), https://www.treccani.it/vocabolario/influencer_res-728101ee-89c5-11e8-a7cb-00271042e8d9_%28Neologismi%29/#:~:text=influencer%20s.%20m.%20e%20f.,di%20comunicazione%20e%20di%20marketing.Con disinfluencer, termine di nostra elaborazione, si intende un influencer che ha acquisito notorietà, accresce la propria fama ed esercita la propria influenza attraverso la diffusione di informazioni o notizie decontestualizzate o non verificate o alle volte fuorvianti o false.

i gruppi che abbiamo seguito i quali registrano il maggior numero di *follower*, interazioni ed engagement proprio sulla piattaforma di Zuckerberg, seppur con alcune eccezioni.

Successivamente, la creazione di un profilo Facebook – adibito alla sola funzione di seguire le pagine e accedere ai gruppi NoVax – ci ha permesso di entrare in contatto con l'ecosistema antivaccinale, che passo passo si è andato a ricostruire di fronte ai nostri occhi. Questo passaggio si è rivelato fondamentale, soprattutto perché agevolato dall'algoritmo di Facebook: poiché avevamo aggiunto alla lista degli amici alcuni "militanti" dell'ecosistema[2], la piattaforma ha iniziato a suggerire, nella sezione "Persone che potresti conoscere", una serie di profili coinvolti nella diffusione di notizie false, tendenziose o fuorvianti sui vaccini. Dunque, l'algoritmo si è rivelato una preziosa guida all'interno dell'articolata struttura dell'ecosistema, favorendo il nostro processo di raccolta manuale di dati.

Oltre al lavoro manuale, abbiamo impiegato anche dei *tool open access*: il monitoraggio sulle interazioni (reazioni e condivisioni) ricevute dai *disinfluencer* su Facebook è avvenuto tramite Facepager; per monitorare l'*engagement* di alcuni siti *web*, ci siamo avvalsi invece di *SimilarWeb*.

Infine, l'interpretazione dei dati raccolti nella fase osservativa-descrittiva ha seguito il paradigma dell'etnografia digitale investigativa. Ci siamo avvalsi delle categorie interpretative fornite da due testi di riferimento: il primo, *Investigative digital ethnography*[3], ci ha fornito un modello per la rappresentazione testuale dell'ecosistema di disinformazione sanitaria; dal secondo, *The Media Manipulation CaseBook*[4], abbiamo attinto gli strumenti esegetici necessari a individuare le tattiche di manipolazione dei *social media* principalmente utilizzate da queste comunità.

II.2. Evoluzione temporale

Durante il periodo preso in considerazione dalla ricerca, si è osservata una variazione nelle narrative adottate dai *disinfluencer* AntiVax. Rispetto al 2020, l'impianto narrativo si è allontanato da narrative legate alla negazione dell'esistenza del Coronavirus, così come del numero delle vittime e dei contagiati -com'era avvenuto in fasi precedenti della campagna disinformativa- per focalizzarsi sulla campagna vaccinale anti COVID-19. Dalle nostre osservazioni è emerso che i principali disinfluencer di queste campagne non sono, come a volte erroneamente riportato, persone con livelli di educazione bassi o classe sociali meno abbienti, bensì appartenenti a categorie professionali quali avvocati, medici, liberi professionisti, giornalisti e politici. Secondo queste osservazioni, è

2 Questi hanno accettato spontaneamente le nostre "Richieste di amicizia".

3 https://mediamanipulation.org/sites/default/files/2020-10/Investigative_Ethnography_v1.pdf.

4 https://mediamanipulation.org/sites/default/files/media-files/Code-Book-1.2-April-21-2021.pdf.

evidente come queste campagne di disinformazione siano costruire da "professionisti della disinformazione" i quali spesso derivano guadagni monetari dalle loro attività on e offline, per esempio vendendo prodotti, tessere associative o richiedendo offerte e donazioni. Le campagne di disinformazione vanno dunque analizzate da un punto di vista di pratiche professionali piuttosto che di fenomeni organicamente emergenti sulle piattaforme.

Nel nostro studio, proponiamo una ripartizione delle odierne tesi antivaccinali basata sulle categorie professionali di appartenenza dei *disinfluencer*. Tra questi si annoverano medici, scienziati, avvocati e giornalisti. Dalle nostre osservazioni, abbiamo rilevato come i diversi gruppi professionali siano caratterizzati da diverse narrative, legate strettamente alla propria professione, e che gli permettono di utilizzare la propria affiliazione professionale come strumento che ne "certifica" l'autorità. Ad esempio, mentre i disinfluencer di professione medica sottolineano la pericolosità dei vaccini, definiti "farmaci genici sperimentali", gli avvocati insistono sull'incostituzionalità dell'obbligo vaccinale per gli operatori sanitari. Attraverso narrative variegate ma sostanzialmente coerenti, i differenti "professionisti della disinformazione" assumono ruoli precisi all'interno dell'ecosistema, prodigandosi nel dare credibilità alle istanze NoVax e contemporaneamente affermandosi come autorità epistemiche all'interno di questi gruppi.

Nei sei mesi di raccolta dati, gli *account*, le pagine, i gruppi e i canali gestiti, sulle differenti piattaforme *online*, dai manipolatori dell'informazione sanitaria hanno registrato rilevanti incrementi di interazioni, *follower* ed *engagement*. Se nell'anno precedente la pandemia aveva favorito questa crescita, l'inizio della campagna vaccinale italiana (27 dicembre 2020) ha decretato un'ulteriore accelerazione del processo di espansione dell'ecosistema Antivax, il cui pubblico si è esteso notevolmente.

