

UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE POLITICHE, GIURIDICHE E  
STUDI INTERNAZIONALI

Corso di laurea *Triennale* in Scienze Politiche



***Fake news* and disinformation: self-regulation and  
regulation in the European Union, Germany and Italy**

***Fake news* e disinformazione: autoregolamentazione e  
regolazione nell'Unione Europea, in Germania e in Italia**

*Relatore:* Prof. PAOLO ROBERTO GRAZIANO

*Laureando:* DANIELE PASUTO  
matricola N. 1200762

A.A. 2021/22



# Indice

<b>Introduzione</b> .....	3
<b>Capitolo 1: Il fenomeno delle <i>fake news</i> online</b> .....	5
1.1 Definizione del fenomeno .....	6
1.2 La diffusione nei social media .....	11
1.2.1 Il ruolo degli algoritmi .....	14
1.2.2 Meccanismi psicologici e tecniche sfruttate .....	16
1.2.3 Effetti nell'opinione pubblica .....	19
1.3 Soluzioni normative? .....	22
<b>Capitolo 2: L'autoregolamentazione della disinformazione e le iniziative europee</b> .....	24
2.1 L'autoregolamentazione .....	24
2.1.1 Facebook .....	25
2.1.2 Twitter .....	27
2.1.3 Google .....	28
2.2 L'approccio europeo .....	29
2.2.1 La consultazione pubblica e l'indagine Eurobarometro .....	30
2.2.2 Il "Codice di buone pratiche sulla disinformazione" e il "Piano d'azione contro la disinformazione" .....	34
2.2.3 Criticità delle azioni dell'UE .....	37
<b>Capitolo 3: L'intervento della Germania</b> .....	42
3.1 La NetzDG .....	43

3.1.1 Critiche e implicazioni .....	47
3.1.2 Primi risultati pratici .....	51
3.1.3 Un bilancio .....	54
<b>Capitolo 4: I tentativi di contrasto dell'Italia .....</b>	<b>56</b>
4.1 I disegni di legge Gambaro e Zanda-Filippin .....	57
4.2 Il ruolo dell'AGCOM .....	63
4.3 Altre iniziative .....	67
<b>Conclusioni .....</b>	<b>70</b>
<b>Bibliografia .....</b>	<b>75</b>
<b>Sitografia .....</b>	<b>77</b>
<b>Elenco delle figure .....</b>	<b>81</b>
<b>Ringraziamenti .....</b>	<b>82</b>

## Introduzione

Nella seguente tesi tratterò un fenomeno che negli ultimi anni ha avuto una notevole rilevanza nel dibattito pubblico, e anche una certa pervasività nella nostra quotidianità, le *fake news*.

In realtà, la diffusione di queste notizie è sempre esistita nella storia. È solo nel XXI secolo che l'incontro di quest'espressione è diventato più frequente, specie su Google e negli altri motori di ricerca, designando quelle "informazioni false, spesso sensazionalistiche, diffuse sotto forma di notizie giornalistiche" (Collins, n.d.). L'utilizzo di questo termine acquisisce visibilità con le elezioni presidenziali americane del 2016 e con la campagna referendaria per la Brexit, entrando nell'uso popolare (Candido, 2020; Magnani, 2019).

In questo elaborato non si andrà ad analizzare l'evoluzione storica del fenomeno, ma ci si concentrerà sulla sua diffusione esponenziale nei social media.

Nel primo capitolo si è scelto di vedere come vengono definite e come si diffondono. Qui sarà utile qualche spunto di psicologia riguardo ai meccanismi che si nascondono dietro la loro diffusione. Ci si concentrerà anche sugli effetti che queste provocano in un'opinione pubblica sempre più digitale, in cui l'avvento di Internet e la nascita dei social network hanno inevitabilmente cambiato il modo di comunicare, socializzare, interagire e informarsi, ma anche disinformarsi.

In seguito, il discorso centrale dell'elaborato verterà sul contrasto di questo fenomeno da parte di vari soggetti, istituzionali e non.

Nella prima parte del secondo capitolo, si andrà a capire quali iniziative hanno messo in atto Facebook, Twitter e Google di fronte a questo problema, principali piattaforme in cui trovano terreno fertile notizie false, che vengono condivise e ricondivise a loro volta molto facilmente e velocemente.

Poi, nella seconda parte del secondo capitolo, si prenderà in considerazione l'Unione Europea, attore fondamentale che negli ultimi anni ha condotto

studi e prodotto report, piani e un Codice di buone pratiche per combattere la disinformazione.

Successivamente, nel terzo capitolo, si passerà alla Germania, primo Stato europeo che ha optato per la linea dura, attraverso una legge ad hoc. Dopo averla descritta, ci sarà spazio per qualche risultato pratico, ma anche per le critiche che ha ricevuto.

Infine, nel quarto capitolo, lo sguardo andrà verso un altro Stato, l'Italia, con i disegni di legge (ddl) che sono stati presentati: Gambaro, prima, e Zanda-Filippin, poi. Nondimeno, anche altre autorità italiane si sono mosse, la Polizia Postale e l'AGCOM. Questa pare aver avuto un ruolo impattante nell'analisi della disinformazione rispetto alla fine che hanno fatto i due ddl. È necessario chiarire che si è cercato di circoscrivere l'argomento, data la sua ampiezza e i suoi continui cambiamenti, fornendo degli esempi concreti d'intervento, al fine di comprenderne i punti di forza e le difficoltà attuative degli stessi, in un mondo sempre più globalizzato e interconnesso, costantemente collegato in rete, dove bisogna tenere conto anche della libertà di espressione e di altri diritti.

Passando in rassegna interventi sia di autoregolamentazione sia di regolazione, con la presente tesi si vuole anche cercare di informare chi fosse interessato a un argomento che inerisce all'ecosistema mediatico, e far conoscere maggiormente una tematica che tocca, spesso inconsapevolmente, un po' tutti.

## Capitolo 1: Il fenomeno delle *fake news* online

Nell'affrontare un tema come quello delle *fake news*, è necessario, prima di tutto, definire il fenomeno e chiarire alcuni concetti connessi utilizzati frequentemente, spesso in modo confuso, quali “disinformazione” e “misinformazione”, per poi analizzare il contesto in cui al giorno d’oggi si sviluppano queste notizie e le ragioni che si nascondono dietro il loro uso. In seguito, verranno presi in considerazione gli effetti che hanno sul pubblico, fruitore, ma anche sempre più produttore di queste notizie (Candido, 2020).

Esse non sono di certo nuove. La storia offre numerosi eventi ricordati proprio per il fatto di essere avvolti da notizie false o distorte. Per fornire qualche esempio, si pensi alla famosa “Great Moon Hoax” di quasi due secoli fa. Il New York Times nel 1835 aveva pubblicato una serie di articoli satirici, poi smentiti, che annunciavano la scoperta della vita sulla Luna (Pitruzzella, 2018), e che avevano provocato un aumento delle vendite del giornale.

Ma si può andare anche molto più indietro con i secoli. Nel IV secolo a.C. lo spartano Pausania tradì i greci per passare al servizio dei persiani di Serse. Ciò sarebbe testimoniato da una lettera inviata da lui stesso al re, non ritenuta però autentica dalla storiografia<sup>1</sup>.

Un altro esempio noto è il documento del 314 d.C., “La Donazione di Costantino”, con cui l'imperatore avrebbe assegnato alla Chiesa il primato del vescovo di Roma sulle chiese patriarcali orientali, la sovranità del pontefice su tutti gli altri sacerdoti, la superiorità del potere papale su quello temporale e la giurisdizione civile sulla città di Roma, sull'Italia e sull'Impero romano d'Occidente<sup>2</sup>. Solo nel 1517 l'umanista Lorenzo Valla rivelò la falsità del testo grazie a degli studi linguistici (Gili e Maddalena, 2018).

---

<sup>1</sup> Petrucci, Armando. 2009. “La storia falsa”. *Studi storici* (1): 281-286. Fondazione Istituto Gramsci.

<sup>2</sup> Ricci, Pier Giorgio. n.d. “Donazione di Costantino”. Enciclopedia Dantesca in Treccani. Ultimo accesso 29 ottobre 2021. [https://www.treccani.it/enciclopedia/donazione-di-costantino\\_%28Enciclopedia-Dantesca%29/](https://www.treccani.it/enciclopedia/donazione-di-costantino_%28Enciclopedia-Dantesca%29/).

Tuttavia, l'obiettivo non sarà quello di guardare come si sono evolute nel tempo, ma concentrare il focus su quelle diffuse nella rete Internet, in particolare nei social media. Questo perché sono cambiati i mezzi di trasmissione delle informazioni. Una volta principalmente erano la radio e i quotidiani cartacei, oggi è la rete. Secondo l'indagine condotta da Demos&Pi per conto di Italiani.coop, per quanto riguarda i canali informativi in Italia, emerge il progressivo declino del giornale cartaceo e l'uso crescente dei social per tenersi informati, anche se la televisione rimane la prima scelta da parte dei cittadini (Ceccarini e Di Pierdomenico, 2018).

### **1.1 Definizione del fenomeno**

È già stato accennato al fatto che le *fake news* siano sempre esistite e che solo con le elezioni presidenziali americane del 2016, che hanno decretato la vittoria di Donald Trump contro Hillary Clinton, e il referendum sulla Brexit, hanno iniziato ad avere un eco mediatico più rilevante, tanto che anche di recente un'ex manager di Facebook, Frances Haugen, ha parlato davanti al Senato americano, tra i tanti argomenti, degli effetti di Instagram sugli adolescenti e della diffusione della disinformazione e dell'odio. Riguardo a questo secondo punto, per lei Facebook ha tolto gli algoritmi che diminuiscono questi contenuti dopo le elezioni che hanno visto la vittoria di Biden, in questo modo non impegnandosi seriamente e tradendo la democrazia<sup>3</sup>.

Già nel 2013 il World Economic Forum aveva sottolineato come il problema di una società iperconnessa, come quella attuale, fosse la disinformazione proveniente dai media digitali<sup>4</sup>.

---

<sup>3</sup> Scott, Pelley. 2021. "Whistleblower: Facebook is misleading the public on progress against hate speech, violence, misinformation". *CBS News*. Ultimo accesso 4 gennaio 2022. <https://www.cbsnews.com/news/facebook-whistleblower-frances-haugen-misinformation-public-60-minutes-2021-10-03/>.

<sup>4</sup> World Economic Forum. 2013. "Digital Wildfires in a Hyperconnected World". Ultimo accesso 29 ottobre 2021. <https://reports.weforum.org/global-risks-2013/risk-case-1/digital-wildfires-in-a-hyperconnected-world/>.

Bisogna fare una premessa. Fornire una definizione chiara delle *fake news* non è semplice, nemmeno è universalmente riconosciuta, ma è opportuno almeno provarci, ricorrendo a classificazioni di esperti in materia.

Intanto lo si può capire dalle definizioni di due dizionari. Il Collins Dictionary definisce come *fake news* tutte quelle “informazioni false, spesso sensazionalistiche, diffuse sotto forma di notizie giornalistiche” (Collins, n.d.), mentre in Italia la Treccani mette in relazione la loro divulgazione “attraverso il Web, i media o le tecnologie digitali di comunicazione” (Treccani, n.d.), evidenziando in questo modo il ruolo della rete nella loro diffusione. Una definizione più generale è, invece, quella dell’Agenzia per l’Italia Digitale, agenzia pubblica fondata nel 2012 per promuovere l’innovazione digitale della Pubblica Amministrazione, secondo la quale è “la diffusione deliberata di disinformazione attraverso i media tradizionali o i social network” (AgID, 2020).

Pitruzzella distingue le *fake news* dalle opinioni. È una distinzione che s’inserisce nell’ampio tema della libertà di espressione, tanto cara ai sistemi democratici occidentali, i quali si fondano sul confronto e sulla competizione di idee e opinioni diverse, e tutelata dalle costituzioni statali. Secondo l’autore, riprendendo la definizione data dagli economisti Hunt Allcott e Matthew Gentzkow, ossia che le *fake news* sono “quegli articoli recanti notizie che sono intenzionalmente e verificabilmente false e potrebbero trarre in inganno i lettori”<sup>5</sup>, sono da escludere da questo gruppo:

- gli errori non intenzionali;
- i *rumor*, cioè pretese dell’esistenza di fatti dei quali non si hanno prove dell’esistenza e che acquistano credibilità perché altre persone credono nella loro veridicità;
- le teorie cospiratorie;
- la satira;
- le false affermazioni dei politici;

---

<sup>5</sup> Allcott Hunt, Gentzkow Matthew. 2017. “Social Media and Fake News in the 2016 Election”. *Journal of Economic Perspectives*, 31 (2): 211-236.

- i report non falsi che possono ingannare.

La limitazione è necessaria, altrimenti si può finire “per pregiudicare la libertà di manifestazione del pensiero” (Pitruzzella, 2018, pp. 32-33).

Inoltre, spesso alle *fake news* vengono accostati altri termini, quali *post-truth* e *hate speech*. In realtà, la post-verità, riconosciuta parola dell'anno 2016 dall'Oxford English Dictionary (Gili e Maddalena, 2018), indica una forma di comunicazione in cui la partecipazione emotiva al fatto di cui si parla è più influente del fatto oggettivo in sé. Il prefisso “*post-*” non significa “dopo”, ma è inteso come “oltre”. La verità passa in secondo piano, è meno importante, così come il suo controllo. Può essere che una *fake news* sia quindi una *post-truth* quando fa più leva sulle emozioni che sulla razionalità. La diffusione di notizie tramite la rete ha sicuramente permesso la propagazione di entrambe.

Il discorso d'odio, invece, è un'altra tipologia di comunicazione. Secondo la definizione data dal Consiglio d'Europa nel 1997, è inteso come “l'insieme di tutte le forme di espressione che si diffondono, incitano, sviluppano o giustificano l'odio razziale, la xenofobia, l'antisemitismo ed altre forme di odio basate sull'intolleranza e che comprendono l'intolleranza espressa attraverso un aggressivo nazionalismo ed etnocentrismo, la discriminazione e l'ostilità contro le minoranze, i migranti ed i popoli che traggono origine dai flussi migratori”<sup>6</sup>. Nel 2010 il Consiglio ha incluso anche l'omofobia e la transfobia (Belluati et al., 2021). Il contenuto di una *fake news* può anche coincidere con quello di un discorso d'odio o può essere che “le campagne d'odio si nutrano anche della diffusione di notizie prive di fondamento”. Si può allora coglierne la differenza nel fatto che l'*hate speech* “presenta una maggiore capacità di tradursi in un effetto incitativo o di istigazione alla commissione di atti di violenza” (Bassini e Vigevani, 2017, pp. 17-18). È un fenomeno che è nell'agenda delle istituzioni europee, italiane, delle corti internazionali e dell'ONU. È ritenuta “una minaccia subdola e persistente,

---

<sup>6</sup> Comitato dei ministri del Consiglio d'Europa. 1997. “Raccomandazione n. 20”. Ultimo accesso 19 gennaio 2022. <https://rm.coe.int/1680505d5b>.

in grado di minare la tenuta delle democrazie contemporanee” (Belluati et al., 2021, p. 53).

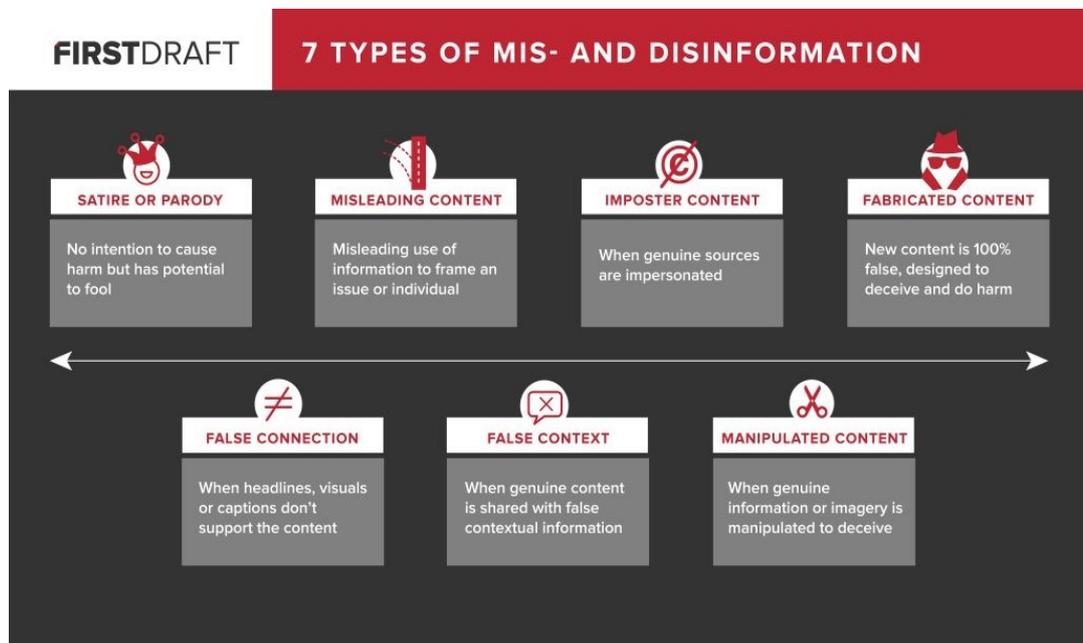
Infine, è opportuno distinguere anche tra due concetti, disinformazione e disinformazione. Entrambi si riferiscono a informazioni non corrette, l'intenzione gioca però un ruolo fondamentale. Per la ricercatrice e direttrice Claire Wardle, che lavora per First Draft News, progetto nato nel 2015 e condotto da Google insieme a Facebook, Twitter e alcune organizzazioni filantropiche per combattere la disinformazione, nella prima rientra una notizia falsa condivisa involontariamente, per errore (Wardle, 2017). Anche per Belluati et al. non c'è l'intenzione di nuocere al destinatario e in questa classe rientrano le false promesse o scoperte, i titoli provocatori che non hanno a che vedere con l'articolo o il video, le burle (Belluati et al., 2021).

Si ricade nella seconda, invece, quando una persona volontariamente scrive o diffonde una notizia o un'informazione in modo distorto e intenzionale, decontestualizzandola o manipolandola volutamente, al punto da renderla verosimile, per influenzare singoli individui, gruppi sociali o istituzioni (Wardle, 2017).

A proposito, la studiosa distingue a grandi linee la disinformazione in sette tipi, in cui rientrano anche le notizie false, come mostra la figura 1.1 sottostante.

- Satira o parodia (*satire or parody*). Non c'è l'intenzione di procurare un danno, ma il contenuto mira a ingannare soprattutto chi è disattento o poco informato.
- Contenuto fuorviante (*misleading content*). L'uso che si fa dell'informazione per inquadrare un problema o un individuo è ingannevole, ad esempio dando una falsa immagine di un avversario politico.
- Contenuto ingannatore (*imposter content*). Il contenuto autentico viene indicato come proveniente da una fonte attendibile, che in realtà non centra con quel fatto.

- Contenuto falso (*fabricated content*). Il contenuto è completamente falso, progettato appositamente e consapevolmente per ingannare e creare un danno al lettore.
- Collegamento ingannevole (*false connection*). L'utilizzo di titoli, immagini o didascalie differiscono dal contenuto scritto nell'articolo.
- Contesto ingannevole (*false context*). Il contenuto vero viene inserito in un contesto falso o modificato.
- Contenuto manipolato (*manipulated content*). Un testo scritto, una fonte, un'immagine o un video di una notizia vengono manipolati e resi il più possibile veritieri, allo scopo di ingannare.



**FIGURA 1.1** Wardle, Claire. 2017. "7 Types of Mis- And Disinformation".

Sempre lei enumera otto cause che portano alla creazione di questi contenuti: il cattivo giornalismo, la parodia, la propaganda, il profitto, l'influenza politica, l'appartenenza a un gruppo ideologico, un interesse particolare o l'intento di provocare qualcuno o qualcosa.

## 1.2 La diffusione nei social media

La rete ha cambiato radicalmente il mondo dell'informazione, oggi sempre più globalizzato. Per rendersi conto di come esso è stato stravolto, Pitruzzella parla di un sistema di produzione dell'informazione fortemente decentralizzato. La possibilità di accesso da più fonti e da quasi tutti i luoghi contemporaneamente è certamente un aspetto innovativo. Basta un computer o un qualsiasi altro dispositivo ed essere connessi a Internet per produrre un'informazione o informarsi (Pitruzzella, 2018).