I *disinfluencer* si sono dimostrati abili nel dirottare il proprio traffico sui siti *web* personali, che sfuggono alle restrizioni contro la disinformazione adottate dai *social media*, identificandosi come raccoglitori sicuri per quei contenuti che propagandano le tesi antivaccinali. Inoltre, i siti personali sono stati impiegati – e continuano ad esserlo – per trarre un tornaconto economico dalla disinformazione: queste piattaforme ospitano infatti shop per la vendita di prodotti, campagne di *crowdfunding* e tesseramenti a pagamento. Le piattaforme di *social media* vengono dunque utilizzate come un'arena nella quale sviluppare *network* di utenti interessati, allo scopo di dirottarli su siti esterni di proprietà dei *disinfluencer*.

Tra la fine di marzo e l'inizio maggio si sono registrate operazioni di *deplatforming* da parte di Facebook, Youtube e Twitter, che hanno colpito anche alcuni manipolatori da noi monitorati. Osservando le reazioni dell'ecosistema, abbiamo compreso le tattiche messe in atto per volgere a

favore della disinformazione i provvedimenti tesi a contrastarla. Torneremo a breve su questo punto fondamentale.

II.3. Tattiche

Concentriamoci adesso sulle tattiche adottate dai manipolatori dell'informazione medico-sanitaria. Nel corso della nostra ricerca, abbiamo analizzato principalmente tre tattiche, identificate come le più rilevanti, ma non le uniche impiegate nella diffusione di disinformazione sui vaccini. Inoltre, le tattiche tendono a sovrapporsi, senza presentare confini netti. Le prime due sono riprese dal *CaseBook*[5], mentre l'ultima è nostra di elaborazione.

***Cloaked Science* (copertura pseudoscientifica)**: l'adozione di un lessico specialistico per nascondere, dietro una ricerca scientifica fittizia, un'agenda politica, ideologica o finanziaria. Il manipolatore può affiancare all'uso del gergo scientifico la presentazione di dati e grafici di difficile interpretazione, utili a presentare le proprie tesi come evidenze empiriche. Nel caso della disinformazione sanitaria, la tattica si rivela di particolare efficacia se impiegata da un medico o scienziato.

Recontextualized Media (ricontestualizzazione dei *media*): quando un'immagine, video, audio, articolo o qualsiasi altro *media* viene privato del suo contesto originale e reinserito in un contesto narrativo differente. Il *media* non subisce alterazioni dalla sua configurazione originale, ma viene solo ricontestualizzato. Durante la pandemia, l'*information overload* generato dai mainstream *media* riguardo a tematiche sanitarie ha garantito un rifornimento continuo di contenuti, che i *disinfluencer* hanno saputo collocare all'interno delle proprie retoriche antivaccinali.

Reazione di Vittimizzazione: reazione adottata dall'ecosistema AntiVax in risposta alle operazioni di *deplatforming* dei *social media*. Quando un *disinfluencer* subisce ban o sospensione temporanea del proprio account, la rete di disinformazione si coordina per presentarlo come martire della libertà di espressione, vittima di censura da parte della piattaforma. La tattica permette di focalizzare l'attenzione sul personaggio in questione, dirottando l'audience sui suoi altri canali di comunicazione ancora attivi; nel caso in cui l'account sospeso venga riattivato, potrebbe registrare un aumento repentino di *engagement*, *follower* e interazioni.

5 https://mediamanipulation.org/sites/default/files/media-files/Code-Book-1.2-April-21-2021.pdf

SEZIONE GIURIDICA

I. Disinformazione e politiche pubbliche: indicazioni di *policy* per istituzioni pubbliche e private,

di Antonio Gullo e Giovanni Piccirilli

Il tema della strumentalizzazione delle piattaforme *online* per l'attuazione di campagne di disinformazione è oggi divenuto centrale nel dibattito pubblico, di cui tali *network* sociali rappresentano ormai una essenziale articolazione.

Lo sviluppo della rete, infatti, ha determinato una peculiare condizione in cui ciascun individuo diventa, contemporaneamente, *recettore* e *produttore* di informazioni e in cui è possibile instaurare un dialogo diretto con l'opinione pubblica, senza il tradizionale filtro dei *media* e degli organi di informazione.

Una situazione, quest'ultima, che ha indubbi effetti positivi in termini di rafforzamento degli strumenti di partecipazione democratica dei cittadini alla vita politica del Paese, essendo ormai il digitale uno strumento irrinunciabile per la collettività nel suo complesso, ma che, al contempo, sta mostrando i suoi risvolti patologici rispetto alla possibilità di "inquinare" il pubblico confronto attraverso la diffusione, frutto di azioni isolate o coordinate, di informazioni false o fuorvianti in grado di incidere, ad esempio, sulla salute e sicurezza pubbliche, sull'integrità di processi elettorali e su altri interessi di rilievo.

Lo scopo delle indicazioni di *policy* per operatori pubblici e privati della sezione giuridica del presente manuale pratico è quello di delineare alcune linee evolutive della materia rispetto al fenomeno della *disinformation*, nell'ambito di tre versanti che costituiscono le principali linee di sviluppo della ricerca: la dimensione politico-istituzionale, la dimensione preventiva e la dimensione punitiva. In relazione a questi tre ambiti differenziali, le indicazioni di *policy* sono raggruppate per natura dei destinatari, articolandole opportunamente – e specificamente – sulla base della loro finalizzazione in relazione a: piattaforme *online*; operatori privati e imprese; istituzioni pubbliche.

Il primo versante, riguardante alcune *best* practice adottabili dalle piattaforme *online*, è stato strutturato in linea con le indicazioni del *Digital Services* Act attualmente in discussione presso le istituzioni dell'UE. Il suggerimento è quello di adottare un articolato sistema di controllo interno rispetto al rischio di strumentalizzazione dei propri servizi per finalità illecite o contrarie alle condizioni d'uso, attraverso, tra l'altro, la nomina di figure *ad hoc* con funzioni ispettive e di controllo e la messa a regime di dettagliate attività di *risk assessment* e *management*, di meccanismi di monitoraggio, *audit* e *reporting* alle autorità, di adeguate verifiche sugli operatori di *business* etc.

Particolare importanza, inoltre, è assunta in tale ambito dall'adesione a codici di condotta e autoregolamentazione, nonché lo svolgimento di periodici *algorithm auditing* sui parametri utilizzati dai sistemi di raccomandazione dei contenuti presenti sul sistema.

Il secondo ambito di indicazioni di *policy* è quello confezionato in relazione a operatori private e imprese. Nei loro confronti, oltre alle richiamate misure "auto-normate" di controllo, monitoraggio e contenimento dei rischi, l'esigenza è quella di un'attenta definizione delle modalità di gestione e accesso ai profili *business* dell'ente registrati su piattaforme *online*, prevedendo idonee misure di controllo che riguardino, tra l'altro, anche gli *user generated* content e le attività di eventuali fornitori.

Specie per i professionisti dell'informazione, poi, il nuovo mondo digitale impone di svolgere con rafforzata accuratezza le tradizionali procedure di controllo sulla veridicità delle fonti e sul rispetto dei principi deontologici dell'attività giornalistica, inglobando nelle predette attività di verifica anche le modalità di gestione e controllo di eventuali profili *social* della testata.

Sotto diverso ma interconnesso versante – accanto all'invito a contemplare puntuali misure di *compliance* preventiva da adottare in tali settori per una adeguata valutazione e gestione del rischio di strumentalizzazione della rete per azioni (coordinate e non) di disinformazione – si evidenzia l'esigenza di una regolamentazione pubblicistica della materia che serva a fornire alle piattaforme alcune indicazioni essenziali con riferimento alla definizione delle condizioni d'uso del servizio e delle relative misure di moderazione dei contenuti, nonché avuto riguardo all'armonizzazione delle *policy* di tali operatori rispetto a talune pericolose modalità d'uso dei loro servizi. Tale cornice normativa, in particolare, dovrebbe assicurare il rispetto – nell'ambito di tali attività private di auto-normazione ed enforcement – dei diritti fondamentali sanciti dalle Carte europee dei diritti, anche con riferimento alla costruzione di un nucleo minimo di garanzie sostanziali e procedurali per i destinatari del servizio. Nelle indicazioni di *policy* si prevede altresì, in sede di revisione delle decisioni delle piattaforme sulla moderazione dei contenuti, l'intervento di autorità pubbliche indipendenti in modo da evitare i rischi connessi all'affidare integralmente un simile compito ai privati.

Il quadro in cui dovrebbero muoversi tali politiche pubbliche è quello di una più ampia e rafforzata *partnership* pubblico-privato finalizzata al contrasto della disinformazione.

Su quest'ultimo versante, in particolare, sarebbe auspicabile il rafforzamento e la promozione di diversi strumenti quali la costituzione di *partnership* pubblico-privato strategiche (PPP) finalizzate alla individuazione e alla raccolta delle *best practices* del settore, nonché di tavoli e gruppi lavoro su questi temi; l'istituzione di punti di contatto per la gestione dei rapporti con il settore privato; la raccolta e l'analisi dei dati relativi alle attività di *private enforcement* delle piattaforme per la moderazione dei contenuti, in modo da comprendere e monitorare, senza soluzione di continuità, tendenze ed eventuali problematiche da risolvere; la previsione, su base annuale, della pubblicazione di un documento di analisi nazionale dei rischi legati alla disinformazione, che abbia altresì il compito di riassumere le priorità del Paese nella lotta alla disinformazione.

Misure, quelle delineate, che dovrebbero operare in sinergia tra loro, nell'ottica di un approccio olistico e integrato ai temi in discussione.

Tali soluzioni, nel loro complesso, consentiranno di addivenire a una condivisibile co-regolamentazione del fenomeno tra pubblico e privato, che sappia adeguatamente bilanciare tutti gli interessi in gioco, senza far sì che il rimedio sia peggiore del male da curare.

II. INDICAZIONI DI *POLICY*

Indicazioni di *policy* per piattaforme *online*

n°	Descrizione
IP-01	**Nomina di responsabili** – Nominare uno o più responsabili per la gestione dei rischi legati alla disinformazione, attribuendo a tale funzione poteri di controllo e/o ispettivi sui contenuti pubblicati in open access sulla piattaforma, nonché poteri di impulso per le azioni di *risk-assessment* e *risk-management*. Il nominativo e il contatto dei responsabili dovranno essere resi pubblici e facilmente accessibili.
IP-02	**Procedure di valutazione dei rischi** – Predisporre idonee procedure di valutazione dei rischi legati alla diffusione di informazioni false, analizzando su base almeno annuale gli ambiti tematici (es. categorie, *hashtag*, profili) più esposti e prevedendo in relazione ad essi adeguate misure di contenimento del rischio in base alle risorse disponibili e al livello di rischio misurato. Le procedure dovranno considerare in particolare i rischi legati alla diffusione di notizie false atte a turbare l'ordine pubblico, la sicurezza pubblica, il dibattito democratico su temi di preminente interesse pubblico, tenuto conto degli esiti della analisi nazionale dei rischi pubblicata ai sensi della IP-24 (se disponibile).
IP-03	**Monitoraggio** – Predisporre idonee procedure per verificare l'effettiva attuazione delle misure di contenimento dei rischi legati alla disinformazione e per assicurare il miglioramento continuo. Le piattaforme dovrebbero coordinare le policies di contrasto alla disinformazione con i sistemi di gestione interni e con le procedure di controllo della qualità dei servizi resi e della sicurezza delle informazioni.
IP-04	**Audit interni** – Prevedere su base almeno annuale lo svolgimento di audit interni, a cura dei responsabili indicati nella IP-01, volti a valutare la conformità delle procedure interne con le fonti di *soft law* (codici etici e di condotta, linee guida, indicazioni di *policies* etc.) e con le norme cogenti di legge.