Lo stesso Internet è cambiato molto nel corso del tempo. Non sono solo più le istituzioni, gli uffici di stampa e le testate online i produttori di notizie (Suffia e Ziccardi, 2020), ma chiunque può commentare un post su Twitter o partecipare alla vita politica in una chat, esprimendo le proprie opinioni e comunicando in un blog o pubblicando un video su Youtube.

Suffia e Ziccardi hanno sottolineato tre problematiche che permettono di comprendere meglio la complessità del contesto informativo nel quale si inscrive il fenomeno oggetto di studio.

In primo luogo l'*overloading* informativo, cioè l'enorme quantità di informazioni, che non siamo in grado di analizzare senza l'ausilio di un computer.

In secondo luogo la perdita di autorevolezza da parte di chi crea notizie, dato che tutti ne hanno la possibilità.

In terzo luogo la difficoltà di controllare la veridicità delle notizie (Suffia e Ziccardi, 2020).

Un ruolo significativo è stato via via assunto da Google, Facebook, Twitter, YouTube, Instagram, dove passano la maggior parte delle informazioni delle quali siamo i destinatari, ma anche dove si creano. Infatti, il prezzo basso per usare un dispositivo elettronico e accedere alla rete fa sì che la popolazione mondiale materialmente ne possa beneficiare a proprio piacimento (Pitruzzella, 2018) e che i costi di creazione di informazioni siano quasi nulli.

Essi sono noti come “social network”, ossia tutti quei servizi informatici, siti web, tecnologie online che permettono agli utenti di condividere contenuti testuali, immagini, video e audio.

È sufficiente registrarsi e creare un proprio profilo con i dati personali per entrare in contatto con altri utenti o per partecipare a discussioni in gruppi privati.

Un'altra trasformazione che è stata identificata concerne il come la massa di informazioni viene ordinata e resa fruibile dai motori di ricerca e dai social media per mezzo degli algoritmi, di cui si dirà meglio più avanti. Essi sono i *gatekeepers* (“portieri”) dell'informazione, intermediari tra i produttori e i fruitori di notizie (Pitruzzella, 2018).

Se però vi è stata un'apertura nella produzione di informazioni, d'altra parte è stata registrata la tendenza a concentrare i “servizi che rendono effettivamente disponibile e utilizzabile questa informazione nelle mani di poche compagnie multinazionali”, soprattutto le cinque menzionate poco sopra (Pitruzzella, 2018, p. 23).

La digitalizzazione di Internet permette di leggere più comodamente le notizie sul proprio smartphone o tablet. Alcuni studi (Ceccarini e Di Pierdomenico, 2018; Pitruzzella, 2018) hanno indagato come si consumano le notizie, attestando un calo dell'utilizzo dei media tradizionali, come i quotidiani cartacei. Può essere utile notare come in Italia le vendite “nel periodo 2007-2016 sono passate da 5,8 milioni a 3 milioni di copie giornaliere”, interessando, solo per citare alcuni dei maggiori giornali, il Corriere della Sera, La Repubblica e IlSole24Ore (Pitruzzella, 2018).

È interessante però osservare che, se da un lato cala la stampa, in controtendenza regge la televisione. Nell'indagine condotta da Ceccarini e Di Pierdomenico, l'84% del campione di italiani dichiara di informarsi tutti i giorni attraverso la televisione, il 9% qualche volta alla settimana, il 2% qualche volta al mese e il 5% mai o meno di una volta al mese. Seguono Internet, i social network, la radio, i quotidiani cartacei e i settimanali (Ceccarini e Di Pierdomenico, 2018).

Tuttavia, in questo contesto essere correttamente informati è un interrogativo che si pongono i cittadini in veste di consumatori di contenuti, che leggono e si imbattono sempre più in notizie false, che vengono percepite come rischio “per il proprio paese” e “per il funzionamento stesso del sistema democratico”. Essi dichiarano di incontrare *fake news* “almeno una volta alla settimana” o un “contenuto disinformativo e fuorviante quasi tutti i giorni”. Delle persone che usano i social, “il 75% dichiara di imbattersi regolarmente in una *fake news*” (Fubini, 2019, p. 245).

Questi dati permettono di capire la portata del fenomeno, in cui “il 71% ritiene di essere in grado di distinguere un contenuto informativo falso da una notizia” (Fubini, 2019, p. 245).

Ma quali possono essere le intenzioni dietro questa diffusione?

I motivi possono essere molteplici. Possono servire per pubblicizzare un determinato prodotto di un’azienda o per screditare un concorrente; per aumentare gli utenti di un social al fine di alzare il valore commerciale dello stesso o per incentivare gli stessi a condividere *fake news*, in modo che l’accesso continuo a queste generi profitto. L’obiettivo dei produttori di tali notizie è quello di realizzare profitti con la pubblicità che rimanda ai loro siti web, com’è stato il caso degli adolescenti di Veles, paesino macedone, i quali hanno guadagnato migliaia di dollari (Comandini, 2018), vendendo notizie false su Donald Trump e Hillary Clinton a siti americani, che poi le hanno a loro volta condivise anche su Facebook.

Sono presenti nel mondo della politica allo scopo “di modificare le opinioni politiche degli utenti, al fine di incrementare il consenso di chi si sostiene o di diminuire quello di chi si contrasta” (Pizzetti, 2017, p. 49), accusando un avversario di comportamenti falsi, ma anche nelle materie scientifiche per “orientare le convinzioni dei cittadini” circa l’affidabilità delle informazioni, ad esempio riguardo a un farmaco o all’ambiente, o per negare avvenimenti storici accertati (Pizzetti, 2017, p. 49), come il negazionismo della Shoah e le teorie terrapiattiste.

Secondo uno studio condotto dall’Istituto Studi Avanzati di Lucca e dall’Università La Sapienza di Roma, le *fake news* possono essere

raggruppate in tre macroaree: geopolitica (63%), clima (18%) e salute (circa il 19%). Le terze riguardano prevalentemente i vaccini, i tumori e l'alimentazione (Ascione, Lopalco e Pavesio, 2020). Come ben si sa e come l'Istituto di Ricerche Mario Negri indica, con il Covid-19 ne sono uscite tra le più disparate, dalla correlazione tra il coronavirus e la rete 5G, al fatto che gli extracomunitari siano immuni a questo virus grazie al vaccino contro la tubercolosi, o che bere bevande calde aiuti a sconfiggerlo. Hanno riscontrato molto seguito anche quelle relative ai farmaci o ai possibili rimedi naturali per curare l'infezione e quelle sulle misure personali per evitare che il virus entri in casa, come lavare i vestiti o assumere determinati cibi<sup>7</sup>. Tutte affermazioni che non trovano da nessuna parte evidenza scientifica e che alimentano la disinformazione, creando confusione e panico.

### **1.2.1 Il ruolo degli algoritmi**

Per comprendere nel concreto come vengono ordinate le informazioni, bisogna soffermarsi sugli algoritmi.

Per reperire le informazioni ci si avvale dei motori di ricerca, come Google, Yahoo, Bing, che selezionano "l'informazione che viene presentata al lettore sullo schermo e stabiliscono altresì l'ordine in cui l'informazione gli viene presentata, determinando in questo modo la sua visibilità" (Pitruzzella, 2018, p. 25), analizzando un insieme indefinito di dati.

Il nodo centrale è che l'ordine di presentazione dipende dagli algoritmi, cioè da procedure matematiche e calcoli per eseguire in un tempo, ormai brevissimo, delle operazioni complesse, come ricerche su temi specifici, che sono alla base dei motori di ricerca e dei social network.

Perciò una falsità, se messa in rilievo nella pagina, logicamente può raggiungere milioni di persone.

---

<sup>7</sup> Istituto di Ricerche Farmacologiche Mario Negri. 2021. "Covid-19: tutte le fake news nate durante la pandemia". Ultimo accesso 19 gennaio 2022.  
<https://www.marionegri.it/magazine/covid-19-e-fake-news>.

Inoltre, questi sono diventati talmente sofisticati da auto-apprendere, cioè “imparano dai dati” che raccolgono da ogni utente, arrivando perfino a stimare la probabilità di un evento”. Le notizie non si incontrano casualmente, ma dipendono anch’esse dal “modo in cui sono disegnati gli algoritmi che guidano la loro distribuzione” (Pitruzzella, 2018, p. 26). Per esempio l’algoritmo del News Feed, lo spazio della pagina principale di Facebook, ordina i contenuti che appaiono nella *homepage* di ciascun utente in base a quanto si interagisce con una determinata pagina o con un determinato contenuto, a quante interazioni quel post ha avuto e a quanto è recente. Vengono mostrati quelli di amici, parenti e conoscenti con i quali si interagisce maggiormente.

Google applica dei filtri che selezionano e ordinano i contenuti in base alla loro rilevanza, misurata attraverso alcuni parametri: “numero di link di ingresso, corrispondenza tra termini ricavati e termini inclusi nei documenti, prestazioni tecniche dei siti” e attribuiscono la rilevanza di un contenuto “in base alla serie storica delle ricerche effettuate da tutti gli utenti di Google” (Pitruzzella, 2018, p. 27).

Gli algoritmi quindi analizzano sempre di più i comportamenti degli utenti, perlopiù memorizzati da precedenti ricerche, allo scopo di capire le loro preferenze e cosa seguono, leggono, approfondiscono. Sempre il News Feed punta a mostrare ciò che piace, suggerendo contenuti personalizzati. Di conseguenza, può venire a crearsi una bolla informativa, una “*filter bubble*”, in cui “i post visualizzati da un utente sono sempre più in linea con gli interessi e le opinioni dello stesso”. Questo è un vantaggio perché riduce i tempi e i costi di una ricerca, ma d’altra parte comporta l’esposizione del soggetto solamente a ciò “che è in sintonia con i suoi pregiudizi” e con le proprie credenze, e la ricezione di “soltanto un’eco delle opinioni e dei gusti” (Pitruzzella, 2018, p. 29). In questo modo, l’individuo seguirà sempre quelle fonti e quei link che ricalcano il proprio background culturale. Per questo Pitruzzella, riprendendo una distinzione fatta dal giurista Cass Sunstein nel 2007<sup>8</sup>, paragona la situazione della *filter bubble*, appena descritta, a quella

---

<sup>8</sup> Sunstein, Cass R. 2007. “*Republic.com 2.0*”. Princeton University Press.

di un consumatore nel libero mercato, in cui si cercano di rendere più facili le sue scelte di consumo, distinguendolo però dal cittadino di uno stato libero che si fonda sul “dibattito pubblico in cui possano confrontarsi idee diverse, e in cui possano trovare accesso anche le idee più lontane dal *mainstream* culturale dominante” (Pitruzzella, 2018, p. 29).

### **1.2.2 Meccanismi psicologici e tecniche sfruttate**

Il noto docente di Psicologia della Comunicazione Giuseppe Riva ha indicato cinque meccanismi ad hoc che permettono alle *fake news* di funzionare:

- gli obiettivi, gli interessi e le personalità dei membri della comunità sono rispecchiati in esse;
- un numero sufficientemente elevato di membri della comunità le vede;
- i membri della comunità non si accorgono del fatto che le notizie che incontrano sono false;
- le altre notizie presenti nella comunità non sono in contrasto con i contenuti delle *fake news*;
- un numero molto basso di membri della comunità si impegna a informarsi al di fuori di esse (Suffia e Ziccardi, 2020).

Se ci si addentra ancora più in profondità, è stato evidenziato, attraverso approfonditi studi psicologici, che l'uomo ha la tendenza a valutare le informazioni che incontra in modo limitato perché operano due distorsioni cognitive (*bias*): il *bias* della conferma e quello della desiderabilità.

Secondo il primo, si è portati a cercare quelle informazioni che confermino ciò di cui si è già convinti e a ignorare quelle che sono in contrasto con le proprie credenze. È stato confermato che questo può compromettere la capacità razionale dell'individuo, che non riesce a comprendere qualcosa di vero solo perché contrario alle proprie visioni e inclinazioni. È quello che

porta, senza freni, a mettere like e a condividere solo quei contenuti che confermano i nostri ideali (Croce e Piazza, 2019).

Il secondo *bias*, invece, porta il soggetto a credere più a informazioni che desidera fortemente ricevere rispetto a quelle che non desidera affatto. Tutto il resto che non è desiderato lo ignora (Croce e Piazza, 2019).

Ne consegue che si possono formare quindi molte bolle, e non solamente una, chiamate “*echo chamber*” (camere dell’eco), ossia gruppi di utenti che interagiscono tra di loro e che condividono le stesse idee e notizie, esposti solo a informazioni in linea con le proprie convinzioni, perché ritenute più credibili e affidabili rispetto alle informazioni non confermate.

Nulla toglie che queste ultime possano essere false, innescando un circolo vizioso di credenze non vere. Infatti, in questo contesto, un gruppo può far circolare, rendendole virali, notizie infondate verso un altro solo perché ha una veduta diversa. Sempre secondo Croce e Piazza, “il mero fatto che i membri della comunità condividano le stesse credenze e valutino le informazioni nello stesso modo offre a ciascuno di loro ulteriore evidenza che i loro compagni sono degni di fiducia, incrementando così i livelli interni di credenza” (Croce e Piazza, 2019, p. 456). In un contesto del genere, perciò, ci si autoconvince delle proprie visioni, uniche ad avere un valore.

A tutto ciò bisogna aggiungere contemporaneamente un’altra tendenza, “il ridotto livello di attenzione che prestiamo ai contenuti dei social media”, conseguenza dell’“enorme mole di dati e informazioni che i social mettono a nostra disposizione” (Croce e Piazza, 2019, p. 452). A riguardo, gli stessi autori citano una ricerca di Microsoft Canada<sup>9</sup>, che ha evidenziato che non riusciamo a mantenere un livello di attenzione prolungata online di fronte a così tante informazioni e che questo potrebbe farci cadere nella trappola di non sapere individuare le notizie non attendibili (Croce e Piazza, 2019). Ciò è aggravato dal fatto che le informazioni di bassa qualità sembrano avere la stessa probabilità di diffondersi di quelle più qualitative (Suffia e Ziccardi, 2020).

---

<sup>9</sup> Microsoft Canada. 2015. “Microsoft Attention Spans Research Report”. Ultimo accesso 19 gennaio 2022. <https://it.scribd.com/document/265348695/Microsoft-Attention-Spans-Research-Report>.

In più oggi, come detto in precedenza, l'autorevolezza da cui proviene una notizia è difficilmente verificabile, dal momento che “tutti, teoricamente, sono in grado di creare notizie degne della pubblica attenzione” (Suffia e Ziccardi, 2020, p. 211).

Rimanendo sempre dentro il campo psicologico, è stato evidenziato che “la ripetizione è una delle tecniche più efficaci per portare le persone ad accettare contenuti manipolati”. Infatti, i post dei social network “appaiono quasi identici sulle piattaforme” e “sono progettati per focalizzarsi sulla storia piuttosto che sulla fonte”. Questo rende difficile “valutare la credibilità di qualsiasi messaggio” (Caranti e Mat, 2019).

Legato alla ripetizione, si innesta il fenomeno dei *bot*, profili presenti nelle piattaforme social note e su WhatsApp, creati da algoritmi. Essi hanno l'obiettivo di distorcere la realtà tramite “pubblicità occulta, creazione di notizie false sulla base degli argomenti maggiormente di attualità e diffusione di creative teorie complottiste”. Il *bot* è “come un account automatizzato, un aggregatore di notizie, o un software”, difficile da riconoscere (Carbone, 2020). Ma come opera?

Sempre secondo Carbone, segue molti account, utilizza come immagine del profilo quella di un personaggio famoso, prendendola dal web, e si nasconde dietro uno pseudonimo o un nome inventato. Le sue pubblicazioni sono ripetitive e continue, spesso con errori grammaticali, così come le sue interazioni con gli altri. Le notizie che diffonde sono “volutamente false, studiate in modo tale da manipolare l'opinione pubblica, creare dissenso, ingenerare sfiducia nel cittadino, suscitare determinate emozioni” (Carbone, 2020).

Sono interessanti alcune ricerche sui *bot*. Infatti, alcuni ricercatori dell'Indiana University hanno applicato su Twitter un sistema per riconoscere i *bot* (Botometer) a 915 account che avevano condiviso un link a uno stesso articolo. L'8% degli account è stato considerato come tale. Ne è risultato che, quella percentuale, anche se rappresentativa di pochi account, è stata considerata responsabile, in larga parte, della condivisione dell'articolo, nello specifico del 33% dei post con i link all'articolo in comune.

O ancora, due ricercatori, utilizzando un algoritmo, hanno fatto emergere che 3,8 milioni di tweet su 20,7 (19%) sono stati generati da 400.000 *bot*, su un totale di 2,8 milioni di account (15%) (Mazziotti Di Celso, 2018).

Un altro fenomeno da considerare è lo *sharing*, cioè la condivisione. Facebook permette di condividere notizie con i propri amici, commentare un post o lasciare un like, così come Twitter di *retweettare* un contenuto o di lasciare una citazione (*quote*). In essi poi un determinato contenuto ha la possibilità di diventare virale “attraverso condivisioni che si incrementano in modo esponenziale, a causa degli innumerevoli utenti che ogni singola condivisione raggiunge”, se non globale (Monti, 2017a, p. 84).

Ma non solo. Lo *sharing* riguarda anche altri soggetti, come le agenzie pubblicitarie che utilizzano i social al fine di attirare un pubblico più vasto, quale quello di Facebook, attraverso link presenti su una pagina Facebook molto seguita, in cui si viene rimandati direttamente a un articolo di un sito web esterno per mezzo di annunci pubblicitari (Pitruzzella, 2018). Ogni rimando al sito permette di guadagnare, poco importa se l’articolo sia falso. Ecco che i social network sono come una “cassa di risonanza” per molti siti web, che probabilmente non avrebbero una così grande visibilità senza la diffusione sui social (Monti, 2017a, p. 83).

### **1.2.3 Effetti nell’opinione pubblica**

Dopo aver visto a livello operativo la complessità di questo fenomeno, è lecito domandarsi quali effetti ne conseguano.

Uno lo abbiamo già visto, ossia la formazione di *echo chamber*. Il fatto che alcuni gruppi si chiudano nel proprio guscio e diffondano solamente notizie false conformi ai propri ideali, sfruttando i *bias* analizzati in precedenza, porta a una chiusura piuttosto netta del confronto pubblico. Si ricordi che le democrazie occidentali si basano sul *government by discussion*, che prevede che il confronto pubblico sia garantito, anche se in esso le idee possono confliggere, attraverso “fori pubblici aperti alle discussioni dove possono essere esposte le idee più disparate” (Pitruzzella, 2018, p. 29). È

quello che può accadere in un gruppo nazionalistico che condanna le politiche sull'asilo ai rifugiati attraverso post falsi sul loro sbarco sulle coste meridionali italiane (Croce e Piazza, 2019), non lasciando nemmeno spazio di cambiare la propria visione, pena l'uscita dal gruppo. Al proprio interno, infatti, le fonti di verifica vengono additate come agenzie corrotte, gestite da gruppi di interesse, portando i membri del gruppo in questione a resistere a tutto ciò che è contrario alla propria visione, seppur evidente (Croce e Piazza, 2019). Secondo Comandini, "lasciare al cittadino la libertà di cambiare la propria opinione in relazione all'accuratezza delle notizie ricevute dai media è un valore sociale importante da preservare e difendere" (Comandini, 2018, pp. 196-197).

Un secondo effetto è quello di trovarsi a convivere con *fake news* e notizie vere, e a dover distinguere, non facilmente, cosa sia vero da ciò che sia falso. Infatti, si consideri che i contenuti possono essere facilmente modificati e manipolati, così come le immagini e i video, grazie alle sofisticate tecniche di *deep fake* (Suffia e Ziccardi, 2020). Nel caso in cui i consumatori confondano notizie false e vere, ne consegue una creazione di opinioni personali non accurate e ciò per esempio si può ripercuotere nella scelta di candidati non onesti e competenti (Comandini, 2018).

Ma non solo. Essi potrebbero arrivare a provare sentimenti negativi, tra cui la rabbia, la paura e l'indignazione. Quest'ultima "è una reazione per un torto o un'ingiustizia subiti, cui è associata l'idea di malafede da parte di chi li ha commessi". Essa porta a un calo "del livello di autocontrollo del target insieme alla squalificazione degli avversari politici, accusati di imbrogliare le carte". Una volta erano i demagoghi che istigavano e provocavano la folla contro un avversario. A proposito, Comandini riporta l'esempio degli Orangisti che, attraverso racconti falsi, spinsero la folla a linciare un politico e matematico che aveva governato il paese. Oggi quest'idea di giustizia sommaria è alimentata dagli *hate speech* sul web, che fanno leva sugli istinti primordiali, che possono portare anche ad azioni violente (Comandini, 2018, p. 197).

Altri aspetti da constatare sono legati al sistema democratico nel senso più ampio. Sicuramente la corretta informazione dei cittadini viene inevitabilmente messa a rischio a causa della circolazione di notizie false o mirate a un certo individuo o gruppo. Si pensi al referendum che ha visto l'uscita del Regno Unito dall'Unione Europea. Durante la campagna favorevole all'uscita, venne diffusa la notizia falsa secondo la quale il primo pagava alla seconda 350 milioni di sterline alla settimana. Tuttavia, secondo un sondaggio, il 47% dei britannici la riteneva credibile, il 39% falsa, mentre il 14% era incerto (Palici di Suni, 2020).

Poi la formazione del consenso elettorale non è più libera se agiscono profili finti o *bot* che manipolano la verità e conducono una campagna elettorale parallela, anche attraverso contenuti d'odio usati per raccogliere consenso o per attaccare un avversario, da cui ne può derivare anche un condizionamento nel voto (Suffia e Ziccardi, 2020). I partiti usano i *bot* perché permettono di produrre artificialmente like e condivisioni e di creare siti uguali tra di loro, al fine di rilanciare la stessa notizia. In questo modo l'impressione che si ha è che quella notizia sia credibile perché molte fonti ne parlano. Inoltre, l'utente si ritrova molti account, in realtà *fake*, che lo convincono del fatto di essere parte di un movimento con molti sostenitori e questo non lo può che portare ad aderire più facilmente al progetto politico (Mazziotti Di Celso, 2018). Se però un politico sfrutta questi *bot* o lui stesso ne è a capo, vuol dire che i cittadini vengono manipolati. Per Luciano Violante i cittadini devono essere assicurati che quello che viene detto e fatto dai politici sia vero. Se il politico quindi mente ai propri concittadini e altera le regole della competizione politica, "la democrazia viene colpita al cuore perché i cittadini diventano strumenti per il suo potere"<sup>10</sup> (Pitruzzella, 2018, p. 33).

Nondimeno, il pericolo delle *fake news* è percepito diversamente tra i paesi. Può incuriosire che negli Stati Uniti e nel Regno Unito la percentuale dei cittadini che si dicono preoccupati è inferiore a quella del Brasile, della Grecia, della Francia e della Spagna, pur essendo stati condizionati

---

<sup>10</sup> Violante, Luciano. 2013. "Politica e menzogna", p. 4. Torino: Einaudi.

maggiormente i primi due durante la campagna presidenziale e in occasione del referendum sulla Brexit. In Russia, in Cina e in Turchia, invece, la libertà d'informazione è limitata o repressa e solo una minoranza è preoccupata.

Gli italiani sono più esposti a essere ingannati perché la loro capacità di comprensione e analisi dei testi scritti è particolarmente bassa (Comandini, 2018).

### **1.3 Soluzioni normative?**

Dopo aver descritto il fenomeno in questione e aver illustrato le varie modalità di diffusione, con le varie conseguenze che ne derivano sul pubblico, la seguente tesi si propone di esaminare la parte regolatoria e delle politiche pubbliche dell'Unione Europea e di due Stati membri di essa, nell'ordine la Germania e l'Italia.

Si cercheranno di analizzare i provvedimenti rilevanti che ci sono stati, attraverso il richiamo di leggi statali, proposte e studi sulle piattaforme digitali che sono stati avviati per debellare un problema che attanaglia non solo i cittadini, ma anche gli Stati, dato che riguarda la società nel suo complesso e che quindi necessita di risposte pubbliche urgenti.

Si scorgeranno le differenze e le criticità delle mosse intraprese dai soggetti poco prima menzionati, per comprendere anche i diversi approcci adottati nell'affrontare una questione comune, che interessa anche tanti altri Stati europei e non. Nel frattempo è cresciuto l'interesse scientifico per questo tema, approfondito anche da studi socio-economici (Magnani, 2019).

Nel secondo capitolo, prima di parlare dell'Europa, si vedrà come hanno agito Facebook, Twitter e Google contro la disinformazione in generale, in modo da inquadrare le loro strategie. A queste grandi *tech companies* possono essere imputate delle responsabilità, vista soprattutto la notevole rilevanza che hanno assunto nell'essere i canali principali dove circolano e vengono fabbricate le notizie, e in quanto spazi di socialità, come i

precedenti paragrafi descrivono? A questa domanda saranno utili le risposte dell'organizzazione sovranazionale e della legge tedesca, perché se da un lato il profilo giuridico dei grandi operatori di Internet non è ancora del tutto preciso, dall'altro la Commissione Europea e la Germania riconoscono il loro ruolo ineluttabile nelle politiche di contrasto alla disinformazione (Magnani, 2019).

Nel prosieguo del lavoro due problematiche verranno incontrate: la difficoltà di giungere a una definizione certa di *fake news*, visti i vari registri stilistici che possono essere utilizzati, non agevola il lavoro di chi si occupa poi di regolamentare, dato che distinguere il vero dal falso, o ciò che è lecito, può non essere così immediato, e l'introduzione di una legislazione speciale per reprimere i contenuti veicolati dai media potrebbe scontrarsi con il principio costituzionale della libertà di espressione, più volte nominato (Magnani, 2019).

## **Capitolo 2: L'autoregolamentazione della disinformazione e le iniziative europee**

Il dibattito sulle *fake news* non si è limitato a descrivere il fenomeno, ma ha anche concentrato l'attenzione sulle politiche pubbliche e sui tentativi per cercare di arginarlo. Ci si è chiesti quali possano essere gli strumenti adeguati.

Su chi ricade la responsabilità? Sono gli Stati che devono occuparsene o sono le piattaforme che devono censurare, dato che ospitano i contenuti? Tutti interrogativi che gli studiosi di scienze sociali, di politologia e di diritto, principalmente, si sono posti, nel tentativo di capire se sia meglio che le piattaforme si autoregolamentino esse stesse o se sia necessaria una qualche forma di regolazione pubblica o se la co-regolazione sia una strada percorribile.

Prima di vedere gli interventi pubblici, verranno passate in rassegna le azioni messe in campo dai social network più noti, Facebook e Twitter, e da Google.

### **2.1 L'autoregolamentazione**

Chiariamo preliminarmente il termine "autoregolamentazione". Per Bonini comprende le "regole predisposte dal Social Network per la disciplina del rapporto tra i propri utenti e tra i singoli utenti e il Social Network" (Bonini, 2020, p. 266).

Essa si inserisce nel progetto di contrasto alla disinformazione promosso dalla Commissione Europea che, dopo un lungo procedimento, è terminato con l'adozione di un Codice. L'obiettivo è di arrivare a una disciplina comune, ma facendo in modo che i social si diano delle regole riguardanti la propria struttura e che godano, loro stessi, anche dell'iniziativa per implementarle. Si parlerà più avanti di questo punto.

Nell'ordine, verranno esplorati Facebook e Twitter, poi Google, principale motore di ricerca, provando a scorgere le differenze e le somiglianze nelle loro azioni.

### **2.1.1 Facebook**

A partire da fine dicembre 2016, Facebook ha iniziato a occuparsi del problema della disinformazione, affidando la verifica dei fatti a terze parti indipendenti, seguito poi anche da Instagram a partire dal 2019. Come indicato nella pagina relativa alla trasparenza del social (Facebook, n.d.), le persone possono segnalare le notizie false attraverso un feedback, che successivamente viene verificato da organizzazioni di *fact-checking*, ossia di verifica dei fatti, che eventualmente le possono eliminare se ritenute non accurate. Viene indicato che la collaborazione comprende più di ottanta organizzazioni di *fact-checking*, certificate dall'International Fact-Checking Network (IFCN), organismo affiliato all'organizzazione di ricerca giornalistica The Poynter Institute.

Editori, giornalisti, ricercatori e accademici appartenenti all'IFCN hanno accesso anche a *CrowdTangle*, uno strumento di Facebook che li aiuta a identificare i post che contengono notizie false, fornendo dati statistici sulle prestazioni dei contenuti pubblicati sui social media.

Capiamo ora il compito del *fact-checker*, come spiegato nella pagina. È un soggetto che analizza i fatti, i dati, le fonti di una notizia, esaminando ogni parte del testo e verificando qualsiasi nome, citazione e riferimento presente al proprio interno. Sono sottoposte al controllo le informazioni false, le bufale e le affermazioni di tendenza false. Al contrario, i contenuti non verificabili, le opinioni e i discorsi di personaggi politici non vengono presi in considerazione.

La procedura è indipendente da Facebook e prevede anche la consultazione di fonti pubbliche e l'autenticazione di immagini e video, se presenti.

A tal proposito, può essere utile vedere come può essere classificato e valutato un contenuto da questi soggetti, fornendo qualche esempio associato a ogni categoria:

- falso (citazioni false, affermazioni impossibili relative a qualcosa che non è accaduto o che non è stato detto, come la segnalazione di un disastro naturale non ancora verificato, contenuti falsificati da finti organi di informazione che si nascondono per veri);
- parzialmente falso (inesattezze, errori di calcolo, mix di informazioni vere e false, opinioni che si basano su dati falsi);
- alterato (immagini e video modificati, omissioni di parole dette da una persona che invertono il significato di un'affermazione);
- privo di contesto (esagerazioni tecnicamente false ma basate su eventi o affermazioni reali, affermazioni non supportate da prove);
- satira (contenuti ironici, esagerati, di siti non chiaramente etichettati come satirici).

Il contenuto falso, parzialmente falso o alterato viene mostrato in basso nella sezione Notizie di Facebook, mentre per quanto riguarda l'ultimo, nella parte inferiore del post, viene aggiunto un articolo con informazioni verificate, pur non venendo contrassegnato come satira. Nulla viene riportato per quello privo di contesto.

Più ampiamente, la strategia della piattaforma contro la disinformazione si fonda su tre pilastri riferiti ai contenuti: la rimozione, la riduzione e l'informazione.

La rimozione dei contenuti avviene una volta violate le linee guida di Facebook. A tal punto, viene inviata una notifica all'utente comprendente i motivi che hanno portato a cancellare quel contenuto e quali norme non sono state rispettate. In base a quanti avvertimenti sono stati ricevuti, alle violazioni già commesse e alla gravità delle stesse, l'account potrebbe venire limitato fino a un massimo di trenta giorni o disabilitato. Si tenga presente che, allo scopo di dare spazio alla libertà di espressione, la rimozione vale solamente in casi limitati, cioè come viene detto, quando la

disinformazione può causare violenza fisica nell'immediato, può interferire con il diritto di voto e quando un video viene manipolato.

La riduzione riguarda i contenuti che non violano le norme di Facebook, ma che sono problematici o di bassa qualità, come commenti che vengono copiati e incollati più volte, link a siti web non funzionanti o lenti, con tante inserzioni.

Quando un *fact-checker* valuta un contenuto come falso, viene ridotta la sua distribuzione nella sezione Notizie, come è stato già detto, e non viene mostrato nei suggerimenti.

L'informazione ha come obiettivo quello di lasciare all'utente la scelta su cosa leggere e condividere. Quando gli utenti incontrano post contrassegnati come sensibili o fuorvianti, vengono fornite spiegazioni dettagliate sul perché siano tali. Un esempio sono le schermate di notifica visualizzate per i contenuti pubblicati da più di novanta giorni, in modo che prima che vengano condivisi si sia informati sulla fonte di provenienza.

### **2.1.2 Twitter**

Anche Twitter intende garantire la divulgazione di notizie attendibili, soprattutto in campo politico, ma non solo.

Come per Facebook, è possibile segnalare i tweet con contenuti dannosi o ingannevoli attraverso delle etichette. Ha fatto molto eco quando Donald Trump ha denunciato i brogli elettorali verso di lui, nell'imminenza della fine del suo mandato. I suoi tweet sono stati eliminati, sospendendo anche il suo account privato<sup>11</sup>.

Nel mese di gennaio 2021, il social ha avviato un progetto pilota innovativo, denominato "*Birdwatch*", che assegna un ruolo di primaria importanza alle persone. Infatti, sono loro stesse che possono inviare delle note riguardo ai

---

<sup>11</sup> Lombardi, Anna. 2021. "Usa, Twitter chiude definitivamente il profilo di Trump". *laRepubblica*. Ultimo accesso 19 gennaio 2022. [https://www.repubblica.it/esteri/2021/01/09/news/usa\\_twitter\\_sospende\\_permanentement\\_e\\_l\\_acconut\\_di\\_trump-281762714/](https://www.repubblica.it/esteri/2021/01/09/news/usa_twitter_sospende_permanentement_e_l_acconut_di_trump-281762714/).

tweet che ritengono essere falsi o fuorvianti, di qualsiasi ambito. Le note vengono mostrate in un sito separato da Twitter, in cui i partecipanti al progetto pilota possono anche valutare l'utilità di quelle aggiunte da altri contribuenti. Essi dovranno anche fornire un numero di telefono e un'e-mail verificati per partecipare, allo scopo di tenere lontani *bot* e malintenzionati, oltre a non essere segnalati per recenti violazioni delle regole interne di Twitter. È un approccio basato sulla comunità, come viene detto nel blog di Twitter, in un articolo relativo alla presentazione del programma (Coleman, 2021). Attualmente, però, è di esclusiva degli Stati Uniti, dell'Australia e della Corea del Sud.

Inoltre, il social collabora anch'esso, come Facebook, con agenzie di stampa, come Reuters e Associated Press, allo scopo, come riportato in un articolo della BBC, di "aggiungere contesto alle conversazioni online, che possono beneficiare di un facile accesso ai fatti", dato che il materiale delle due agenzie "migliorerebbe la credibilità delle informazioni sulla piattaforma" (Timmins, 2021).

In più, si precisa anche che la collaborazione si affianca e non si sostituisce al lavoro che compie il team di esperti di Twitter per determinare se i tweet violano le regole interne (Timmins, 2021).

### **2.1.3 Google**

La politica di Google è chiara ed è delineata in un documento presente sul sito della Camera dei Deputati, intitolato "Come Google combatte la disinformazione" (Camera dei Deputati, 2019). Essa ha tre obiettivi principali, riferiti ai suoi prodotti e servizi come Ricerca Google e Google News: dare importanza alla qualità dei sistemi di ranking, contrastare i soggetti malintenzionati e fornire contesto agli utenti.

Il primo si riferisce alla qualità dell'informazione e agli algoritmi che organizzano le informazioni, in modo che siano utili agli utenti che le incontrano e autorevoli. Viene fatto notare che le pagine ingannevoli o gli articoli disinformativi vengono relegati in posizioni meno visibili nella pagina

della ricerca, in modo da trovare prima le fonti più affidabili e conosciute. È quello che si è visto che è presente su Facebook riguardo ai contenuti falsi, parzialmente falsi o alterati.

Il secondo indica tutte le norme espressamente indicate che descrivono i comportamenti proibiti, come lo spam o la non trasparenza.

Il terzo include tutti i riquadri che informano riguardo a una persona o un tema, le etichette che spiegano perché si vede un determinato annuncio e i pulsanti di feedback per segnalare contenuti ritenuti non appropriati. È il punto di Facebook che concerne l'informazione.

Ma Google va oltre il mero controllo. Come Facebook e Twitter, collabora con la stampa e gli autori di *fact-checking*, anche perché spesso la maggior parte delle notizie che si trovano provengono da giornalisti e agenzie di notizie. Allo scopo di migliorare il giornalismo online, Google dice di aver investito in programmi che incrementino la qualità di esso e di collaborare con l'International Fact-Checking Network di Poynter, organizzazione no-profit che raggruppa agenzie di *fact-checking* presenti in vari stati del mondo.

Obiettivo che si prefigge il motore di ricerca è anche proteggere l'integrità delle elezioni in modo che si svolgano equamente. A questo scopo, operano team che disattivano l'account di soggetti sospetti e che propongono corsi di formazione ai partiti politici sulle modalità di protezione dagli attacchi informatici.

È indicato anche che Google News proibisce tutti quei contenuti che sono violenti o che incitano alla violenza.

## **2.2. L'approccio europeo**

L'Unione Europea si è occupata in prima linea del problema della disinformazione. Già nel 2015 ha lanciato la *task force* East StratCom del Servizio europeo per l'azione esterna (SEAE) per combattere quella proveniente dalla Russia e per sostenere il pluralismo dei media nei paesi orientali, anche se è soprattutto negli ultimi anni che se n'è occupata con

maggior forza, in collaborazione con gli Stati. Non a caso, la Commissione Europea, in vista delle elezioni del Parlamento Europeo del 2019, ha invitato le autorità nazionali a identificare gli attacchi informatici e a reprimere la disinformazione (Corte dei Conti UE, 2021).

Il Parlamento europeo ha incaricato la Commissione Europea di analizzare la situazione. Inizialmente, essa ha aperto una consultazione pubblica, svoltasi nel periodo che va da novembre 2017 a febbraio 2018. Successivamente, l'indagine Eurobarometro Flash e il report redatto da un gruppo di esperti, pubblicato poi ad aprile 2018, hanno permesso di elaborare una strategia europea riguardo alla diffusione di notizie false, culminata nella redazione del "Code of Practice on Disinformation" nel luglio dello stesso anno.

In seguito, è stato elaborato un "Piano d'azione contro la disinformazione", in cui rientra anche il Codice, e un "Sistema di Allerta Rapido".

### **2.2.1 La consultazione pubblica e l'indagine Eurobarometro**

La consultazione pubblica, promossa dalla Commissione, ha visto la partecipazione di persone fisiche, tra cui giornalisti, cittadini ed esperti, ma anche società di media e università (Commissione Europea, 2018e). Allo scopo di far emergere le opinioni delle parti interessate riguardo al dibattito sulle *fake news*, si è capito quali siano i canali di informazione in base alla diversa età degli intervistati. Infatti, coloro con più di cinquant'anni utilizzano meno i social media (59%) rispetto alle generazioni più giovani (72%), e di più la televisione e la radio, perché nutrono poca fiducia nei siti web.

La percezione della quasi totalità dei partecipanti è che esse si diffondano più facilmente online perché vengono create per attirare le emozioni di chi le legge. Più della metà crede che servano anche per generare entrate o per orientare il dibattito politico intorno a temi caldi come l'immigrazione, le minoranze etniche e religiose e la sicurezza dei paesi membri dell'UE.

Non trascurabile è il fatto che negli Stati membri si ritiene che il *debunking*, cioè smascherare notizie false, e il *fact-checking* non siano misure

sufficienti per arginare il fenomeno della disinformazione, in quanto non raggiungono tempestivamente l'utente.

In generale, è stato evidenziato che la maggior parte dei lettori di notizie, il più delle volte, non è consapevole della necessità di verificare, controllare e confrontare che le fonti e i fatti siano realmente accaduti.

Alla domanda riguardo a cosa essi si aspettino come misure e interventi, è condiviso il bisogno di alfabetizzare e di responsabilizzare gli utenti, rendendoli più consapevoli dei mezzi collegati alla rete. Al contrario, l'idea di porre delle misure repressive a carico delle piattaforme online passa in secondo piano, in quanto è vista, soprattutto dai cittadini e dai giornalisti, come una censura, che limita la libertà di espressione online (Commissione Europea, 2018e).

L'indagine Eurobarometro, chiamata "Fake News and disinformation online", pubblicata a marzo 2018, è stata una ricerca che ha interessato più di ventiseimila cittadini dell'Unione appartenenti a diversi gruppi sociali e demografici (Commissione Europea, 2018c). Attraverso le interviste telefoniche si è indagato:

- sulla fiducia che ripongono gli intervistati nelle notizie e nelle informazioni incontrate nei vari mezzi d'informazione, come la radio, la televisione, i social network, ecc.;
- sulla percezione delle persone rispetto alla frequenza d'incontro di notizie false;
- sulla percezione nel saperle riconoscere;
- sul loro punto di vista rispetto alla portata del problema, sia nel proprio paese sia per la democrazia;
- su chi debba avere la responsabilità nel fermare la loro diffusione.