IP-05	**Informativa agli utenti** – Includere nelle condizioni generali del servizio idonee previsioni contrattuali volte a vietare la diffusione di notizie false ove ciò costituisca reato o condotta illecita sulla base delle regole del diritto applicabile.
IP-06	**Sistemi di segnalazione delle informazioni illecite o lesive delle condizioni d'uso del servizio. Rimozione di contenuti e denunce all'Autorità** – Predisporre strumenti e interfacce per consentire agli utenti di segnalare la presenza nel loro servizio di informazioni illecite o lesive delle condizioni d'uso del servizio. Predisporre procedure interne di esame della segnalazione entro 24 ore, che assicurino l'immediata rimozione dei contenuti in questione, prevedendo specifici obblighi di motivazione della decisione sul contenuto. Prevedere che venga altresì data notizia all'autore del contenuto dell'avvenuta presentazione di una segnalazione, ovvero dell'adozione di un provvedimento di rimozione. Predisporre procedure interne per la denuncia all'Autorità di fatti o circostanze che facciano sospettare l'avvenuta commissione o la possibile commissione di un reato attraverso l'uso dei propri servizi.

IP-07	**Definizione delle condizioni d'uso del servizio, delle sanzioni disciplinari e dei reclami** – Definire le regole d'utilizzo del servizio nel rispetto dei fondamentali principi di garanzia sanciti dalle Carte europee dei diritti (su tutti, il diritto alla libertà di espressione dell'utente). Disciplinare le violazioni e le collegate misure di carattere sanzionatorio/interdittivo – dalla etichettatura o rimozione del contenuto, al blocco temporaneo al servizio, fino alla sospensione temporanea o permanente dell'*account* – nel rispetto delle correlate garanzie *sostanziali* e *procedurali*, tra cui, ad es.: il principio di legalità delle violazioni e delle misure sanzionatorie/interdittive, con i relativi corollari della irretroattività, della tassatività/precisione delle previsioni punitive, e del divieto di analogia, con una chiara definizione dei soggetti titolari della potestà di dettare tali regole; il principio di proporzionalità del trattamento sanzionatorio rispetto alla concreta gravità della violazione; il divieto di responsabilità oggettiva e l'affermazione del principio di colpevolezza, con la necessità di specificare l'elemento soggettivo (dolo o colpa) necessario per integrare la violazione; il diritto al contraddittorio e la garanzia di terzietà e indipendenza del soggetti deputati a irrogare la sanzione e a decidere sui connessi reclami; il diritto di richiedere il riesame della decisione etc. Assicurare un elevato livello di trasparenza e dettaglio nel rendere pubbliche le modalità di funzionamento e le specifiche fasi delle procedure interne di applicazione delle misure sanzionatorie/inibitorie e per la gestione dei correlati reclami da parte degli utenti.
IP- 08	**Pubblicità *online*** – Istituire un registro di informazioni chiare, corrette e trasparenti in merito all'identità o a caratteristiche di terzi che sponsorizzano propri prodotti o servizi sulla piattaforma. Imporre ai professionisti (es. agenzie di *marketing*, intermediari etc.) che si avvalgono dei servizi di pubblicità intra-piattaforma di indicare il nominativo del cliente e/o il titolare effettivo dell'annuncio che sarà mostrato sulla piattaforma. Prevedere procedure di controllo, anche a campione, sulle pubblicità mostrare dalla piattaforma in ambiti ritenuti a rischio ai sensi della IP-02.

IP-09	**Verifiche sugli operatori *business* –** Prevedere procedure di controllo, anche a campione, sui contenuti diffusi da operatori *business* (es. profili *social* di grandi imprese, istituzioni, ONG, profili di persone politicamente esposte) attivi in ambiti ritenuti a rischio ai sensi della IP-02. Assicurare che le segnalazioni relative a tali operatori siano trattate in via prioritaria rispetto alle altre segnalazioni. Sottoporre a tali operatori una informativa sulle procedure, le misure e gli strumenti applicabili alle condotte di disinformazione sulla piattaforma, in modo da ottenere una presa d'atto per accettazione.
IP-10	**Codici di condotta** – Adottare strumenti di regolazione flessibile e *best practices* per il contenimento dei rischi legati alla disinformazione, aderendo se del caso a codici di condotta già esistenti elaborati da enti o istituzioni qualificate. Prevedere, in tali strumenti, procedure e controlli particolari in contesti e periodi temporali definiti particolarmente esposti al rischio di disinformazione (es, periodi precedenti alle elezioni politiche, contesti emergenziali).
IP-11	**Algoritmi di raccomandazione** – Svolgere controlli periodici ed effettuare *algorithm auditing* sui parametri utilizzati dai sistemi di raccomandazione dei contenuti presenti sulla piattaforma, con particolare riguardo agli ambiti tematici a rischio di disinformazione ai sensi della IP-02. Prevedere misure atte a prevenire che un contenuto afferente a tali ambiti possa essere "consigliato" dagli algoritmi di raccomandazione, diventando così "virale" nel *web*, senza che detti algoritmi siano stati sottoposti a controllo o validazione, anche in osservanza degli standard internazionali applicabili.
IP-12	**Report periodici** – Pubblicare report periodici sulle attività di segnalazione, moderazione e rimozione di contenuti operati dalla piattaforma ai sensi della IP-06. Tali report dovrebbero essere formulati in modo chiaro ed essere resi facilmente accessibili.

Indicazioni di *policy* per operatori privati e imprese

n°	Descrizione
IP-13	**Valutazione dei rischi** – Effettuare con cadenza almeno annuale la valutazione dei rischi legati alla diffusione di informazioni false sui canali *social* e sulle piattaforme utilizzate dall'impresa. Analizzare in particolare gli ambiti di attività (es. linee di *business*, tipologie di prodotti etc.) particolarmente esposti al rischio di disinformazione e prevedere in relazione ad essi adeguate misure di contenimento del rischio in base alle risorse disponibili e al livello di rischio misurato. Le procedure dovranno considerare in particolare i rischi legati alla diffusione di notizie false atte a turbare l'ordine pubblico, la sicurezza pubblica, il dibattito democratico su temi di preminente interesse pubblico, tenuto conto degli esiti della analisi nazionale dei rischi pubblicata ai sensi della IP-24 (se disponibile).
IP-14	**Gestione dei profili *business*** – Predisporre adeguate procedure organizzative e di controllo per l'utilizzo delle utenze e dei profili registrati su piattaforme *online*, prevedendo in particolare che i privilegi di amministratore della pagina e le credenziali di accesso siano attribuiti a soggetti all'uopo designati, sottoposti alla vigilanza di organi e funzioni di controllo.
IP-15	**Controllo sui contenuti** – Predisporre adeguate procedure di controllo da parte di responsabili aziendale prima della pubblicazione di notizie (es. post, messaggi, articoli) su piattaforme *online*, in ambiti particolarmente esposti a rischio ai sensi della IP-13. Prevedere la necessità di una autorizzazione preventiva per la pubblicazione di contenuti ritenuti particolarmente sensibili in base agli esiti della valutazione dei rischi.