Sul primo punto è emerso che si nutre maggiore fiducia nella radio (70%), seguono poi la televisione (66%) e la stampa (63%), con il 47% che si fida dei giornali online (27%), dei social network e delle app di messaggistica (26%). Se si considera l'età, sono i giovani, di età compresa tra i 15 e i 24 anni, a fidarsi delle fonti online in misura maggiore rispetto a quanto

dichiarato da chi ha dai 55 anni in su, tendenza già rilevata nella consultazione pubblica precedente.

Riguardo alla frequenza, il 37% ha detto di ricevere notizie false ogni giorno, o quasi, mentre in ogni paese almeno la metà ha dichiarato di incontrarle almeno una volta alla settimana. I giovani sono quelli che si imbattono più facilmente nelle *fake news* almeno una volta alla settimana, così come gli uomini (73%) rispetto alle donne (64%).

Sul saperle identificare, il 71% si ritiene abbastanza convinto di poterle riconoscere, anche se solo il 15% lo è del tutto. Chi le incontra più frequentemente è poi convinto di saperle svelare una volta incontrate (79%) rispetto a coloro che le trovano raramente (55%). I giovani, oltre a incontrarle spesso, sono i più convinti di saperle riconoscere.

Sul quarto punto, per il 44% le *fake news* e la disinformazione sono un problema per il proprio paese, mentre è bassa la percentuale di chi si dissocia completamente (3%). Si noti che i paesi che hanno attraversato crisi economiche o politiche dimostrano di essere più preoccupati, ad esempio l'Italia e la Grecia (90%). Ma esse sono percepite come un problema anche per la democrazia (45%), solo il 4% lo nega.

Interessante è l'ultima tappa dell'indagine, di cui si riporta la figura 2.1 nella prossima pagina, che mostra chi si ritiene che abbia la responsabilità di eliminare la loro diffusione. Il 45% dice che ce l'abbiano i giornalisti, invece il 36% la stampa. Salta all'occhio che le autorità nazionali sono menzionate di più delle istituzioni dell'UE o delle organizzazioni non-governative, rispettivamente il 39% contro il 21% e il 15%. Il 32% pensa che siano i cittadini stessi che dovrebbero agire, mentre il 26% crede che la responsabilità ricada sui social network.

I giornalisti sono la prima risposta in ventidue paesi membri, la stampa in tre paesi (Svezia, l'allora Regno Unito e la Repubblica Ceca), le autorità nazionali in quattro paesi (Bulgaria, Italia, Ungheria e Lettonia). Le istituzioni dell'UE hanno il dato più alto in Spagna (33%) e le organizzazioni non-governative in Austria e in Polonia (22%), mentre i cittadini stessi in Francia,

in Austria e in Portogallo (38%) e i social network in Irlanda e nel Regno Unito (38%).

Chi frequenta spesso i social, soprattutto i più giovani, assegna la responsabilità alle piattaforme, ma anche ai cittadini stessi.

Nel complesso:

- una piccola minoranza di chi ha risposto ha una fiducia totale in qualsiasi fonte, perché tende a fidarsi maggiormente dei media tradizionali;
- il problema è rilevante perché due terzi dice di incontrarle almeno una volta a settimana e perché è percepito tale nel proprio paese e in relazione alla democrazia;
- pochi sono molto convinti di saperle identificare (15%);
- è un'*issue* riconosciuta da diversi Stati e tra differenti gruppi sociali e demografici;
- non vi è ancora un consenso unanime tra il pubblico su chi dovrebbe intervenire (Commissione Europea, 2018c).

Q5 News or information that misrepresent reality or that are even false are called "fake news". Which of the following institutions and media actors should act to stop the spread of "fake news"? (MAX. 3 ANSWERS) (% - EU)



**FIGURA 2.1** Commissione Europea. 2018. "Flash Eurobarometer 464. Fake News and disinformation online", p. 27.

## **2.2.2 Il “Codice di buone pratiche dell’UE sulla disinformazione” e il “Piano d’azione contro la disinformazione”**

Sulla scorta di questi due documenti, la Commissione Europea ha poi incaricato un team di esperti, composto da accademici, giornalisti, organizzazioni televisive e di *fact-checking*, piattaforme online e membri della società civile, di studiare delle iniziative pubbliche per contrastare le *fake news* e la disinformazione.

Dall’High Level Expert Group (HLEG), letteralmente “Gruppo di Esperti di Alto Livello”, è uscito un report riassuntivo del loro lavoro, pubblicato ad aprile 2018 (Commissione Europea, 2018a).

In primo luogo viene condiviso che la disinformazione va oltre le *fake news*. Infatti, essa include tutte le forme di falsità progettate per causare un danno pubblico o per guadagnare. Non per forza i contenuti devono essere completamente falsi. Anche i comportamenti che concernono la disinformazione nelle piattaforme online, come i commenti, le condivisioni e i tweet, vengono fatti rientrare.

In secondo luogo le norme adottate dovrebbero essere valide in tutti gli Stati membri e queste non dovrebbero scontrarsi con l’Articolo 11 della Carta dei diritti fondamentali dell’Unione Europea, cioè il principio della libertà di espressione. Per questo viene auspicato un approccio multidimensionale che coinvolga istituzioni europee, governi nazionali, piattaforme online, agenzie di comunicazione, giornalisti e cittadini, basato su cinque obiettivi:

1. migliorare la trasparenza delle notizie online;
2. promuovere l’alfabetizzazione dei media e aiutare gli utenti a navigare online;
3. sviluppare strumenti che responsabilizzino gli utenti e i giornalisti;
4. salvaguardare la libertà di espressione, la libertà di stampa e il pluralismo dei media;
5. studiare l’impatto della disinformazione in Europa attraverso ricerche continue (Commissione Europea, 2018a).

Qualche mese più tardi è stato redatto il “Codice di buone pratiche sulla disinformazione”, o “Code of Practice on Disinformation” (Commissione Europea, 2018b).

Viene ripresa la stessa definizione di disinformazione dell’HLEG, secondo cui essa è “un’informazione rivelatasi falsa o fuorviante”, “concepita, presentata e diffusa a scopo di lucro o per ingannare intenzionalmente il pubblico” e “che può arrecare un pregiudizio pubblico”, inteso come “minacce ai processi politici democratici e di elaborazione delle politiche e a beni pubblici quali la tutela della salute dei cittadini, dell’ambiente e della sicurezza dell’UE”. Non sono incluse “la pubblicità ingannevole, gli errori di segnalazione, la satira e la parodia” e le “comunicazioni di parte” (Commissione Europea, 2018b, p. 1).

Il Codice esplicita chiaramente che esso si applica tenendo conto di normative vigenti nell’UE e negli Stati membri, soprattutto la Carta dei diritti fondamentali dell’UE, la Convenzione Europea dei diritti dell’uomo e il regolamento 679/2016 sul trattamento dei dati personali (Commissione Europea, 2018b).

Il Codice comprende cinque aree, comprensive di tutto quello che i firmatari devono impegnarsi a rispettare:

1. inserzioni pubblicitarie. Posizionare le inserzioni pubblicitarie in modo da ridurre la possibilità di profitto dei fornitori di disinformazione; obbligare a collaborare chi acquista e vende pubblicità online e fornisce servizi pubblicitari, per limitarla sui profili e sui siti web di chi fa disinformazione;
2. messaggi pubblicitari di natura politica e campagne di sensibilizzazione. Garantire la trasparenza di tali messaggi per far capire agli utenti perché compaiono determinate pubblicità rispetto ad altre; fare in modo che gli annunci pubblicitari siano ben distinguibili dai contenuti editoriali, comprese le notizie; “consentire la divulgazione al pubblico dei messaggi pubblicitari di natura politica” (Commissione Europea, 2018b, p. 5);

3. integrità dei servizi. Identificare e chiudere gli account falsi e stabilire dei meccanismi per la segnalazione dei *bot*; non vietare l'utilizzo di profili e servizi anonimi; "attuare politiche chiare in materia di identità e abuso di *bot* automatizzati nei loro servizi" (Commissione Europea, 2018b, p. 6);
4. responsabilizzazione dei consumatori. Permettere all'utente di reperire contenuti affidabili e di accedere a varie fonti che rappresentino punti di vista alternativi; fornire strumenti per segnalare i casi di disinformazione e indicatori oggettivi per valutare l'"affidabilità delle fonti dei contenuti, la proprietà dei media e la verifica dell'identità" (Commissione Europea, 2018b, p. 7);
5. responsabilizzazione della comunità dei ricercatori. Consentire ai ricercatori l'accesso ai dati per monitorare la disinformazione e fornire informazioni sul funzionamento degli algoritmi.

La sottoscrizione del Codice e dei relativi impegni è volontaria, come ribadito al proprio interno. Ogni firmatario deve presentare relazioni periodiche alla Commissione riguardo all'attuazione degli impegni (Commissione Europea, 2018b). Nell'ottobre dello stesso anno hanno subito aderito Facebook, Twitter, Google, Mozilla, inserzionisti e associazioni di categoria del settore pubblicitario. Microsoft l'ha firmato nel maggio 2019, seguito da TikTok a giugno 2020 (Corte dei Conti, 2021). Il Codice si inserisce nel "Piano d'azione contro la disinformazione", pubblicato alla fine del 2018, che si fonda su quattro pilastri:

1. migliorare le capacità delle istituzioni dell'Unione di individuare, analizzare e denunciare la disinformazione;
2. potenziare le risposte coordinate e comuni;
3. mobilitare il settore privato;
4. sostenere azioni di sensibilizzazione e rafforzare la resilienza sociale (Commissione Europea, 2018d).

Nel primo pilastro si sottolinea la necessità di incrementare il personale di comunicazione strategica del SEAE e di investire in strumenti di analisi,

come programmi informatici, al fine di estrarre e analizzare molti dati (Commissione Europea, 2018d).

Il secondo riguarda la creazione di un “Sistema di Allerta Rapido”, lanciato a marzo 2019, che consente di segnalare immediatamente le campagne di disinformazione in un’apposita piattaforma digitale. Questa permette di condividere i dati e le migliori pratiche immessi dagli Stati membri e dalle istituzioni dell’UE, allo scopo di coordinare e valutare, continuamente e più rapidamente, le proprie attività d’intervento e di migliorare le risposte, con conseguente risparmio di tempo e di risorse. Il SEAE, in cooperazione con la Commissione, ma anche con la NATO, il G7 e altri partner, facilita gli scambi tra i soggetti, con l’aiuto anche di *fact-checker* indipendenti (SEAE, 2019).

Nel terzo coloro che hanno firmato il Codice di buone pratiche vengono esortati ad attuare le azioni individuate in esso ed è predisposto un monitoraggio per garantirne l’osservanza. Inoltre, le piattaforme online dovrebbero “collaborare con le autorità nazionali di regolamentazione del settore audiovisivo e con i ricercatori e i verificatori di fatti indipendenti” (Commissione Europea, 2018d, p. 10).

Nell’ultimo si sostiene l’importanza di capire perché i cittadini siano attratti dalla disinformazione. Conferenze e dibattiti, con ricercatori e *fact-checker*, sono fondamentali per sensibilizzare il pubblico sulle minacce derivanti da questa problematica, così come i corsi di formazione per i media. In più, è essenziale il lavoro di denuncia da parte dei giornalisti investigativi e dei media indipendenti (Commissione Europea, 2018d).

### **2.2.3 Criticità delle azioni dell’UE**

Grazie ai documenti sintetizzati si sono visti i passi compiuti dall’Unione Europea per fronteggiare la disinformazione, accompagnati dai dati dell’indagine dell’Eurobarometro e dello studio degli esperti, e dal Codice. Ora, nel concludere il secondo capitolo, si passerà a fare qualche considerazione generale in merito al Codice dell’Unione e al Piano.

Il “Code of Practice on Disinformation” è stato firmato da partner digitali importanti, ma è molto flessibile. Infatti, i sottoscrittori possono applicare i suoi principi come meglio credono, così come sono liberi di non aderire o di non assumere più gli impegni da un momento all’altro, attraverso un semplice avviso alla Commissione e agli altri aderenti. D’altra parte è anche vero che nuovi attori possono entrare liberamente (Monti, 2019), sebbene l’European Regulators Group for Audiovisual Media Services (ERGA), nel suo recente rapporto, lamenta il numero limitato di sottoscrittori del Codice e raccomanda di aumentarlo in futuro, includendovi per esempio anche WhatsApp (ERGA, 2020).

Secondo Monti, “il Codice ha l’indubbio merito di chiarire che cos’è una fake news”, che fa parte della disinformazione, secondo la definizione data dal gruppo di esperti, escludendo la satira e le comunicazioni politiche. A proposito delle ultime, lui ricorda che nella comunicazione politica il falso rientra nel concetto di libertà di manifestazione del pensiero, mentre il falso come informazione non vi è incluso. Perciò, se da un lato si puniscono i mezzi d’informazione online che non si conformano alle regole del giornalismo, dall’altro è opportuno evitare che avvenga una “censura privata” dei pensieri politici (Monti, 2019, p. 321).

Sempre secondo Monti, lo si può annoverare tra gli strumenti di *soft law* e un punto di forza sono le buone pratiche indicate al proprio interno, che i privati sono liberi di attuare e implementare (Monti, 2019). Tuttavia, il fatto che gli impegni non siano del tutto chiari e oggettivamente misurabili, e che non si possa effettuare un controllo sulla loro implementazione, porterebbe a non ricondurre il Codice nella categoria degli atti di *soft law* (Pagano, 2019). Questo autore evidenzia la presenza di elementi privatistici in cui:

- un soggetto pubblico non ha un ruolo predominante nella fase di adozione;
- il consenso è necessario per produrre degli effetti giuridici;
- i sottoscrittori possono limitare il proprio impegno solo ad alcuni obiettivi;

- un termine finale di scadenza è presente, per decidere se continuare ad applicare le disposizioni del Codice o se cambiare strategia;
- il carattere delle disposizioni è flessibile;
- la possibilità di uscire dal Codice richiama il modello della contrattazione privata (Pagano, 2019).

Però lo stesso autore non nega che il Codice prevede un monitoraggio e una valutazione degli obiettivi da parte della Commissione. La stessa ha esercitato un potere di guida nel procedimento d'adozione dell'atto, all'inizio, e ha indirizzato le condotte dei firmatari, poi. Con i primi report di valutazione e con le successive raccomandazioni, i soggetti si sono conformati alle indicazioni dell'istituzione europea, prova concreta del potere esercitato da un soggetto pubblico nel determinare le modalità di attuazione. Sulla base di queste considerazioni, per l'autore il Codice ha una natura mista, in cui "ai tratti tipici della regolazione prodotta da soggetti privati, accosta elementi caratteristici della regolazione *soft* di natura pubblicistica", ed è riconducibile alla co-regolazione, testimoniato dal ruolo della Commissione, che definisce il contenuto delle relazioni periodiche, valuta l'adempimento degli obblighi e determina le conseguenze di possibili inadempimenti, al punto da poter pubblicizzare il soggetto inadempiente (Pagano, 2019, p. 29). Tra l'altro l'idea della co-regolazione è stata ribadita anche dall'ERGA nel suo rapporto (ERGA, 2020).

Pitruzzella, nel suo saggio di qualche anno fa, auspicava "un insieme di regole che specifichino meglio quali sono gli obblighi nella rete, le responsabilità delle piattaforme, e che prevedano, in caso di conflitto, un rapido intervento di istituzioni terze rispetto alle parti" (Pitruzzella, 2018, p. 45). Riguardo a queste ultime parole, nel Codice pare esserci proprio una terza parte che promuove e controlla una regolazione, e non lascia "ad un manipolo di compagnie multinazionali, ciascuna dotata di un enorme potere economico e di un'incredibilmente vasta capacità di influenza, il monopolio in ordine al controllo dell'informazione sulla rete" (Pitruzzella, 2018, p. 45). Anche il Piano d'azione è stato esaminato a fondo. Può essere utile

soffermarsi su qualche considerazione fatta dalla Corte dei Conti europea in una sua recente relazione (Corte dei Conti UE, 2021).

Secondo la Corte, il Piano si appropria in maniera sia reattiva, attraverso la riduzione e la visibilità dei contenuti di disinformazione, sia proattiva, a lungo termine, con misure di alfabetizzazione mediatica. È stato ritenuto pertinente perché ha coinvolto molti soggetti, privati, pubblici, della società civile e *fact-checker*.

Tuttavia, viene lamentato il fatto che il Piano sia stato poco monitorato e che la prima e unica relazione sull'attuazione dello stesso, di giugno 2019, sia carente perché non fornisce indicatori di misura delle performance.

Inoltre, manca un piano finanziario per coprire i costi delle attività e non sono sempre garantiti finanziamenti a lungo termine.

Nello specifico, la Corte ha anche valutato l'attuazione del Piano e come esso ha migliorato le azioni dell'Unione.

Riguardo al primo pilastro, la *task force* East StratCom del SEAE ha contribuito a combattere la disinformazione russa nei paesi orientali dell'UE, ma non ad esempio quella proveniente dalla Cina e da altri paesi.

Il "Sistema di Allerta Rapido" rappresenta uno strumento utile per condividere le informazioni, ha avvicinato gli Stati membri e le istituzioni, offrendo nuovi spunti d'intervento, ma, almeno fino a quanto dichiarato dalla relazione della Corte, non ha emesso segnalazioni. È stato creato in vista delle elezioni europee del 2019 e prima di allora non c'era mai stato qualcosa di simile, ma lo scopo primario era creare una comunità di operatori. Per la Corte questo ha ingenerato nel pubblico interessato confusione, così come la sua attivazione, che si ha solo quando la disinformazione ha un "impatto transnazionale significativo", espressione troppo indefinita nella formulazione (Corte dei Conti UE, 2021, p. 31).

In più, secondo le statistiche, solo un terzo degli Stati membri partecipano regolarmente e sono molto attivi nelle riunioni, il cui picco di attività è stato raggiunto nelle elezioni europee e nelle prime settimane successive al *lockdown* di metà marzo 2020, per poi diminuire.

Grazie al Codice di buone pratiche le piattaforme online hanno preso posizione in merito alla disinformazione. Infatti, Google ha bloccato o rimosso oltre 82,5 milioni di pubblicità in occasione del Covid-19 e ad agosto 2020 oltre quattro milioni di utenti europei hanno visitato fonti autorevoli sul tema. I “centri di informazione” di Facebook e Instagram dedicati al virus, a luglio e ad agosto, sono stati visitati rispettivamente da più di 13 e 14 milioni di utenti nell’UE.

Sintetizzando, tra i punti di debolezza del Codice vi sono:

- scarsa trasparenza sul come attuarlo;
- misure troppo generiche in quanto a contenuto e struttura;
- numero limitato di firmatari del Codice;
- mancanza di sanzioni per non avere rispettato gli impegni, vista l’adesione volontaria (Corte dei Conti UE, 2021).

### Capitolo 3: L'intervento della Germania

Dopo aver visto alcune azioni di autoregolamentazione messe in campo dalle piattaforme e, in particolare, dall'Unione Europea, ora si proseguirà con le politiche adottate a livello nazionale da due Stati, la Germania e l'Italia. Nel panorama europeo, un'attenzione intensa alle *fake news* e alla disinformazione l'ha posta proprio la Repubblica tedesca, primo Stato in Europa che ha varato una legge specifica per regolamentare una piaga sociale, visto che negli ultimi anni i social network sono diventati colmi di contenuti offensivi e d'odio, che spesso possono degenerare in violenza, e di *fake news*, grazie anche all'anonimato di Internet. Un fenomeno che si è proliferato progressivamente, soprattutto in seguito ai tanti profughi provenienti dal Medio Oriente ed entrati in Germania, all'inizio del 2015, portando estremisti di destra a scagliarsi contro i rifugiati, ma anche contro i funzionari governativi (Echikson e Knodt, 2018).

In risposta, il ministro della Giustizia Heiko Maas ha creato un'*équipe*, che ha incontrato Facebook, Google, Twitter, rappresentanti della società civile e aziende tecnologiche impegnate a creare strumenti di segnalazione intuitivi (Echikson e Knodt, 2018).

A dicembre 2016, il Servizio Ricerche del Bundestag aveva pubblicato un report per affrontare la disinformazione, spinto anche da una denuncia penale che era stata presentata dalla politica Renate Künast, del Partito dei Verdi, contro gli autori di una *fake news*, pubblicata in più pagine Facebook, le quali mostravano un'immagine di lei che, riguardo all'omicidio di una studentessa di Friburgo, ribadiva di aiutare il killer, un giovane rifugiato, rimasto traumatizzato dall'accaduto. Lei criticava la lentezza di Facebook nell'eliminare le sue affermazioni false, tolte solamente dopo tre giorni (Levush, 2019).

Inoltre, alcuni parlamentari tedeschi avevano chiesto di introdurre un obbligo, a carico delle piattaforme, di identificazione dei *bot*, e di controllo verso chi pubblica annunci politici, ideologici o religiosi (Levush, 2019).

Per Maas il pugno duro, attraverso una legge, era l'unico modo per affrontare le offese nei social media e per stare dalla parte degli utenti lesi (Echikson e Knodt, 2018).

Di seguito, verranno esposti contenuti e finalità della legge menzionata all'inizio di questo capitolo, ma anche profili critici che sono stati avanzati, oltre a qualche risvolto pratico che si è potuto osservare.

### 3.1 La NetzDG

La *Netzwerkdurchsetzungsgesetz*, d'ora in poi NetzDG, in italiano tradotta come "Legge per il miglioramento dell'applicazione del diritto nei social network" e in inglese "Network Enforcement Act", è stata approvata dalla coalizione CDU/CSU, su proposta del Ministro della Giustizia e la Tutela dei Consumatori Heiko Maas (SPD). I parlamentari di sinistra hanno votato contro di essa, mentre i Verdi si sono astenuti (Echikson e Knodt, 2018). È entrata in vigore il primo ottobre 2017 (Senato, 2017b), dopo le elezioni federali del 24 settembre 2017.

Il provvedimento consta di tre articoli, da cui derivano alcuni obblighi a carico dei social network, come:

- la redazione di una relazione semestrale sul trattamento dei reclami riguardanti i contenuti illegali;
- la rimozione o il blocco all'accesso dei contenuti entro un certo termine;
- l'individuazione del soggetto ricevente servizi in Germania (Senato, 2017b).

Nel primo paragrafo dell'articolo 1 si definiscono i *provider*, che sono "tutti quei fornitori di servizi di telecomunicazione che a fine di lucro amministrano piattaforme Internet progettate per permettere agli utenti di condividere qualunque tipo di contenuto o di renderlo accessibile al pubblico" (Magnani, 2019, p. 14), esclusi quelli con meno di due milioni di iscritti, né le piattaforme che offrono contenuti giornalistici o editoriali la cui

responsabilità è del fornitore di servizi, né quelle per la comunicazione individuale (Senato, 2017b), o per servizi come Messenger o WhatsApp. Sono dunque interessati Facebook, Twitter, Google, Instagram, YouTube (Rinceanu, 2021).

Nel secondo viene previsto l'obbligo, per i gestori che abbiano ricevuto più di 100 segnalazioni di contenuti illeciti all'anno, di redigere una relazione semestrale di gestione di tali reclami, che poi verrà pubblicata sulla Gazzetta federale e sul proprio sito web. Questa dev'essere sempre disponibile e accessibile e deve mettere in risalto le azioni intraprese dal *provider*, deve indicare i criteri utilizzati nella scelta se bloccare o cancellare i contenuti, il numero dei reclami ricevuti, i motivi delle denunce e le informazioni sul personale che si occupa della gestione delle segnalazioni (Senato, 2017b).

Nel terzo è descritta la procedura di trattazione delle denunce. Dopo aver verificato che il contenuto denunciato è illegale, il *provider* rimuove o blocca l'accesso ai contenuti, a seconda che siano manifestamente illeciti o meno. Per i primi deve avvenire entro 24 ore dalla ricezione del reclamo dell'utente, mentre per i secondi entro 7 giorni, estendibili se la decisione dipende da falsa accusa o se, entro 7 giorni dalla ricezione del reclamo, la piattaforma delega la decisione a un'agenzia di autoregolamentazione esterna. Questa è tale se:

- è indipendente e dispone di tecnici;
- analizza rapidamente i reclami, al massimo entro 7 giorni;
- adotta norme procedurali che regolano l'ambito e la durata dell'analisi, stabiliscono i requisiti di ammissione dei social network affiliati e la possibilità di riesaminare le decisioni;
- ha istituito un servizio reclami;
- è finanziata da diversi *provider* di social network o istituzioni che garantiscano la disponibilità dei servizi ed è aperta all'ammissione di altri fornitori di servizi (Senato, 2017b).

È importante chiarire che non vengono create nuove categorie di contenuti illegali (Leerssen e Tworek, 2019). Infatti, i contenuti rientranti nell'illecito sono elencati, in modo tassativo, in un catalogo di ventidue reati previsti dal codice penale tedesco (Leerssen e Tworek, 2019; Levush, 2019). Tra questi vi è l'incitamento all'odio, la diffamazione, la diffusione di materiale propagandistico o di utilizzo di simboli di organizzazioni incostituzionali (Rinceanu, 2021). Si applica poi anche ad altre categorie, come la violazione dell'intimità, la falsificazione di dati destinati a fornire prove, la diffusione di rappresentazioni di violenza e la formazione di organizzazioni terroristiche (Leerssen e Tworek, 2019).

Inoltre, il *provider* deve notificare al denunciante e all'utente ogni decisione in modo tempestivo, fornendo una spiegazione dell'accettazione o del rifiuto, ed è tenuto a conservare il contenuto rimosso per 10 settimane. Il personale del social network, tra l'altro, deve monitorare mensilmente la gestione dei reclami e seguire corsi di formazione professionale (Senato, 2017b).

Nel quarto si indicano le sanzioni conseguenti all'inosservanza degli obblighi. Si ha un illecito amministrativo, con sanzione pecuniaria che varia da 500.000 euro e che può arrivare fino a 5 milioni di euro, se:

- la relazione sui reclami non viene presentata, è incompleta o tardiva;
- la procedura per trattare i reclami di contenuti illegali, presentati dagli organismi di reclamo o dagli utenti residenti o con sede legale in Germania, non viene predisposta;
- il controllo sulla gestione dei reclami non è presente o non viene attuato il monitoraggio;
- le carenze organizzative non vengono rettificate tempestivamente;
- la formazione al personale impiegato nella procedura non viene offerta;
- il soggetto obbligato non nomina una persona autorizzata a ricevere il servizio in Germania o non nomina quella che deve ricevere le richieste di informazione dalle autorità tedesche o, in veste di

rappresentante nazionale autorizzato a ricevere il servizio, non risponde alle richieste di informazione.

Tra gli operatori vi sono anche persone giuridiche, a cui l'entità della sanzione può essere inasprita fino a 50 milioni di euro (Senato, 2017b).

Nel quinto è disciplinato l'obbligo di nomina di una persona autorizzata a ricevere il servizio in Germania e di un'altra incaricata a ricevere le richieste di informazione dalle autorità tedesche (Senato, 2017b).

Con l'articolo 2, il *provider* ha la possibilità di informare, in casi individuali, sui dati relativi agli abbonati, "nella misura in cui ciò sia strettamente necessario ai fini della tutela di diritti personali bisognevoli di protezione dalla violazione derivante dalla pubblicazione di contenuti illegittimi su piattaforme Internet" (Senato, 2017b, p. 4).

Il 28 giugno 2021 è entrata in vigore una legge di modifica della NetzDG.

In primo luogo è stato previsto che la procedura per presentare i reclami sui contenuti illeciti ai fornitori di social network sia facilmente accessibile e più intuitiva (Gesley, 2021). Eppure, questo requisito non è stato implementato in modo uniforme dai fornitori e alcuni moduli per inviare i reclami sono risultati nascosti o disponibili solo dopo diversi click, come poi si vedrà.

In secondo luogo vengono obbligati i fornitori di social network a istituire un meccanismo in base al quale il denunciante e l'utente interessato possono avviare un riesame della decisione di rimuovere o meno i contenuti segnalati, che all'inizio non era previsto, ma che molti lamentavano. In aggiunta l'emendamento autorizza l'Ufficio federale di giustizia ad approvare l'intervento di organi arbitrali per risolvere, in via extragiudiziale, le controversie tra ricorrenti e *provider* (Gesley, 2021).

In terzo luogo viene richiesto, ai social network che ricevono più di 100 reclami annuali e che sono tenuti a pubblicare rapporti semestrali in tedesco su come gestiscono tali reclami, che nelle relazioni sulla trasparenza siano incluse maggiori informazioni. Gli interessati devono segnalare:

- le procedure per il rilevamento automatico di contenuti illegali, se vengono utilizzate;

- quali dati di formazione per il sistema vengono utilizzati e quali procedure per l'assicurazione della qualità o la valutazione sono in atto;
- il numero di reclami, suddivisi in base al tempo impiegato per rimuovere il contenuto segnalato (entro 24 ore, entro 48 ore, entro una settimana o in un secondo momento);
- le informazioni sulla nuova procedura di ricorso (Gesley, 2021).

In quarto luogo la legge di modifica conferisce all'Ufficio federale di giustizia il potere di vigilare sull'osservanza della legge. Secondo la precedente versione, l'Ufficio poteva emettere ammende solo per il mancato rispetto delle disposizioni della NetzDG. Accertata una violazione, l'Ufficio può richiedere al *provider* di porvi rimedio e ricevere informazioni sulle misure di attuazione, sul numero di utenti registrati in Germania e sul numero di reclami ricevuti nell'ultimo anno (Gesley, 2021).

### 3.1.1 Critiche e implicazioni

La legge NetzDG è stata ritenuta un grande sforzo da parte di uno Stato di responsabilizzare le piattaforme di social network per quanto riguarda la lotta all'*hate speech*. In un sondaggio di marzo 2018, l'87% ha approvato il provvedimento, con il 67% che lo approvava fermamente e solo il 5% che lo disapprovava. Stefan Heumann, co-direttore del *think thank* di politica digitale Stiftung Neue Verantwortung, sosteneva tale legge, strumento di protezione delle minoranze e della *rule of law* online (Leerssen e Tworek, 2019).

Tuttavia, per altri è sembrata molto controversa ed è stata criticata per essere incostituzionale, in particolare rispetto alla libertà di espressione, al punto che sono state presentate proposte per modificare o abrogare tale legge (Levush, 2019). Per la German Journalists Association e la Global Network Initiative (GNI), organismo di autoregolamentazione, il discorso

democratico è minacciato, così come per altri soggetti, come Wikimedia Deutschland e la German Startups Association (Leerssen e Tworek, 2019). Una prima preoccupazione riguardava il fatto che la legge avrebbe incoraggiato la rimozione di contenuti legali, portando a un *over-removal*, una rimozione quindi eccessiva. Questo perché si sosteneva che le piattaforme online non avrebbero avuto il tempo o l'esperienza per valutare dettagliatamente ogni reclamo, in quanto tali valutazioni richiedono conoscenze approfondite della lingua e della giurisprudenza tedesca e specifiche capacità di analisi. Oltre a queste, vi sono sanzioni non da poco, come è stato visto nel paragrafo precedente. Perciò, le piattaforme avrebbero un incentivo a soddisfare la maggior parte dei reclami, indipendentemente dai loro meriti (Leerssen e Tworek, 2019). Per Rinceanu i fornitori diventano quindi dei "censori contro la loro volontà", dato che spesso si ritrovano al punto di rimuovere dei contenuti di cui non è facile accertarne l'illiceità. Il rischio è che possano essere cancellati anche contenuti leciti (*overblocking*), per cui non vige ancora un divieto di cancellazione (Rinceanu, 2021, p. 10).

In questo modo, i critici vedono che con la NetzDG sono le piattaforme private che valutano la legalità dei contenuti, piuttosto che i tribunali o altre istituzioni legittimate. Non è necessaria un'ingiunzione del tribunale prima della rimozione dei contenuti e gli utenti non possono ricorrere per cercare un risarcimento (Leerssen e Tworek, 2019). "Lo Stato delega ai provider il potere di decidere sull'applicazione di misure censorie, creando perciò una torre di guardia, privata, sulle opinioni". Questi a loro volta, possono delegare la verifica a un organismo di verifica, come la legge prescrive, secondo il modello dell'autoregolamentazione, anche se solo in casi controversi, cioè per i contenuti non manifestamente illeciti (Rinceanu, 2021, pp. 12-13).

Timori più ampi, invece, sono stati avanzati riguardo ai possibili effetti sulla democrazia. Secondo l'"effetto Streisand", casi importanti di cancellazione potrebbero alimentare sentimenti antigovernativi o pubblicizzare il materiale cancellato molto più ampiamente. È quello che è successo pochi giorni

dopo l'entrata in vigore del provvedimento. Beatrix von Storch, politica dell'Alternative für Deutschland (AfD), ha visto che uno dei suoi post è stato rimosso da Facebook e Twitter, in base alla legge. I media hanno ampiamente diffuso questo incidente, includendo il contenuto del post e la sua potenziale illegalità, mentre per l'AfD, la NetzDG ha messo a tacere delle opinioni (Leerssen e Tworek, 2019).

Si temeva anche che la legge potesse fungere da modello per regimi autoritari, così come espresso dalla GNI. Per esempio la Russia ha copiato alcune disposizioni per una legge contro il terrorismo che obbligava i *provider* a salvare per sei mesi tutte le comunicazioni (Leerssen e Tworek, 2019).

Una questione spinosa che merita un approfondimento è la compatibilità della legge in questione con i diritti umani, in primis la libertà di espressione. Bisogna precisare che, nell'ambito della tutela della libertà di espressione, secondo l'articolo 19 del Patto internazionale sui diritti civili e politici (ICCPR), rientrano le opinioni, dichiarazioni caratterizzate dalla "presa di posizione e dall'esprimersi in favore di qualcosa". Queste possono essere anche esagerate, polemiche e offensive, ma tali restano, e quindi meritano di essere tutelate. Le *fake news*, invece, non contribuendo alla formazione di un'opinione, non lo sono. Per Rinceanu "la limitazione della libertà di espressione [...] non è sufficientemente chiara né prevedibile" (Rinceanu, 2021, p. 12). I privati devono decidere se un contenuto online corrisponde a uno dei reati elencati nel primo articolo, in tempi rapidi e con il rischio di pesanti sanzioni, senza sentire l'utente o il giudice. D'altra parte, non disponendo di strumenti determinati, per loro diventa difficile capire quando una fattispecie rientra nel reato o nell'opinione. Spesso espressioni volgari sono rientrate, per poco, dentro il limite di ciò che è inteso come libertà di espressione (Rinceanu, 2021).

Inoltre, con la NetzDG, i *provider* possono "effettuare numerose incursioni nel diritto all'autodeterminazione informativa, richiedendo altresì l'archiviazione per settimane dei dati personali degli autori dei contenuti ed eventualmente anche dei denunciati e dei trasgressori". Gli utenti non

possono scegliere quali dati e contenuti, scritti o immagini, rimuovere, ma è la legge che specifica quelli che devono essere memorizzati o cancellati, per quanto tempo e come. Le vittime e i reclamanti potrebbero “rifuggire dal contatto con i social network, se non potranno più essere sicuri del fatto che i loro dati personali rimarranno tra privati e non dovranno essere immagazzinati per consentirne l’accesso allo Stato” (Rinceanu, 2021, p. 14).

Infine, è intaccata anche la libertà di professione, quindi di scelta dell’occupazione che si vuole ricoprire e di libertà di esercizio della stessa, come è propria dei fornitori di servizi informatici. Secondo la costituzione federale tedesca, questa libertà può essere limitata “in base alla legge e nel rispetto del principio di proporzionalità”, per esempio per motivi di sicurezza pubblica o per modificare la cultura del dibattito nella lotta all’*hate speech* e alle *fake news*. Perciò, l’obbligo, a carico dei fornitori, di cancellare o bloccare i contenuti manifestamente illeciti e quelli che non lo sono, interferisce con la loro libertà professionale (Rinceanu, 2021). Sempre Rinceanu si chiede se questo intervento legislativo sia allora un mezzo proporzionato al raggiungimento dei suoi scopi, “se cioè sia adeguato, necessario e proporzionato in senso stretto”. La cancellazione di contenuti illeciti “è idonea ad eliminare disturbi alla sicurezza pubblica e a modificare la cultura del dibattito per combattere i crimini d’odio e le *fake news*”, ma non è necessaria ed è sproporzionata. Infatti, vi sono altri mezzi meno duri che consentono di raggiungere l’obiettivo, come “un irrigidimento delle regole sociali della comunicazione (*policy rules*), stabilite dai provider stessi”, e provvedimenti di vigilanza, che al contempo garantiscono un margine di manovra ai *provider*, in modo che il pubblico cooperi con il privato. Per il secondo punto, in molti casi gli obblighi a breve termine conducono a rimuovere o bloccare contenuti leciti, come visto, e questo può danneggiare anche la libertà di comunicazione, tanto che è possibile dire che tali obblighi “vanno al di là di quanto è necessario al perseguimento degli obiettivi legislativi”. In più l’articolo 3 della legge, riguardante gli oneri, non distingue “in base alla gravità della lesione”, perciò non è chiaro se

dichiarazioni, lette da poche persone, debbano essere rimosse. Fatto sta che la minaccia di sanzioni legali verso i *provider*, “non solo viola la loro libertà professionale, ma li induce anche, indirettamente, a violare il diritto fondamentale alla libertà di espressione degli utenti, ossia dei loro clienti, attraverso giudizi sommari sulla liceità delle opinioni manifestate da costoro” (Rinceanu, 2021, pp. 15-16).

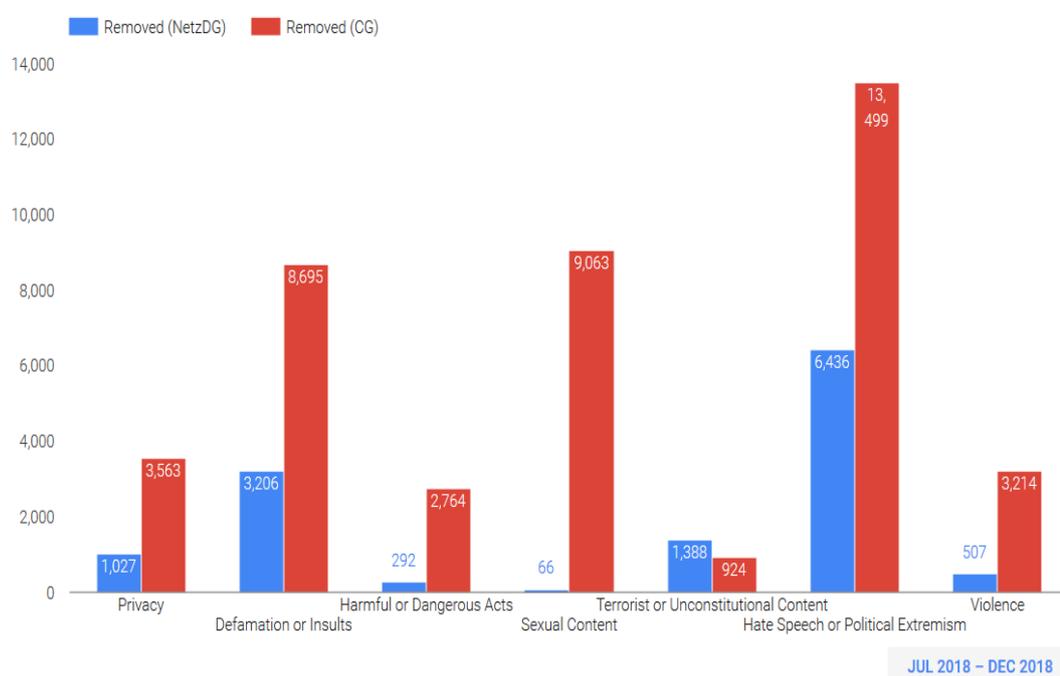
### **3.1.2 Primi risultati pratici**

Per avere una prova degli effetti di questa legge, possono essere utili i primi rapporti sulla trasparenza, pubblicati da Google (YouTube), Facebook, Twitter e Change.org.