IP- 16	**Meccanismi di segnalazione degli *user-generated* contents** – Prevedere procedure di controllo sui contenuti diffusi da utenti privati e collegati alla pagina *social* dell'impresa (o dell'organizzazione) mediante il sistema dei tag. Segnalare senza indebito ritardo al gestore della piattaforma notizie non veritiere relative ad ambiti ritenuti a rischio ai sensi della IP-13, al fine di consentirne la tempestiva rimozione. Tale segnalazione dovrebbe essere effettuata anche nel caso in cui il contenuto diffuso dagli utenti non sia direttamente collegato alla pagina social dell'impresa (o dell'organizzazione), ma quest'ultima ne abbia comunque avuto conoscenza.
IP-17	**Doveri di diligenza per i professionisti dell'informazione** – Predisporre adeguate procedure di controllo sulla veridicità delle fonti e sul rispetto dei criteri di verità, pertinenza e continenza nell'attività giornalistica e di informazione su aree tematiche ritenute a rischio ai sensi della IP-13. Laddove il professionista dell'informazione (es. agenzie di stampa, operatori radio e televisivi, testate telematiche registrate, quotidiani *online*) disponga di una pagina su una piattaforma *online* coordinare tali procedure di controllo con quelle previste dalla IP-15. Predisporre adeguate procedure di controllo sul rispetto delle disposizioni contenute in codici etici e di condotta al quale il professionista dell'informazione abbia aderito.
IP-18	**Codici di condotta** – Adottare strumenti di regolazione flessibile e best practices per il contenimento dei rischi legati alla disinformazione, aderendo se del caso a codici di condotta già esistenti elaborati da enti o istituzioni qualificate. Tale misura dovrebbe essere seguita in particolare dalle organizzazioni che operano come professionisti dell'informazione.
IP-19	**Controlli sull'attività dei fornitori** – Prevedere procedure di controllo, anche a campione, sulle attività affidate in *outsourcing* a terzi fornitori (es. gestione del profilo social da parte di agenzie di stampa o di *marketing*) in ambiti ritenuti a rischio ai sensi della IP-13 o ad essi connessi o correlati.

Indicazioni di *policy* per istituzioni pubbliche

n°	Descrizione
IP-20	**Elaborazione di codici di condotta e strumenti di regolazione flessibile. Definizione di una cornice legislativa pubblicistica per le attività di moderazione dei contenuti da parte delle piattaforme di rilevanti dimensioni** – Incentivare l'elaborazione di codici di condotta, linee guida e istruzioni operative per la gestione dei rischi legati alla disinformazione e sul contrasto alle operazioni coordinate di disinformazione. Monitorare costantemente l'adozione dei codici di condotta da parte degli operatori del settore (v. IP-10 e IP-18), provvedendo se del caso all'aggiornamento e al miglioramento continuo di tali codici in relazione ai risultati dell'analisi nazionale dei rischi e alle indicazioni delle istituzioni dell'Unione Europea. Incentivare iniziative specifiche di studio e di ricerca finalizzate alla elaborazione di strumenti di regolazione flessibile. Definizione di una cornice legislativa per la responsabilizzazione delle piattaforme, che, oltre al versante degli obblighi di trasparenza/*disclosure* e di *risk assessment* e *management*, si muova nella direzione di delineare un preciso set di regole per la definizione delle regole d'uso del servizio e per la correlata implementazione, da parte degli operatori, delle attività di *private enforcement* in merito alla moderazione dei contenuti illeciti e lesivi di tali *policy* in conformità ai diritti delineati dalle principali Carte europee, tra cui, su tutti, il diritto alla libertà di espressione e, nel rispetto, circa la definizione delle violazioni delle condizioni d'uso e delle relative misure di moderazione dei contenuti, dei correlati principi di garanzia *sostanziali* e *procedurali*, tra cui come *minimo*, ad es.: il principio di legalità delle violazioni e delle misure sanzionatorie/interdittive, con i relativi corollari della irretroattività, della tassatività/precisione delle previsioni punitive, e del divieto di analogia, con una chiara definizione dei soggetti titolari della potestà di dettare tali regole; il principio di proporzionalità del trattamento sanzionatorio rispetto alla concreta gravità della violazione; il divieto di responsabilità oggettiva e l'affermazione del principio di colpevolezza, con la necessità di specificare l'elemento soggettivo (dolo o colpa) necessario per integrare la violazione; il diritto al contraddittorio e la garanzia di terzietà e indipendenza del soggetti deputati a irrogare la sanzione e a decidere sui connessi reclami; il

	Prevedere, in capo alle piattaforme, l'obbligo di assicurare un elevato livello di trasparenza e dettaglio nel rendere pubbliche le modalità di funzionamento e le specifiche fasi delle procedure interne di applicazione delle misure sanzionatorie/inibitorie e per la gestione dei correlati reclami da parte degli utenti. Istituire un'autorità pubblica indipendente con il compito di vigilare sul rispetto di tali normative – adottando le relative sanzioni di natura pecuniaria e interdittiva e vigilando sulle correlate procedure di *cooperative compliance* da introdurre per la definizione del procedimento punitivo nei confronti delle piattaforme –, con la possibilità, altresì, di intervenire quantomeno in sede di riesame della decisione sulla moderazione dei contenuti contestata dall'utente, adottando una decisione il cui contenuto sia vincolante per l'operatore privato.
IP-21	**Costituzione di gruppi di lavoro e *partnership* con gli operatori privati** – Avviare consultazioni pubbliche e costituire tavoli di lavoro per la discussione sui temi della disinformazione. Istituire *partnership* pubblico-privato strategiche (PPP) finalizzate alla individuazione e alla raccolta delle best practices del settore. Diffondere la cultura della "buona informazione" nel rispetto del pluralismo democratico e della libertà di espressione, sensibilizzando i cittadini e gli operatori economici sui rischi legati alla manipolazione dell'informazione.
IP-22	**Istituire punti di contatto** – Nominare uno più responsabili per la gestione dei rapporti con il settore privato in relazione alle iniziative di cui alla IP-20 e IP-21. Assicurare che i nominativi e in contatti dei responsabili siano facilmente accessibili sul sito internet istituzionale dell'ente pubblico.
IP-23	**Raccolta di statistiche e elaborazione di dati aggregati** – Predisporre adeguate procedure per la raccolta e l'analisi dei dati relativi alle azioni di moderazione, segnalazione e rimozione di contenuti pubblicati dalle piattaforme conformemente alla IP-12. Elaborare dati e statistiche aggregate per settori di attività o per aree tematiche in relazione ai risultati delle analisi.

IP-24	**Analisi nazionale dei rischi legati alla disinformazione** – Intraprendere iniziative, anche attraverso il coordinamento con altre pubbliche amministrazioni, per elaborare, su base almeno annuale, un documento riassuntivo delle priorità nazionali nella lotta alla disinformazione mediante diffusione di notizie false su piattaforme *online*. Tale documento dovrebbe prevedere, in particolare, le aree maggiormente esposte ai rischi di disinformazione sulla base dei risultati delle analisi condotte ai sensi della IP-23. Il documento contenente l'analisi nazionale dei rischi dovrebbe essere pubblicato e reso facilmente accessibile per tutti gli operatori privati.

Glossario

- **Contenuto sintetico:** Contenuto prodotto, manipolato o modificato utilizzando mezzi automatizzati, particolarmente di intelligenza artificiale. Fanno parte di questa categoria i cosiddetti *deep fakes*.
- ***Coordinated Inauthentic Behavior:*** Comportamento coordinato allo scopo di ingannare utenti di *social media* circa la provenienza di informazioni, tramite l'apertura di *account* falsi, l'operazione di *bots*, l'uso di *sockpuppets*, impersonificazione di altri utenti o persone fisiche e altri metodi di inganno.
- **Disinformazione:** Informazione falsa creata con l'obiettivo causare un danno.
- ***Disinfluencer:*** Con *disinfluencer*, termine di nostra elaborazione, si intende un influencer che ha acquisito notorietà, accresce la propria fama ed esercita la propria influenza attraverso la diffusione di informazioni o notizie decontestualizzate o non verificate o alle volte fuorvianti o false.
- **Disordine dell'informazione:** Qualsiasi disordine dell'informazione nel contesto degli ambienti di comunicazione digitali, come misinformazione, disinformazione, e malinformazione.
- **Ecosistema dell'informazione:** Ecosistema dell'informazione composto dall'informazione diffusa sui *media* tradizionali e l'ecosistema in cui individui e comunità interagiscono *online*.

- **Guerra ibrida:** Strategia militare, caratterizzata da grande flessibilità, che unisce la guerra convenzionale, la guerra irregolare e la guerra fatta di azioni di attacco e sabotaggio cibernetico.
- **Malinformazione:** Informazione che, pur essendo vera, è diffusa con l'obiettivo di causare un danno.
- **Misinformazione:** Informazione falsa diffusa inconsapevolmente
- **Operazioni di informazione:** L'uso integrato di guerra elettronica, *computer network operations*, operazioni psicologiche, inganno militare e operazioni di sicurezza che, assieme a relative capacità strategiche, vengono utilizzate allo scopo di influenzare, distruggere, corrompere od usurpare il potere decisionale tanto di avversari umani che artificiali.

Tattiche di manipolazione dell'informazione

Strategie

Il piano d'azione o la serie di azioni elaborate per raggiungere un obiettivo complessivo, come osservato dalle evidenze disponibili.

- ***Astroturfing*** - *l'astroturfing* si verifica quando gli operatori delle campagne di disinformazione cercano di creare una falsa percezione di ampio supporto supporto radicato su una questione, campagna, o posizione, celando le proprie identità, assumendo identità fittizie e usando altre pratiche ingannevoli, come nascondere le origini dell'informazione diffusa o gonfiare artificialmente le statistiche di engagement, per esempio tramite l'uso di *sockpuppets* o *bots*.
- ***Butterfly attack*** - I *butterfly attacks* si verificano quando impostori imitano i comportamenti tipici di un gruppo sociale (solitamente un gruppo che deve lottare per essere rappresentato). Gli impostori fingono di far parte del gruppo per infiltrare retoriche divisive e disinformazione nelle conversazioni popolari *online* o nei *network* di informazione usati da questi gruppi. Distinto dall*'astroturfing,* che cerca di falsificare il supporto radicato di una questione, i *butterfly attacks* sono pensati per infiltrare communità esistenti, campagne mediatiche o *hashtags* per ostacolare le loro operazioni e screditare il gruppo attraverso la diffusione di informazioni divisive, provocatorie o fuorvianti. Coniato da Patrick Ryan per descrivere una serie di campagne di manipolazione che afferma di aver orchestrato nel 2013, il termine è ispirato dall'atteggiamento imitativo di alcune specie di farfalle, che impersonano l'andamento del volo di altre specie per confondere i predatori.
- ***Gaming an algorithm*** - Cercare di manipolare l'algoritmo per guadagnare attenzioni. Ciò può includere tattiche che spingono un contenuto nella *trending list* di una piattaforma, venendo consigliato agli altri utenti, o posizionandolo nella *top ten* dei risultati di un motore di ricerca.
- ***Meme war*** - La propagazione intenzionale di *memes* politici sui social *media* con l'obiettivo di creare persuasione politica, costruire

comunità *online*, o per diffondere strategicamente narrative o messaggi fondamentali per una campagna di *media* manipulation.