Nel report di giugno 2018, Facebook ha ricevuto molte meno segnalazioni di YouTube e Twitter, rispettivamente 1.704 contro 241.827 e 264.818, cioè più di cento volte in meno. Questo perché era difficile accedere al modulo di reclamo di Facebook, posizionato in un'altra pagina, quindi meno visibile per gli utenti, e disponibile dopo alcuni passaggi; mentre YouTube e Twitter hanno integrato i reclami nell'interfaccia di segnalazione, accessibile tramite un collegamento diretto, posto accanto a ogni contenuto (Leerssen e Tworek, 2019).

Bisogna considerare anche che la maggior parte delle rimozioni sono avvenute in base alle linee guida (o *terms of service*), piuttosto che alla legge tedesca. Infatti, Facebook, Google e Twitter controllano prima che i reclami siano conformi alle loro linee guida, valutando se risultano violati i loro standard comunitari. Qualsiasi contenuto che non supera questo controllo, viene rimosso, mentre solo se il contenuto passa è possibile rimuoverlo ai sensi della legge NetzDG. Come mostra il rapporto sulla trasparenza di Google, la maggior parte delle decisioni di rimozione si basa sugli standard privati e non sulla legge tedesca. Allo stesso modo, Facebook e Twitter hanno esaminato i reclami dando priorità alle regole della community, pur non specificando i dati nei loro rapporti (Leerssen e Tworek, 2019). La figura 3.1 sottostante mostra, tra luglio e dicembre 2018,

la quantità di contenuti segnalati, che sono stati rimossi sia ai sensi della legge tedesca, sia secondo le linee guida (Google, 2018). Di quelli relativi alla privacy, 1.027 rimozioni sono avvenute in base alla NetzDG e 3.563 secondo le linee guida della comunità; 3.206 contenuti diffamatori o insultanti in base alla NetzDG e 8.695 secondo le linee guida; 6.436 contenuti classificati come *hate speech* o affermazioni estremiste in base alla NetzDG e ben 13.499 secondo le linee guida.



**FIGURA 3.1** Google. 2018. “Applicazione delle Norme della community e statuti NetzDG a confronto (Luglio 2018 – Dicembre 2018)”.

Come evidenzia il grafico presente nel rapporto, durante questo periodo la maggior parte degli elementi segnalati è stata rimossa in conformità alle norme della community e non in ragione del provvedimento tedesco.

I rapporti sulla trasparenza suddividono i reclami anche a seconda del tipo di contenuto. A loro volta, Facebook e Twitter suddividono i loro dati in modo diverso da Google, elencando i dati per ogni specifico reato separatamente, rispetto al primo che li aggrega per reati comparabili, come “diffamazione”

e “insulto”. Secondo i primi report, i casi di *hate speech* e diffamazione o insulto erano i più comuni. Per Google, i reclami relativi all'incitamento all'odio e all'estremismo politico erano 75.892, seguiti da diffamazione o insulto, con 45.190, e contenuti sessuali, con 27.308. Su Facebook i reati legati agli insulti predominavano, tanto da essere citati in oltre la metà di tutte le denunce; mentre su Twitter l'*hate speech* superava l'insulto, con 82.095 denunce rispetto a 75.925. Change.org ha visto pochi reclami, forse perché inizialmente la NetzDG non era nota tra gli utenti della piattaforma, fino a quando non sono comparsi articoli sulla legge da parte dei media, facendo registrare un aumento del numero dei reclami (Echikson e Knodt, 2018).

Inoltre, i rapporti delineano le procedure delle aziende per avvisare gli *uploader*, ossia chi carica i contenuti, i quali ricevono prima una conferma di ricezione del reclamo e poi un altro aggiornamento, quando viene presa una decisione sulla rimozione dei contenuti; non vengono informati quando viene ricevuto un reclamo su di loro, o quando tali reclami vengono respinti (Leerssen e Tworek, 2019).

Un punto interessante del rapporto è che Google, di fronte a richieste incomplete, per le quali servivano più informazioni da parte del richiedente, o prive di fondamento, non ha ricontattato gli utenti. Facebook e Twitter, invece, non hanno affrontato questo problema nei loro rapporti (Leerssen e Tworek, 2019).

Un mese dopo, è stato pubblicato un rapporto successivo, a fine gennaio 2019, che ha rivelato cambiamenti riguardo al volume di reclami. Le tre principali piattaforme hanno registrato diminuzioni nel numero totale di reclami ricevuti, così come i tassi di rimozione per tipo di reclamo sono calati. Il caso più significativo è stato quello di Twitter, che ha visto diminuire il numero di denunce di casi che riguardano l'*hate speech*, di oltre il 50% (Leerssen e Tworek, 2019).

Per quanto riguarda la critica all'*over-removal* (Leerssen e Tworek, 2019), sono stati aperti numerosi casi legali contro Facebook per la rimozione di contenuti, sia secondo la legge tedesca, sia in base alle sue stesse

definizioni di incitamento all'odio. Alcuni giudici hanno invocato l'articolo 5 della Costituzione tedesca, che tutela la libertà di espressione, mentre in altri casi hanno affermato il diritto di Facebook di far rispettare le sue linee guida, applicabili a tutta la community. Se da un lato Facebook ha dovuto cancellare i post, a causa del rischio di multe significative, dall'altro ha corso il pericolo di essere citato in giudizio per la cancellazione di contenuti legali. Questo sottolinea la complessità della determinazione e del trattamento dei contenuti illegali (Echikson e Knodt, 2018).

### **3.1.3 Un bilancio**

Dai primi rapporti, ma anche dai successivi, si è compreso che sono state applicate di più le linee guida della comunità, piuttosto che le disposizioni della legge (Leerssen e Tworek, 2019).

Vengono indicati i requisiti di trasparenza come un punto di partenza per consentire una ricerca più solida (Leerssen e Tworek, 2019). La trasparenza è anche l'unica parte della legge che sembra aver ricevuto un sostegno quasi universale. I futuri rapporti sulla trasparenza potrebbero contenere maggiori dettagli su come le aziende addestrano il personale addetto alla moderazione, gestiscono i meccanismi di ricorso e conducono il controllo di qualità (Leerssen e Tworek, 2019).

È stato visto che le implementazioni dei meccanismi di reclamo da parte di Google e Twitter sono state più intuitive rispetto a quelle di Facebook, come attestano i dati iniziali sulle segnalazioni (Leerssen e Tworek, 2019). Il partito dei Verdi, il progetto Counter Extremism e il Center for European Policy Studies hanno studiato nuove tecniche per rendere più visibili e facili da usare i moduli di reclamo (Leerssen e Tworek, 2019), come la modifica alla legge richiede.

Un punto che l'emendamento oggi offre, è la possibilità per gli *uploader* di ricorrere, se credono che il loro contenuto sia stato cancellato ingiustamente. Gli utenti che caricano i contenuti ora possono appellarsi alla

piattaforma per far eventualmente reintegrare i propri contenuti da un organo di controllo indipendente o da un giudice.

Tuttavia, è necessario informare gli *uploader* di possibili reclami presentati sui loro contenuti. Nessuna delle principali piattaforme si occupa di questo punto (Leerssen e Tworek, 2019).

Inoltre, ci si domanda se le parti interessate esterne possano e debbano essere coinvolte maggiormente nei processi di moderazione dei contenuti della piattaforma o nella loro regolazione. In effetti, la legge NetzDG è stata elaborata con un contributo scarso da parte delle organizzazioni della società civile. Si sostiene quindi che, per affrontare un tema che muta rapidamente, sia necessario cooperare con le società di social media, con i governi e con tali organizzazioni. La creazione di Social Media Councils, che coinvolgano piattaforme, governo e organizzazioni della società civile, può essere utile per condividere informazioni (Leerssen e Tworek, 2019).

Sul fronte penale, deve venire coinvolta anche la polizia criminale di Stato (LKA), per affrontare la criminalità informatica, in cooperazione con le aziende tecnologiche (Echikson e Knodt, 2018).

Sul fronte delle adesioni, si consiglia di includere anche altri servizi di comunicazione, come WhatsApp (Echikson e Knodt, 2018), ma anche social network meno noti, però di dimensioni importanti, come quello russo VK.

Alla fine, sembra che i sostenitori e i critici rimangano fermi nelle loro posizioni, a distanza di tempo. I primi vedono la legge come una misura vitale per tenere a freno le piattaforme e per preservare la democrazia tedesca, mentre i secondi si preoccupano delle implicazioni sulla libertà di espressione (Leerssen e Tworek, 2019) e la vedono come un tentativo di creare un nuovo regime di censura, costringendo le piattaforme a rispondere a questa nuova responsabilità con eliminazioni esagerate (Echikson e Knodt, 2018).

## Capitolo 4: I tentativi di contrasto dell'Italia

Per quanto riguarda il nostro ordinamento interno, l'Italia è stata tra i primi Stati che si è interessata al fenomeno crescente della disinformazione nella società, e in particolare alle *fake news* (Magnani, 2019).

Recentemente il rapporto Censis, uscito nell'aprile 2021, ha sottolineato come la circolazione di disinformazione e di *fake news* costituisca uno dei pericoli maggiori che si annidano nel web e che questo si sia reso ancora più visibile con la pandemia dovuta al Covid-19 (Censis, 2021).

Riguardo alle possibili soluzioni per combattere la disinformazione, l'indagine svolta da Censis mostra che la maggior parte della popolazione condivide il fatto di coinvolgere direttamente le piattaforme. Le stesse, aderenti al Codice europeo di cui al secondo capitolo, hanno adottato misure per declassare contenuti falsi o sensibili per la salute (Censis, 2021), come è stato visto (Corte dei Conti UE, 2021). In particolare:

- il 56,2% ritiene di dover prevedere delle pene più severe per chi diffonde notizie false;
- il 52,2% opta per l'obbligo di rimozione delle *fake news* da parte delle piattaforme;
- il 41,5% è convinto che debbano essere attivati sistemi di *fact-checking* nei social media;
- il 34,7%, perlopiù giovani tra i 18 e i 34 anni (41,6%), punta sulle campagne di sensibilizzazione riguardo un uso corretto dei social network;
- il 17,5% pone l'attenzione sui motori di ricerca, che dovrebbero riservare una posizione privilegiata ai contenuti istituzionali e di qualità;
- il 16,2% vorrebbe istituire riconoscimenti e premi per quelle piattaforme che si siano contraddistinte per l'informazione di qualità (Censis, 2021).

Nel proseguire il discorso e creando una sorta di aggancio con il primo punto, si andranno a vedere due disegni di legge che sono stati presentati

per debellare le *fake news*, il primo da parte della senatrice Gambaro e il secondo dai senatori Zanda e Filippin. Si cercherà di capire cosa prevedevano e perché sono stati criticati.

Dopo aver analizzato i tentativi del legislatore, si passerà ad altri soggetti istituzionali che si sono occupati da vicino dei fenomeni distorsivi dell'informazione, il più importante dei quali pare essere, ancora oggi, l'Autorità per le Garanzie nelle Comunicazioni (AGCOM).

#### **4.1 I disegni di legge Gambaro e Zanda-Filippin**

Un dibattito serio è stato avviato anche in Italia, visto il ruolo crescente che i movimenti populistici hanno assunto negli ultimi anni e l'impiego massiccio di *fake news* in ambito politico, che influenzano quotidianamente l'opinione pubblica. Seguendo le reazioni della Germania e della Francia, è emersa l'esigenza di intervenire a livello normativo per controllare i contenuti diffusi in rete, eventualmente rimuovendoli.

Ricalcando gli indirizzi dell'Assemblea parlamentare del Consiglio d'Europa, espressi nella risoluzione n. 2143 del 25 gennaio 2017, intitolata "I media *online* e il giornalismo: sfide e responsabilità", è stato presentato il disegno di legge (ddl) n. 2688, contenente le "Disposizioni per prevenire la manipolazione dell'informazione *online*, garantire la trasparenza sul *web* e incentivare l'alfabetizzazione mediatica", noto come ddl Gambaro, dal cognome della senatrice Adele che aveva avviato l'iniziativa parlamentare il 7 febbraio 2017, insieme ad altri senatori (Senato, 2017a). Con il termine della legislatura, il ddl è stato poi lasciato da parte. Nonostante ciò, sarà utile analizzare questa proposta.

L'articolo 1 del ddl, al comma 1, prevedeva l'aggiunta di una nuova contravvenzione nell'articolo 656 del codice penale:

“chiunque pubblici o diffonda notizie false, esagerate o tendenziose che riguardino dati o fatti manifestamente infondati o non veritieri, attraverso *social media* o altri siti che non siano espressione di giornalismo *online*, è punito, se il fatto non

costituisce un più grave reato, con l'ammenda fino a euro 5.000"  
(Senato, 2017a, p. 8).

In caso di diffamazione, al comma 2, era prevista la possibilità, per la persona offesa, di ottenere una somma a titolo di riparazione, oltre al risarcimento dei danni (Senato, 2017a).

Al fine di distinguere l'attività giornalistica professionistica da quella che non lo era, erano escluse dalla prima disposizione le testate giornalistiche.

L'articolo 2 introduceva due nuovi delitti che ampliavano l'articolo 265 del codice penale, rispettivamente sarebbero nati il 265-*bis* e il 265-*ter*.

Con il primo:

“chiunque diffonde o comunica voci o notizie false, esagerate o tendenziose, che possono destare pubblico allarme, o svolge comunque un'attività tale da recare nocimento agli interessi pubblici o da fuorviare settori dell'opinione pubblica, anche attraverso campagne con l'utilizzo di piattaforme informatiche destinate alla diffusione *online*, è punito con la reclusione non inferiore a dodici mesi e con l'ammenda fino a euro 5.000”  
(Senato, 2017a, p. 9).

Mentre con il secondo:

“Ai fini della tutela del singolo e della collettività, chiunque si rende responsabile, anche con l'utilizzo di piattaforme informatiche destinate alla diffusione *online*, di campagne d'odio contro individui o di campagne volte a minare il processo democratico, anche a fini politici, è punito con la reclusione non inferiore a due anni e con l'ammenda fino a euro 10.000”  
(Senato, 2017a, p. 9).

Al fine di contrastare l'anonimato e di garantire maggiore trasparenza, l'articolo 3 disponeva che, all'apertura di un sito web o di una piattaforma elettronica destinata alla diffusione online di informazioni presso il pubblico, l'amministratore dovesse fornire, tramite posta elettronica certificata, l'URL

(Uniform Resource Locator) del sito, il proprio nome e cognome, il domicilio, il codice fiscale e l'indirizzo di posta elettronica certificata, al tribunale territorialmente competente (Senato, 2017a).

L'articolo 4 riconosceva la possibilità di rettificare un'informazione errata, in tempi brevi, mentre l'articolo 5 di chiedere la rimozione, dal web, di contenuti diffamatori o di dati personali, lesivi dell'onore o della reputazione di un soggetto, che violavano la normativa vigente, con la possibilità di rivolgersi anche al giudice (Senato, 2017a).

Il ddl non si limitava ad aggiungere delle pene o ad assicurare più trasparenza, piuttosto che la rettifica di informazioni sbagliate. All'articolo 6, esortava anche a promuovere l'impegno per l'alfabetizzazione mediatica, modificando la legge n. 107 del 2015 (c.d. "Buona scuola"), e a sostenere progetti di sensibilizzazione nelle scuole secondarie di primo e di secondo grado e programmi di formazione, rivolti agli studenti interessati alla professione di giornalista, anche attraverso stage presso testate online. All'articolo 8, invece, si raccomandava maggiore attenzione da parte dei media delle emittenti radiotelevisive pubbliche rispetto ai contenuti generati dagli utenti o da terzi (Senato, 2017a).

Ma soprattutto, con l'articolo 7, i gestori dei siti sarebbero stati tenuti a monitorare costantemente quanto diffuso sulle proprie piattaforme, compresi i commenti degli utenti, come in Germania. In caso di diffusione di notizie non attendibili o veritiere, anche segnalate dagli utenti, avrebbero dovuto rimuoverle, altrimenti sarebbero stati soggetti alla sanzione di cui all'articolo 656-*bis* (Senato, 2017a).

Tuttavia, alcuni studiosi hanno ravvisato diverse criticità nella proposta (Bassini e Vigevani, 2017; Candido, 2020; Cuniberti, 2017; Donati, 2018; Magnani, 2019).

Intanto, secondo Cuniberti, il monitoraggio che veniva richiesto, avvalendosi di strumenti informatici o delle segnalazioni degli utenti, poteva non essere efficace e portare perfino all'eliminazione di contenuti inoffensivi (Cuniberti, 2017).

Inoltre, colpiva l'idea di sanzionare la falsità della notizia in sé, dato che "l'affermazione di un fatto falso in sé non può essere considerato reato" (Candido, 2020, p. 116) e che "non comporta normalmente né responsabilità civile né sanzioni penali", secondo l'articolo 21 della Costituzione, a meno che non sia "preordinata o idonea ad arrecare un danno ingiusto o un ingiusto svantaggio ad altri" (Cuniberti, 2017, p. 5). Anche Bassini e Vigevani si discostano da una "concezione del falso come elemento in sé illecito e generativo di responsabilità in capo a chi lo dissemini", che il ddl pareva avere (Bassini e Vigevani, 2017, p. 15).

In aggiunta, si tenga conto che non si doveva applicare a chi esercitava professionalmente l'attività giornalistica, con il paradosso che il giornalista avrebbe potuto godere di un trattamento favorevole riguardo al proprio operato (Cuniberti, 2017).

Sotto il profilo tecnico, la proposta sembrava formulata male. Alcune disposizioni sono state ritenute vaghe e indeterminate, come "nocumento agli interessi pubblici" o "minare il processo democratico, anche a fini politici" (Senato, 2017a, p. 9), mentre gli obblighi di comunicazione e rettifica, seppur apprezzabili, sono stati considerati inutili, dato che ci si chiedeva perché i primi avrebbero dovuto avere come destinatario il tribunale, di cui non si sapeva se e come avrebbe verificato l'autenticità delle informazioni fornitegli (Cuniberti, 2017). Non è stato poi condiviso il richiamo alla sentenza della Cassazione del 1956, che prevede il dovere del cittadino di non procurare pubblico allarme, ma anche "di non denigrare all'estero la propria patria con notizie false, esagerate e tendenziose sulle condizioni interne". Ciò è stato visto come un modo per giustificare una limitazione della libertà di manifestazione del pensiero (Cuniberti, 2017, p. 6).

Se fosse stata approvata, avrebbe introdotto "una surrettizia forma di censura" (Donati, 2018, p. 443), gestita non dal pubblico, ma da privati (Magnani, 2019), di conseguenza portando a una limitazione della libertà di espressione dell'individuo.

Tra l'altro, il ddl appariva in contrasto con la direttiva 31/2000 della Comunità europea (CE), secondo cui gli Stati membri non possono obbligare un *hosting provider* a sorvegliare sulle informazioni che memorizza (Candido, 2020).

I gestori dei siti Internet in questo caso sarebbero stati ritenuti responsabili. Diverso è quando le piattaforme vengono assoggettate all'obbligo, previsto dagli Stati membri, di informare le autorità giudiziarie di eventuali illeciti di cui siano a conoscenza (Magnani, 2019) e, su loro richiesta, di rimuoverli immediatamente (Donati, 2018).

Qualche mese più tardi, il 14 dicembre 2017, è stato presentato, ma non depositato, un altro ddl, su iniziativa dei senatori Luigi Zanda e Rosanna Filippin, appartenenti al Partito Democratico, dal titolo "Norme generali in materia di *social network* e per il contrasto della diffusione su *internet* di contenuti illeciti e delle *fake news*" (Senato, 2017c), abbreviato ddl Zanda-Filippin.

Fortemente ispirato alla legge NetzDG, come dichiarato nel testo stesso (Senato, 2017c), esso mirava a limitare fortemente la pubblicazione e la circolazione di *fake news* nei social network. Come per la legge tedesca, l'obiettivo era quello di responsabilizzare i social network, con più di un milione di utenti registrati sul territorio nazionale. Secondo Monti, applicare la disciplina solo a quelli con un numero elevato, ignorando tutti quelli inferiori a questa cifra, avrebbe escluso molte persone, lasciandole esposte alla disinformazione (Monti, 2017b). Si ricordi che erano escluse le piattaforme che offrivano contenuti giornalistici o editoriali e quelle per comunicare tra individui (Senato, 2017c), come WhatsApp.

Gli obblighi a loro carico erano di:

- predisporre una procedura trasparente ed efficace per la ricezione e la gestione dei reclami relativi a contenuti illeciti;
- rimuovere o bloccare tali contenuti entro un tempo definito;
- pubblicare ogni sei mesi, sulla Gazzetta Ufficiale e sul sito web, un rapporto dettagliato sulla gestione dei reclami, per coloro che ne avessero ricevuti più di 100 all'anno (Senato, 2017c).

Diversamente dal ddl Gambaro, non veniva introdotto un reato come il 656-*bis*. Venivano distinti i contenuti illeciti in due categorie, delitti contro la persona e delitti contro la Repubblica. Secondo il testo, nella prima rientravano per esempio la diffamazione, la minaccia e lo stalking; nella seconda, solo per citarne alcuni, l'associazione a delinquere, la propaganda all'odio e una serie di reati terroristici (Senato, 2017c). Alcuni sono stati considerati non legati alle *fake news*, come la pornografia minorile all'interno del primo gruppo (Monti, 2017b).

“Aggiungere un'ulteriore fattispecie criminosa relativa alla diffusione di false notizie online o estendere i meccanismi correttivi delle false notizie ai media della rete” sarebbe stata probabilmente la soluzione migliore (Monti, 2017b, p. 3).

Anche la procedura e le sanzioni erano delineate secondo l'impostazione della legge tedesca, quindi erano previsti termini di rimozione una volta ricevuta la denuncia (24 ore o 7 giorni), organismi di autoregolamentazione, un periodo di tempo di conservazione dei contenuti rimossi (10 settimane) e somme pecuniarie (da 500.000 fino a 5 milioni). I gestori avrebbero dovuto controllare mensilmente i reclami, risolvere carenze organizzative e organizzare corsi di formazione al personale che si occupava dei reclami (Senato, 2017c).

Le due categorie di contenuti avevano poi una procedura specifica. Per quelli legati ai delitti contro la persona, la risposta alla richiesta di rimozione sarebbe dovuta avvenire entro 24 ore in caso di contenuti manifestamente illeciti o entro 7 giorni se fosse stato necessario accertare la veridicità del contenuto. Per i delitti contro la Repubblica, il Pubblico Ministero avrebbe ordinato ai social network la rimozione entro 48 ore (Senato, 2017c).

Sempre secondo Monti, i social network avrebbero così assunto un ruolo editoriale nella valutazione della verità e, per non incorrere nelle ingenti sanzioni, avrebbero semplicemente rimosso ogni contenuto segnalato, e così sarebbero andati a ledere la libertà di espressione. Per questo sarebbe stato preferibile inserire la possibilità di rettifica, prevista invece nel ddl

Gambaro, per avvisare e informare correttamente gli utenti che sono stati oggetto di disinformazione (Monti, 2017b).

Inoltre, organismi indipendenti di autoregolamentazione, riconosciuti dal Ministro dello sviluppo economico, di concerto con il Ministro della giustizia e sentito il Garante per la protezione dei dati personali, avrebbero potuto analizzare i contenuti, segnalati da utenti non lesi direttamente dai contenuti illeciti (Senato, 2017c). È anche vero che il fatto che lo Stato riconoscesse questi soggetti sulla base dell'indipendenza e della competenza, nascondeva una fiducia del legislatore verso i social network, considerati più indipendenti e competenti (Monti, 2017b).

Seppur l'idea legittima fosse quella di tutelare il discorso pubblico, il ddl non prendeva in considerazione "la distorsione, ben più rilevante, del paradigma della stampa e della libertà di informazione" (Monti, 2017b, p. 2).

#### **4.2 Il ruolo dell'AGCOM**

Oltre al legislatore, un altro soggetto istituzionale che avuto un ruolo fondamentale nell'analisi e nel monitoraggio dell'informazione online e che si è occupato da vicino del problema delle *fake news*, e della disinformazione in generale, è stata l'AGCOM.

Nel 2013 ha creato un Osservatorio sulle comunicazioni, uno sul giornalismo e un altro sulle testate online (Magnani, 2019). Negli ultimi anni ha avviato discussioni, convegni e ricerche, collaborando con il mondo accademico e scientifico. Allo scopo di promuovere l'autoregolamentazione delle piattaforme, a novembre 2017 è stato creato il "Tavolo tecnico per la garanzia del pluralismo e della correttezza dell'informazione sulle piattaforme digitali" (AGCOM, 2018). È stata un'occasione per le piattaforme (Google, Facebook, Wikipedia), gli editori di quotidiani e televisioni, i giornalisti, le compagnie pubblicitarie, le associazioni di categoria e le istituzioni accademiche, per condividere informazioni e scambiarsi buone prassi (AGCOM, 2018). Oltre alla funzione istituzionale,

l'Autorità ha un ruolo di coordinamento tra i diversi *stakeholder*, anche se non esplicitamente prevista (Magnani, 2019).

Da un punto di vista operativo, nel Tavolo sono stati creati cinque gruppi di lavoro, ognuno con un compito specifico: monitoraggio dei fenomeni di disinformazione e *hate speech*; controllo del sistema della pubblicità online; *fact-checking*; media e *digital literacy*; informazione dei cittadini sulla disinformazione. Si è giunti alla conclusione che la disinformazione si diffonde “dove il sistema dell'informazione fallisce”, dove si cerca di monetizzare, attraverso il *clickbaiting*, e dove non s'investe in informazioni di qualità e in sistemi di verifica (Panza e Sciacchitano, 2020, p. 125).

Il 2016 è stato identificato come l'anno in cui si è propagato l'allarme verso il fenomeno delle *fake news*, però è stato riconosciuto che l'impiego di questa nozione è stato troppo ampio, portando l'AGCOM a focalizzarsi sulla disinformazione, dove “sembrano più forti i pericoli per l'informazione” (Magnani, 2019, p. 24).

L'Autorità svolge regolarmente specifiche analisi e indagini conoscitive che confluiscono poi in rapporti. Ne è un esempio il report “News vs. fake nel sistema dell'informazione” (AGCOM, 2018). L'indagine ha considerato circa 35 milioni di documenti, prodotti in più di due anni (da aprile 2016 ad agosto 2018), da circa 1800 fonti informative, tra cui canali televisivi e radiofonici, quotidiani, testate online e relative pagine social, analizzando circa 700 notizie, reali e false, nell'arco di un anno.

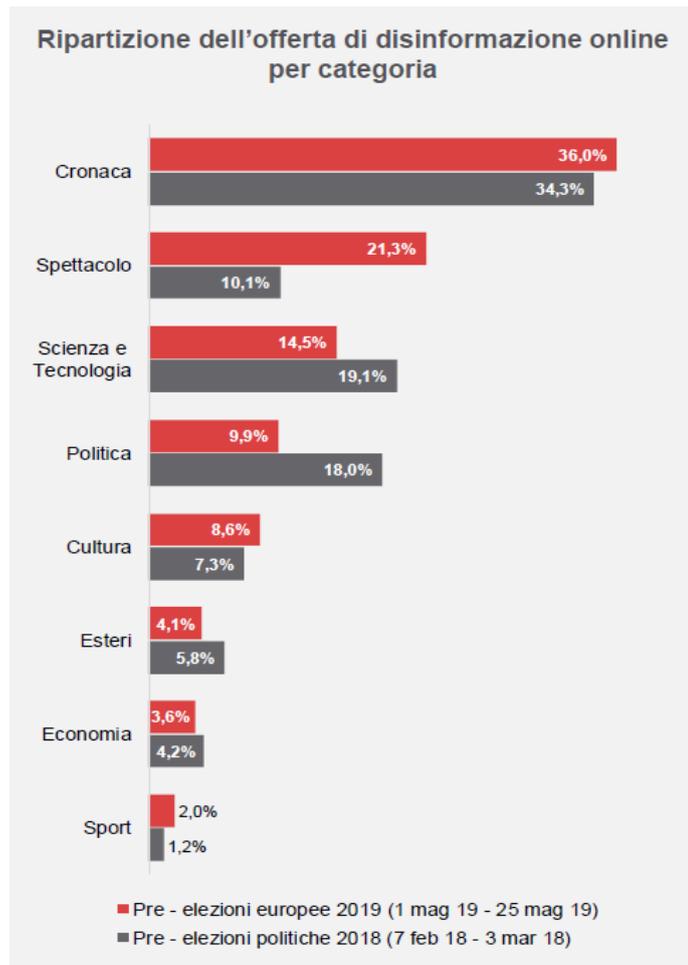
In primo luogo è interessante quello che è emerso se si associa il fenomeno della disinformazione a due variabili: la stagionalità e il ciclo politico. La produzione di *fake news*, e di notizie in generale, risultava diminuita in estate rispetto alle altre stagioni, mentre durante la campagna elettorale e le elezioni politiche del 4 marzo 2018 è stato rilevato un aumento del tasso di informazioni prodotte, ma soprattutto ha colpito la loro rapidità di diffusione attraverso le condivisioni degli utenti e la breve durata di vita di una *fake news* rispetto a una notizia reale. È risultato che in Italia politica e cronaca sono stati tra gli argomenti più bersagliati da *fake news*, per il 57%, seguiti da quelli di carattere scientifico, per il 20%, oltre a diritti umani,

economia, salute, ambiente, famiglia, fede, esteri, scienza e immigrazione. Tutti argomenti che possono suscitare un impatto emotivo e provocare reazioni, anche divisive (AGCOM, 2018).

I documenti dell'AGCOM risultano ancora più utili quando si traggono informazioni riguardo a certe tendenze. In generale, ci sono stati molti meno contenuti disinformativi nei 25 giorni precedenti le elezioni europee del 2019 rispetto al periodo delle elezioni politiche del 2018, come mette in luce l'Osservatorio, che ha analizzato oltre 7 milioni di documenti generati in Italia (nei primi cinque mesi del 2019 e nel mese antecedente alle elezioni politiche del 2018) da più di 2.000 fonti informative (AGCOM, 2019).

Entrando più nel dettaglio e osservando la figura 4.1 sottostante, "cronaca" risulta la categoria prevalente degli articoli di disinformazione, per il 36%, poco sopra al periodo pre-elettorale del 2018, del 34%. Gli articoli dedicati allo spettacolo sono aumentati dal 10,1% al 21,3%. È anche vero che vi è stata una riduzione per la "politica", che passa dal 18% del periodo pre-elettorale del 2018 al 9,9% nel periodo precedente alle elezioni europee del 26 maggio 2019, e per "scienza e tecnologia", dal 19,1% al 14,5%. Nel mese delle elezioni europee è poi cresciuto lo spazio dedicato dalle fonti di disinformazione a temi rilevanti a livello europeo, come la criminalità, la disoccupazione e l'immigrazione (AGCOM, 2019).

Nel mese di maggio 2019, tra i trenta termini più frequenti nei siti di disinformazione, vi sono per esempio "Salvini", "immigrati", "clandestini", "porti", per la tematica "immigrazione"; "maggio", "temporali", "tempo", "piogge", per il "meteo"; "casa", "fratello", "puntata", "uomini", per lo "spettacolo"; "euro", "governo", "caso", "Lega", per la "politica"; "vita", "fatto", "mondo", "polizia", per la "cronaca nera" (AGCOM, 2019).



**FIGURA 4.1.** AGCOM. 2019. “Ripartizione dell’offerta di disinformazione online per categoria”, p. 4.

Come precisato nel Tavolo, tra le misure di contrasto, l’AGCOM consiglia azioni coordinate tra i diversi soggetti operanti nel mercato dell’informazione online, non escludendo una possibile coesistenza di interventi di autoregolamentazione e di regolazione, o una loro complementarietà. Oltre a promuovere continuamente approfondimenti di un tema complesso come quello della disinformazione, attraverso indagini e report, a incentivare la *media literacy* e il *fact-checking*, un percorso condiviso tra i vari attori pare essere una strada da intraprendere (Magnani, 2019).

### 4.3 Altre iniziative

Anche la Polizia postale italiana ha cercato di limitare la diffusione di notizie false, ingiuriose o diffamatorie. Con il comunicato stampa del 18 gennaio 2018 iniziava il progetto “*Red Button*”, un servizio collocato all’interno del sito del Commissariato di Polizia, grazie al quale l’utente poteva segnalare possibili *fake news* alla Polizia, cliccando sul bottone e inserendo tutte le informazioni nella pagina che si apriva. Dopo opportune verifiche da parte di un team di esperti, appartenenti al Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (Cnaipic), che si serviva di software di analisi (Polizia di Stato, 2018), essa avrebbe poi smentito nel proprio sito web e nei propri canali social istituzionali le notizie *fake*, oscurandole per sempre dalla piattaforma online e “inviando gli atti all’autorità giudiziaria, nel caso in cui vi fossero stati aspetti di rilevanza penale” (Candido, 2020, p. 118).

Tuttavia, sono state avanzate molte critiche riguardo a questa iniziativa.

Innanzitutto, il servizio rispondeva alla crescente sensibilità manifestata a livello europeo dalla Commissione, prima con il lancio di una consultazione pubblica (Commissione, 2018e) e poi con la creazione dell’HLEG (Commissione Europea, 2018a), e in occasione della campagna elettorale per le elezioni politiche del 2018.

In un’intervista, il noto giurista Pizzetti l’ha definita come un’iniziativa “priva di base normativa”, “presentata come legittima” per difendere la libertà di informazione durante le elezioni, ricordando che in Italia essa “non è sottoposta a autorizzazioni o censure”, se non “su atto della autorità giudiziaria o per intervento di un ufficiale di polizia giudiziaria, e solo nei casi previsti dalla legge sulla stampa” (Pizzetti, 2018).

In aggiunta, il relatore speciale dell’ONU David Kaye, in un comunicato del 20 marzo 2018<sup>12</sup>, ha affermato che le restrizioni sulle notizie false sembravano essere incoerenti con i criteri di legalità, proporzionalità e necessità, previsti dalla Convenzione internazionale sui diritti civili e politici

---

<sup>12</sup> Kaye David. 2018. Ultimo accesso 20 gennaio 2022.  
<https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-ITA-1-2018.pdf>.

(ICCPR, articolo 19, paragrafo 3), secondo cui è tutelata la diffusione di idee attraverso i media.

Una delle maggiori preoccupazioni riguardava l'ampia discrezionalità che il potere politico avrebbe avuto nel reprimere dichiarazioni critiche nei confronti di personalità pubbliche, oltre alla vaghezza dei termini oggetto di contrasto.

Inoltre, la scarsa chiarezza del protocollo attuativo e la minaccia di sanzioni avrebbero creato un sistema in cui sarebbero state eliminate quelle che possono essere delle critiche al governo e le opinioni impopolari, controverse o di minoranza, tipiche di una società democratica, in una sorta di censura della libertà di espressione da parte dell'autorità pubblica. Per questo Kaye ha suggerito al governo altre misure, come la promozione di controlli indipendenti di *fact-checking*, la formazione nelle scuole e l'alfabetizzazione dei media.

Alla fine, non ci sono stati risultati di questo progetto, che, infatti, si è arenato, con la pagina che attualmente non funziona più.

Di recente, il 4 aprile 2020, in risposta all'esplosione di *fake news* riguardanti il coronavirus, è stata istituita, con decreto del Sottosegretario alla Presidenza del Consiglio dei Ministri, un'"Unità di monitoraggio per il contrasto della diffusione di fake news relative al COVID-19 sul web e sui social network", composta da tre rappresentanti, uno della Presidenza del Consiglio, un altro del Ministero della Salute e un terzo del Dipartimento della Protezione Civile, che si aggiungevano a un gruppo di otto esperti già nominati dal Governo, e dall'AGCOM (Candido, 2020).

L'Unità aveva i compiti di:

- classificare i contenuti falsi, non dimostrati, relativi al Covid-19, soprattutto riguardanti le misure di contenimento del contagio;
- promuovere campagne di comunicazione, coinvolgendo il Ministero della Salute e il Dipartimento della Protezione Civile;
- rendere visibile le informazioni provenienti da fonti istituzionali, posizionandole meglio nei motori di ricerca e nei social media;

- stringere accordi con agenzie di *fact-checking* e con i principali motori di ricerca e con le piattaforme;
- coinvolgere cittadini e utenti dei social nell'individuazione di contenuti non veritieri relativi al Covid-19, i quali sarebbero stati segnalati alla stessa Unità di monitoraggio, (Candido, 2020).

La *task force* governativa, seguendo le iniziative della Commissione europea, dell'Organizzazione Mondiale della Sanità e del Ministero della Salute, si poneva l'obiettivo di evitare che le falsità durante la pandemia andassero in qualche modo a indebolire le misure di contenimento del contagio. È stato però anche osservato che, in un momento di forti restrizioni alle libertà costituzionali dovute all'emergenza sanitaria, la scelta di disciplinare gli strumenti di contrasto attraverso un atto amministrativo mal si conciliava con il principio della libertà di informazione, soprattutto perché la limitazione di questo diritto avveniva con un atto normativo secondario (Candido, 2020).

## Conclusioni

Ripercorrendo il percorso intrapreso, nel primo capitolo si è inquadrato il fenomeno delle *fake news*. Oltre ad averne fornito una definizione, connessa strettamente alla rete, per completezza sono stati chiariti anche altri termini, come “*post-truth*”, “*hate speech*” e “disinformazione”. Quest’ultima è stata classificata in sette tipi, tra i quali rientrano anche le *fake news*, come mostra la figura 1.1 (Wardle, 2017).

Si è poi passati alla loro diffusione nei *social network* e si è capito che la facilità di utilizzo di questi dispositivi permette a chiunque di poter creare notizie false, per i motivi più disparati: pubblicità, profitto, propaganda politica, concorrenza commerciale, provocazione, parodia, convinzioni ideologiche (negazionismo) e di salute, come è accaduto con il Covid-19. Algoritmi, distorsioni cognitive (*bias*), condivisioni, *bot*, insieme a un ridotto livello di attenzione che si presta alle notizie al giorno d’oggi (Croce e Piazza, 2019), a una quantità enorme delle stesse e al venir meno dell’autorevolezza di chi scrive (Suffia e Ziccardi, 2020), permettono alle *fake news* di attecchire. Ciò può portare alla creazione di *echo chamber* chiuse, che polarizzano il dibattito e che possono confondere ciò che c’è di vero intorno a una notizia con quello che in realtà è falso (Croce e Piazza, 2019). Tutto questo a scapito di una corretta informazione e di una formazione libera dei cittadini circa determinati interessi.

Nel secondo capitolo si è intravista qualche misura di autoregolamentazione adottata dalle piattaforme. Facebook, Twitter e Google hanno inserito meccanismi di segnalazione dei contenuti che violano le proprie linee guida e promosso il *fact-checking* da parte di organizzazioni indipendenti. Il fatto che tutti e tre releghino, in modo da rendere meno visibili, gli articoli disinformativi o alterati, e informino, attraverso feedback e segnalazioni, gli utenti, sono segnali positivi. Tuttavia, nell’elaborato non si è indagato sull’effettiva utilità di questi strumenti, attraverso qualche dato quantitativo. In futuro sarà opportuno farlo.

Successivamente si è visto che l’Unione Europea, in particolare la Commissione, si può annoverare tra i soggetti che si sono occupati in prima

linea della conoscenza della disinformazione. Dopo la consultazione pubblica e l'indagine Eurobarometro, è stato redatto un Codice di buone pratiche da seguire, al fine di responsabilizzare le piattaforme riguardo alla disinformazione. Secondo Monti, esso ha il merito di chiarire che cos'è una *fake news* e, in quanto atto di *soft law*, è abbastanza flessibile, lasciando ai privati un certo margine d'implementazione delle disposizioni (Monti, 2019). L'ERGA, nel suo rapporto, ha però lamentato una bassa adesione, che raccomanda di aumentare, includendo anche WhatsApp (ERGA, 2020). Un altro punto debole è la libertà, da un momento all'altro, di venir meno agli impegni assunti (Monti, 2019). Per Pagano, gli impegni non sono nemmeno chiari e misurabili e il Codice ha più una natura mista pubblico-privata, che riconosce un ruolo di supervisione e monitoraggio alla Commissione (Pagano, 2019), una sorta di istituzione terza che controlla una regolazione tra privati, soluzione che auspicava Pitruzzella (Pitruzzella, 2018).