- ***Muddy the waters* -** La distribuzione di informazioni con lo scopo di creare confusione su eventi controversi, che precede od occulta informazioni verificate e opinioni diffuse. Nel fare ciò, il soggetto preso di mira diventa più confuso quando fonti credibili o autorevoli sono costrette a competere con speculazioni, affermazioni infondate o informazioni del tutto false.
- ***Targeted harassment* -** Molestia *online* coordinata e organizzata nei confronti di un individuo o gruppo di individui per minacciarli, censurarli o innervosirli o per interrompere le loro operazioni o comportamenti.
- ***Trading up the chain*** - Ottenere visibilità collocando informazioni o artefatti di disinformazione in luoghi dove è probabile che essi vengano ripresi e amplificati da altri sistemi, individui o pubblicazioni. In genere, le informazioni possono essere introdotte su *blog* più piccoli o sui *social media* prima di essere riportate dai principali *media* o politici e altri individui influenti.

Tattiche

Azioni eseguite in supporto delle strategie, come osservato dalle evidenze disponibili.

- ***Bots*** - *Social media accounts* automatizzati e impiegati nelle campagne di disinformazione per amplificare messaggi, condizionare algoritmi di trending o raccomandazione, aumentare le interazioni su un *account*.
- ***Cheap Fake*** - Alterazione di immagini o video con tecniche convenzionali di editing, come *speeding, slowing, cutting*, per creare una percezione falsificata di individui e avvenimenti.
- ***Cloaked science*** - L'adozione del gergo scientifico per nascondere un'agenda politica, ideologica o finanziaria dietro le sembianze di una ricerca scientifica. Ciò può includere, oltre all'uso di un lessico specialistico, la presentazione di grafici, diagrammi e dati apparentemente scientifici, atti a presentare determinate tesi come evidenze empiriche e aumentare la credibilità delle informazioni propagandate. Le istanze pseudoscientifiche vengono diffuse tramite server pubblici, banche dati, giornali e pubblicazioni con scarsi standard di revisione, oppure da giornalisti incapaci di verificarne la veridicità. Questa definizione è costruita sulla ricerca di Jessie Daniel sui *clocked websites*, da lei descritti come "siti pubblicati da individui o gruppi che nascondono gli autori per mascherare un'agenda politica," e ispirata alla descrizione di Sarah Richardson delle politiche transfobiche che vengono "nascoste nella scienza". Lo studioso Timothy Caulfield, nel descrivere un fenomeno simile — l'uso del linguaggio scientifico per mascherare motivazioni non scientifiche — usa il termine "*scienceploitation*". Si noti che la tattica *cloaked science* consiste nell'uso deliberato di informazioni mascherate da scienza e non andrebbe confuso con "junk science", termine usato per screditare scoperte, affermazioni e dati scientifici

come fraudolenti o fuorvianti, così come "*fake news*" può essere utilizzato per screditare notizie riportate sui *media*.

- **Copypasta** - Neologismo nato dall'unione delle parole "copy," "paste," e "pasta,"si riferisce a ogni tipologia di testo che viene ripostato ripetutamente sui *social media*, nelle *app* di messaggistica, nelle sezioni commenti e nei forum di discussione.
- ***Distributed amplification*** - Appello rivolto ai partecipanti di un determinato gruppo o *community online*, che vengono esortati a diffondere il più velocemente possibile il materiale di una campagna propagandistica o di disinformazione.
- ***Evidence collage*** - Documenti creati inserendo numerose informazioni (soprattutto *screenshots* e brevi testi), spesso sia false che verificate, in un singolo file condivisibile (solitamente un'immagine).
- ***Forgery*** - Creazione di documenti falsi che vengono poi diffusi dai manipolatori, così da simulare una fuga di notizie riservate o incriminanti un personaggio pubblico.
- ***Hijacked accounts*** - L'uso non autorizzato di un *account* individuale (*email* personale, *social media account, app* di messaggistica e ogni altro *account* associato a *digital services*) al quale si è avuto accesso tramite hacking o furto delle credenziali.
- ***Impersonation*** - Fingersi un'altra persona imitandone il comportamento o creando un *account fake*.
- ***Keyword squatting*** - Il controllo strategico di una parola chiave unica o poco utilizzata su un *social media* o motore di ricerca, che permette di influenzare i contenuti e le ricerche degli utenti in favore degli obiettivi degli operatori di una campagna di disinformazione.
- ***Leak*** - La divulgazione non autorizzata di materiale sensibile o documenti.
- ***Memes*** - Termine coniato da Richard Dawkins (1976) per indicare delle unità di cultura che si propagano tramite la diffusione di idee. I Meme sono particolarmente importanti *online*, perché internet li cristallizza in artefatti di comunicazione e ne accelera la diffusione all'interno delle subculture. Nelle campagne di disinformazione si identificano con immagini, gifs o video.
- ***Misinfographic*** - Infografiche che riportano dati falsi o fuorvianti. Sono spesso classificabili anche come *forgery,* in particolare quando prendono in prestito il logo e l'estetica di qualche organizzazione esistente, in modo tale da attribuire a tale organizzazione la diffusione di quei contenuti.
- ***Phishing*** - Cercare di ottenere informazioni confidenziali come *usernames, passwords* e dettagli della carta di credito fingendosi un individuo o un'organizzazione affidabile (solitamente tramite mail).
- ***Recontextualized media*** - *Media* (image, video, audio) che è stato preso dal contesto originale e inserito in un nuovo contesto che ne riformula il senso per uno scopo od una narrativa completamente diversi.
- ***Swarming*** - Quando un gruppo di utenti *online* inizialmente poco organizzato si riunisce e collabora per raggiungere determinati obiettivi

- ***Trolling*** - Assunzione di un atteggiamento offensivo, provocatorio e divisivo da parte di un utente di una *community online*, al fine di provocare una forte reazione emotiva, spesso negativa, negli altri utenti.
- ***Typosquatting*** - Registrazione intenzionale di un nome di dominio che si configura con una variazione tipografica di un altro preesistente, in modo tale da attirare un numero maggiore di visitatori. La variazione nel nome consiste solitamente in un errore di *spelling* o in un differente *top domain*.
- ***Viral sloganeering*** - Tecnica che si avvale della formulazione di brevi slogan per veicolare e diffondere messaggi reazionari, nel tentativo di influenzare gli spettatori, forzare la copertura mediatica su tematiche divisive, e provocare risposte istituzionali.

Biografie

Antonio Gullo

Il Professor Antonio Gullo è ordinario di diritto penale e Prorettore alla didattica presso l'Università Luiss Guido Carli. È stato Ricercatore di Diritto penale presso la Facoltà di Giurisprudenza dell'Università degli Studi di Brescia e Professore associato di Diritto penale presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Messina. È stato professore a contratto di Diritto penale presso l'Università Commerciale Luigi Bocconi di Milano.

È Coordinatore del Dottorato in Diritto e Impresa attivo presso il Dipartimento di Giurisprudenza dell'Università Luiss e Coordinatore dei Master universitari di secondo livello in Diritto penale d'impresa, in *Cybersecurity*: politiche pubbliche, normativa e gestione e in Compliance e prevenzione della corruzione nei settori pubblico e privato dell'Università Luiss.

È membro del Comitato di direzione della rivista Diritto penale contemporaneo e membro del Comitato scientifico della rivista Diritto penale contemporaneo – Rivista Trimestrale. È membro del comitato di direzione della rivista *Diritto commerciale e delle obbligazioni*. È componente del gruppo di revisori della rivista *La Legislazione penale* e della *Rivista trimestrale di diritto penale dell'economia*.

Irene Pasquetto

Irene V. Pasquetto è una studiosa nel campo degli studi dell'informazione e della comunicazione. Ha lanciato come Chief Editor la Harvard Kennedy School Misinformation Review presso lo Shorenstein Center della Harvard Kennedy School. Ora è Assistant Professor alla School of Information dell'Università del Michigan. Prima di entrare alla Kennedy School, è stata assistente di ricerca presso l'UCLA Center for Knowledge Infrastructures (CKI) e ricercatrice presso l'UCLA Institute for Society and Genetics. La Dott.ssa Pasquetto ha conseguito un dottorato di ricerca in Information Studies presso l'UCLA, un Master in *Media Studies and Journalism* ed una laurea in Scienze della Comunicazione presso l'Università degli Studi di Verona.

Gianni Riotta

Visiting Professor alla Princeton University presso il Dipartimento di francese e italiano, specializzato in digital humanities, machine writing, storia sociale e storia visiva dell'Italia. Dal 2018 dirige il Master in Giornalismo e Comunicazione multimediale e il Centro di Ricerca Data Lab dell'Università Luiss di Roma dove coordina l'Italian Digital Media Observatory finanziato nell'ambito del bando europeo CEF-TC-2020-2 EDMO, volto a costituire un hub internazionale per supportare e implementare il lavoro dell'European Digital Media Observatory (EDMO). I partner del progetto, TELECOM, RAI, GEDI, l'Università di Torvergata, Newsguard, Pagella Politica, T6 Ecosystem, uniranno le forze ed expertise per combattere la disinformazione. Ha partecipato nell'abito degli Horizon 2020 al Progetto SOMA contro la disinformazione costituendo il Centro di Eccellenza Aletheia e MediaFutures "*Data-driven innovation hub for the media value chain*" e un progetto contro la diffusione della disinformazione in collaborazione con l'Università di Harvard e il Ministero degli Affari Esteri italiano. Fa parte dell'Advisory Board NewsGuard e dell'Edmo (European Digital Media Observatory). Riotta è giornalista di fama internazionale. Editorialista per La Stampa, Repubblica e Huffington Post già direttore del TG1 e del Sole 24 Ore. Contribuisce al BBC World Service. I suoi editoriali sono stati pubblicati dal New York Times, The Washington Post, Le Monde, The Wall Street Journal, Financial Times, The Guardian, El Pais, Suddeutsche Zeitung, Foreign Affairs.

Costanza Sciubba Caniglia

Costanza Sciubba Caniglia è una giornalista e ricercatrice specializzata ad Harvard sui temi della mis- e disinformazione. È affiliata allo Shorenstein Center for Media, Politics and Public Policy della Harvard Kennedy School, dove ha co-fondato la rivista accademica HKS Misinformation Review. È Direttrice e Fondatrice dell'Istituto di Geopolitica Digitale, un think tank attivo sui temi della governance dell'era digitale. Al momento sta lavorando alla strategia anti-disinformazione di Wikipedia, per la Wikimedia Foundation. Ha lavorato per molti anni presso le Nazioni Unite a New York in *policy* e comunicazione, incluso come vice portavoce della Rappresentanza Permanente d'Italia presso l'ONU durante il mandato in Consiglio di Sicurezza. Scrive e fa consulenza sui temi della mis- e disinformazione e i suoi lavori sono stati presentati in diverse Università, tra cui Harvard, Columbia, Luiss, Michigan University e sui *media*, tra cui la CNN, The Washington Post, La Stampa, and RSI News. La Dott.ssa Sciubba Caniglia ha conseguito una Laurea in Public Administration (MPA) presso l'Università di Harvard, una Laurea Magistrale in Studi teorico-critici ed una Laurea in Filosofia presso l'Università La Sapienza di Roma, ed un Master di specializzazione in relazioni internazionali e protezione internazionale dei diritti umani presso la SIOI.