Il "Piano d'azione contro la disinformazione" è stato ritenuto pertinente, coinvolgente, ma poco monitorato, con relazioni sulla sua attuazione piuttosto carenti. Al suo interno, il "Sistema di Allerta Rapido" non ha emesso segnalazioni, mentre il Codice sembra aver smosso le piattaforme intorno al tema della disinformazione, come testimoniano i dati rilevati dalla Corte dei Conti in uno dei suoi ultimi documenti, ma, tra i punti di debolezza, le misure sono sembrate troppo generiche (Corte dei Conti UE, 2021). Le relazioni sull'attuazione del Piano potrebbero fornire qualche informazione aggiuntiva su come viene attuato il Codice, che vede ancora poca partecipazione e nessuna sanzione in caso di uscita.

Nel terzo capitolo è stata analizzata la legge tedesca NetzDG, che ha rappresentato un primo esempio, in Europa, di regolazione ad hoc intorno a questo fenomeno. Ha ricevuto critiche riguardo all'incompatibilità con la libertà di espressione, dato che sarebbero state censurate molte opinioni, viste anche le ingenti sanzioni. I primi rapporti sulla trasparenza hanno mostrato che sono state applicate di più le linee guida delle piattaforme piuttosto che le disposizioni della legge NetzDG, come evidenzia la figura 3.1 nel caso di Google (Youtube), che, insieme a Twitter, ha ricevuto più

reclami di Facebook (Leerssen e Tworek, 2019). Viene fatto sapere che un successivo rapporto ha registrato diminuzioni nel numero totale di reclami ricevuti, così come sono calate le rimozioni per tipo di reclamo (Leerssen e Tworek, 2019). I meccanismi di reclamo da parte di Google e Twitter sono stati ritenuti più intuitivi e semplici rispetto a quelli di Facebook. La possibilità di ricorrere in caso di cancellazioni ingiuste, a un organo indipendente o a un giudice, è una facoltà che inizialmente il provvedimento non prevedeva e che è stata inserita successivamente con un emendamento. È necessario però che gli autori dei contenuti vengano informati di possibili reclami presentati nei loro confronti da altri soggetti (Leerssen e Tworek, 2019). Come nel caso del Codice dell'UE, si consiglia di includere anche altri servizi di comunicazione, come WhatsApp (Echikson e Knodt, 2018).

In generale, la legge da alcuni è stata vista come una misura essenziale per responsabilizzare le piattaforme sulla disinformazione che circola in rete, mentre da altri è stata espressa preoccupazione per la censura a cui sono costrette le piattaforme attraverso eliminazioni forzate, che vanno a colpire la libertà di espressione (Echikson e Knodt, 2018).

Nel quarto capitolo i due ddl italiani sono parsi come dei tentativi per provare ad arginare la disinformazione. Fatto sta che poi si sono arenati. Il primo aggiungeva delle pene, promuoveva l'alfabetizzazione mediatica e progetti di sensibilizzazione nelle scuole. Ma, all'articolo 7, le piattaforme avrebbero dovuto rimuovere le notizie non attendibili o distorte, altrimenti sarebbero state soggette a sanzioni. È stata criticata la rimozione eccessiva che anche in questo caso ci sarebbe stata, la vaghezza delle disposizioni, il non rispetto dell'articolo 21 della Costituzione (Cuniberti, 2017) e il contrasto con la direttiva 31/2000 della CE riguardo agli obblighi di controllo delle piattaforme sulle informazioni memorizzate (Candido, 2020).

Il secondo ddl, ispirato alla legge tedesca NetzDG per quanto riguarda gli obblighi, le procedure e le sanzioni, seppur inferiori, mirava a responsabilizzare i social network, però solamente quelli con più di un milione di utenti registrati in Italia. Erano escluse poi le piattaforme che offrivano contenuti giornalistici o editoriali e, anche in questo caso,

WhatsApp. Non veniva aggiunta una fattispecie criminosa relativa alla diffusione di notizie false e, come per la NetzDG, vi sarebbero state sanzioni elevate, che avrebbero portato a un *over-removal*, e quindi a una lesione della libertà di espressione (Monti, 2017b).

In Italia, tra gli altri soggetti citati, sembra che il ruolo più rilevante lo abbia esercitato l'AGCOM, attraverso specifiche analisi, indagini conoscitive e conseguenti report, come quello "News vs. fake nel sistema dell'informazione", che ha sottolineato alcune tendenze, come il fatto che la produzione di *fake news* risultava diminuita in estate rispetto alle altre stagioni o aumentata durante la campagna elettorale del 2018 (AGCOM, 2018). Politica, cronaca e scienza sono stati rilevati tra gli argomenti preferiti dai creatori di *fake news* (AGCOM, 2019).

Anche l'Autorità incentiva la media *literacy* e il *fact-checking*, consigliando un coordinamento di azioni tra giornalisti, piattaforme, governo e scuole (AGCOM, 2019).

La Polizia Postale, invece, con il progetto *Red Button* ha prodotto poco nulla. Infatti, oltre a poche segnalazioni, non ci sono stati risultati significativi e la pagina è stata poi chiusa.

In conclusione, per combattere la disinformazione sarà necessaria un'indagine continua, visto il suo carattere mutevole nel tempo e viste le varie sfaccettature che può assumere, ormai non prescindendo dall'analisi del funzionamento dei social network, degli algoritmi, della tecnologia e dei meccanismi psicologici che sottendono la sua diffusione.

Complessivamente, bisognerà investire nella qualità delle fonti informative, sia online sia offline, e nella trasparenza degli algoritmi delle piattaforme.

Ma soprattutto la sfida maggiore sarà quella culturale, riguardante la preparazione e la consapevolezza dell'utente, in modo che sia in grado di verificare l'attendibilità di una notizia (Cuniberti, 2017), incrociando le fonti, e che nutra uno spirito critico. Canali YouTube, gruppi Telegram e WhatsApp e siti di *fact-checking* istituzionali, creati per segnalare le *fake news*, potrebbero risultare utili. Oltre ai meccanismi di segnalazione, le testate online potrebbero dedicare pagine o sezioni apposite in cui relegare tutti gli

articoli che sono stati analizzati e reputati, da esperti di *fact-checking*, come disinformativi, spiegando brevemente perché non sono attendibili, sia sotto il punto di vista contenutistico sia formale, rispondendo alle eventuali perplessità degli utenti.

Si può dire che gli interventi intravisti, più o meno efficaci che siano, segnalano sicuramente un'attenzione maggiore intorno alle *fake news*, e in generale alla disinformazione, che rappresenta un tema molto complesso da arginare.

Appare condivisibile l'idea dell'AGCOM di prevedere una coesistenza di interventi di autoregolamentazione e di regolazione, o anche una loro complementarietà (AGCOM, 2019), in modo che la responsabilizzazione delle piattaforme private non significhi censura e che ci sia un controllo pubblico su come operino.

Si è quindi compreso che, nel caso di futuri interventi normativi, si cercherà, seppur non facilmente, di contemperare le esigenze di rimozione di notizie false o fuorvianti con quelle dei diritti fondamentali online, come la libertà di manifestazione del pensiero e di libera formazione delle opinioni.

## Bibliografia

Ascione Guido, Lopalco Pierluigi, Pavesio Diego. 2020. "Il Patto Trasversale per la Scienza e la lotta alle pseudoscienze". *federalismi.it* (11): 196-204.

Bassini Marco, Vigevani Giulio Enea. 2017. "Primi appunti su fake news e dintorni". *MediaLaws* (1): 11-22.

Belluati Marinella, Caielli Mia, Cepernich Christopher, Patti Viviana, Scamuzzi Sergio, Stecca Stefania, Tipaldo Giuseppe. 2021. "Fake news e hate speech. I nodi per un'azione di policy efficace". *Problemi dell'informazione* (1): 49-81.

Bonini, Paolo. 2020. "L'autoregolamentazione dei principali Social Network. Una prima ricognizione delle regole sui contenuti politici". *federalismi.it* (11): 265-281.

Candido, Alessandro. 2020. "Libertà di informazione e democrazia ai tempi delle fake news". *federalismi.it* (20): 105-122.

Ceccarini Luigi, Di Pierdomenico Martina. 2018. "Fake news e informazione via social media". *Problemi dell'informazione* (2): 335-340.

Comandini, Vincenzo Visco. 2018. "Le fake news sui social network: un'analisi economica". *MediaLaws* (2): 183-212.

Croce Michel, Piazza Tommaso. 2019. "Epistemologia delle fake news". *Sistemi intelligenti* (3): 439-467.

Cuniberti, Marco. 2017. "Il contrasto alla disinformazione in rete tra logiche del mercato e (vecchie e nuove) velleità di controllo". *MediaLaws* (1): 26-40.

Donati, Filippo. 2018. "Fake news e libertà di informazione". *MediaLaws* (2): 440-446.

Echikson William, Knodt Olivia. 2018. "Germany's NetzDG: A key test for combatting online hate". *CEPS* (9).

Fubini, Alice. 2019. "Fake news and disinformation online". *Problemi dell'informazione* (1): 243-250.

Gili Guido, Maddalena Giovanni. 2018. "Post-verità e fake news: radici, significati attuali, inattesi protagonisti e probabili vittime". *Media Education*, 9 (1): 1-16.

Leerssen Paddy, Tworek Heidi. 2019. "An Analysis of Germany's NetzDG Law". *Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression*.

Levush, Ruth. 2019. "Government Responses to Disinformation on Social Media Platforms: Argentina, Australia, Canada, China, Denmark, Egypt, European Union, France, Germany, India, Israel, Mexico, Russian Federation, Sweden, United Arab Emirates, United Kingdom". *Law Library of Congress* (9): 86-95.

Magnani, Carlo. 2019. "Libertà d'informazione online e fake news: vera emergenza? Appunti sul contrasto alla disinformazione tra legislatori statali e politiche europee". *Forum di Quaderni costituzionali - Rassegna* (4).

Mazziotti Di Celso, Andrea. 2018. "Dal Primo Emendamento al bavaglio malese. Fake news, libertà di espressione e il rovesciamento delle categorie politiche tradizionali". *MediaLaws* (3): 90-109.

Monti, Matteo. 2017a. "Fake news e social network: la verità ai tempi di Facebook". *MediaLaws* (1): 79-90.

Monti, Matteo. 2017b. "La proposta del ddl Zanda-Filippin sul contrasto alle fake news sui social network: profili problematici". *Diritti comparati*.

Monti, Matteo. 2019. "Il Code of Practice on Disinformation dell'UE: tentativi in fieri di contrasto alle fake news". *MediaLaws* (1): 320-324.

Pagano, Gianluca. 2019. "Il Code of Practice on Disinformation. Note sulla natura giuridica di un atto misto di autoregolazione". *federalismi.it* (11): 1-31.

Palici di Suni, Elisabetta. 2020. "Fake news e referendum". *federalismi.it* (11): 140-149.

Panza Alessandra, Sciacchitano Francesco. 2020. "Fake news e disinformazione online: misure internazionali". *MediaLaws* (1): 102-130.

Pitruzzella, Giovanni. 2018. "La libertà di informazione nell'era di Internet". *MediaLaws* (1): 19-47.

Pizzetti, Francesco. 2017. "Fake news e allarme sociale: responsabilità, non censura". *MediaLaws* (1): 48-59.

Rinceanu, Johanna. 2021. "Verso una forma di polizia privata nello spazio digitale? L'inedito ruolo dei provider nella disciplina tedesca dei social network". *Sistema penale*.

## **Sitografia**

AGCOM. 2018. "News vs. fake nel sistema dell'informazione". Ultimo accesso 31 dicembre 2021.

<https://www.agcom.it/documents/10179/3744102/Allegato+22-11-2018/3aff8790-8039-4456-8f9a-dae2497289a4>.

AGCOM. 2019. "Osservatorio sulla disinformazione online", n. 4. Ultimo accesso 31 dicembre 2021.

<https://www.agcom.it/documents/10179/15564025/StudioRicerca+01-07-2019/721fe550-fcb0-4a05-b3d9-30012a98c616?version=1.0>.

Agenzia per l'Italia Digitale (AgID). 2020. "Fake news: definizione e caratteristiche". Ultimo accesso 6 settembre 2021.

<https://cert-agid.gov.it/news/fake-news-definizione-e-caratteristiche/>.

Camera dei Deputati. 2019. "Come Google combatte la disinformazione". Ultimo accesso 29 ottobre 2021.

[https://www.camera.it/application/xmanager/projects/leg18/attachments/upload\\_file\\_doc\\_acquisiti/pdfs/000/003/888/Google\\_Paper\\_Disinformazione.pdf](https://www.camera.it/application/xmanager/projects/leg18/attachments/upload_file_doc_acquisiti/pdfs/000/003/888/Google_Paper_Disinformazione.pdf).

Caranti Niccolò, Mat Fazıla. 2019. “Dossier: Disinformazione”. *OBCT*. Ultimo accesso 19 gennaio 2022.

<https://www.balcanicaucaso.org/ECPMF/ECPMF-news/Dossier-Disinformazione-192000#9>.

Carbone, Maria Rita. 2020. “Il lato oscuro dei bot, macchine di disinformazione: come difendersi”. Ultimo accesso 20 settembre 2021.

<https://www.agendadigitale.eu/cultura-digitale/il-lato-oscuro-dei-bot-macchine-di-disinformazione-come-difendersi/>.

Censis. 2021. “Disinformazione e fake news durante la pandemia: Il ruolo delle agenzie di comunicazione”. Ultimo accesso 15 dicembre 2021.

[https://www.censis.it/sites/default/files/downloads/Rapporto%20Ital%20Communications-Censis\\_def.pdf](https://www.censis.it/sites/default/files/downloads/Rapporto%20Ital%20Communications-Censis_def.pdf).

Coleman, Keith. 2021. “Introducing Birdwatch, a community-based approach to misinformation”. Ultimo accesso 29 ottobre 2021.

[https://blog.twitter.com/en\\_us/topics/product/2021/introducing-birdwatch-a-community-based-approach-to-misinformation](https://blog.twitter.com/en_us/topics/product/2021/introducing-birdwatch-a-community-based-approach-to-misinformation).

Collins Dictionary. n.d. s.v. “fake news.” Ultimo accesso 6 settembre 2021.

<https://www.collinsdictionary.com/it/dizionario/inglese/fake-news/>.

Commissione Europea. 2018a. “A multi-dimensional approach to disinformation. Report of the independent High level Group on fake news and online disinformation”. Ultimo accesso 4 novembre 2021.

<https://op.europa.eu/it/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1/language-en>.

Commissione Europea. 2018b. “Codice di buone pratiche dell’UE sulla disinformazione”. Ultimo accesso 22 novembre 2021.

[https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=59121/](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=59121/).

Commissione Europea. 2018c. “Flash Eurobarometer 464. Fake News and disinformation online”. Ultimo accesso 2 novembre 2021.

<https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=65673>.

Commissione Europea. 2018d. “Piano d'azione contro la disinformazione”. Ultimo accesso 5 novembre 2021.

<https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2018:0036:FIN:IT:PDF>.

Commissione Europea. 2018e. “Summary report of the public consultation on fake news and online disinformation”. Ultimo accesso 16 novembre 2021.

<https://www.spir.cz/sites/default/files/prilohy/Summaryreportofthepublicconsultationonfakenewsandonlinedisinformation-pdf.pdf>.

Corte dei Conti UE. 2021. “La disinformazione nell’UE: combattuta ma non vinta”. Ultimo accesso 6 novembre 2021.

[https://www.eca.europa.eu/Lists/ECADocuments/SR21\\_09/SR\\_Disinformation\\_IT.pdf](https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_IT.pdf).

ERGA. 2020. “ERGA Report on disinformation - Assessment of the implementation of Code of Practice”. Ultimo accesso 23 novembre 2021.

<https://erga-online.eu/wp-content/uploads/2020/05/ERGA-2019-report-published-2020-LQ.pdf>.

Facebook. n.d. “Approccio alla disinformazione”. Ultimo accesso 23 novembre 2021.

<https://transparency.fb.com/it-it/features/approach-to-misinformation/>.

Gesley, Jenny. 2021. “Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech”. *Library of Congress*. Ultimo accesso 4 dicembre 2021.

<https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/>.

Pizzetti, Franco. 2018. "Governo e fake news, Pizzetti: "Nessuna base normativa, molti i pericoli". *Agenda digitale*. Ultimo accesso 17 dicembre 2021.

<https://www.agendadigitale.eu/cultura-digitale/governo-contro-le-fake-newspizzetti-iniziativa-senza-base-normativa-molti-i-pericoli/>.

Polizia di Stato. 2018. "Fake news: da oggi puoi segnalarle alla Polizia". Ultimo accesso 13 dicembre 2021.

<https://www.poliziadistato.it/articolo/155a6077fdb05e3865595940>.

Senato. 2017a. "Disposizioni per prevenire la manipolazione dell'informazione online, garantire la trasparenza sul web e incentivare l'alfabetizzazione mediatica". Ultimo accesso 21 ottobre 2021.

<https://www.senato.it/service/PDF/PDFServer/BGT/01006504.pdf>.

Senato. 2017b. "La legge tedesca per il miglioramento dell'applicazione delle norme sulle reti sociali". Ultimo accesso 30 novembre 2021.

<https://www.senato.it/service/PDF/PDFServer/BGT/01045672.pdf/>.

Senato. 2017c. "Norme generali in materia di social network e per il contrasto della diffusione su internet di contenuti illeciti e delle fake news". Ultimo accesso 13 dicembre 2021.

<https://www.senato.it/service/PDF/PDFServer/BGT/01066653.pdf>.

Servizio europeo per l'azione esterna (SEAE). 2019. "Rapid Alert System". Ultimo accesso 5 novembre 2021.

[https://eeas.europa.eu/sites/default/files/ras\\_factsheet\\_march\\_2019\\_0.pdf](https://eeas.europa.eu/sites/default/files/ras_factsheet_march_2019_0.pdf).

Timmins, Beth. 2021. "Twitter works with news sites to tackle disinformation". Ultimo accesso 29 ottobre 2021.

<https://www.bbc.com/news/business-58065463>.

Treccani. n.d. s.v. "fake news". Ultimo accesso 6 settembre 2021.

<https://www.treccani.it/enciclopedia/fake-news/>.

Wardle, Claire. "Fake news: It's complicated". 2017. Ultimo accesso 26 ottobre 2021.

<https://firstdraftnews.org/articles/fake-news-complicated/>.

## **Elenco delle figure**

Fig. 1.1 Wardle, Claire. 2017. "7 Types of Mis- And Disinformation". FirstDraftNews.org.

[https://firstdraftnews.org/wpcontent/uploads/2017/02/FDN\\_7Types\\_Misinfo-01-1024x576.jpg](https://firstdraftnews.org/wpcontent/uploads/2017/02/FDN_7Types_Misinfo-01-1024x576.jpg).

Fig. 2.1 Commissione Europea. 2018. "Flash Eurobarometer 464. Fake News and disinformation online", p. 27.

<https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableid=65673>.

Fig. 3.1 Google. 2018. "Applicazione delle Norme della community e statuti NetzDG a confronto (Luglio 2018 - Dicembre 2018)".

[https://transparencyreport.google.com/netzdg/youtube?hl=it&community\\_guidelines\\_enforcement=period:Y2018H2&lu=community\\_guidelines\\_enforcement](https://transparencyreport.google.com/netzdg/youtube?hl=it&community_guidelines_enforcement=period:Y2018H2&lu=community_guidelines_enforcement).

Fig. 4.1 AGCOM. 2019. "Ripartizione dell'offerta di disinformazione online per categoria" in "Osservatorio sulla disinformazione online" n. 4, p. 4.

<https://www.agcom.it/documents/10179/15564025/Studio-Ricerca+01-07-2019/721fe550-fcb0-4a05-b3d9-30012a98c616?version=1.0>.

## **Ringraziamenti**

Giunto al termine del percorso di laurea, ho svolto un lavoro di tesi su un argomento d'interesse, che avevo voglia di esplorare. Spero che questo elaborato possa anche essere utile.

Colgo l'occasione per ringraziare la mia famiglia per il supporto necessario che mi ha dato in questi anni di Università.

Ho svolto un anno e mezzo in presenza e altrettanto tempo a distanza, vagliando metodi di studio differenti e appassionandomi di vari argomenti. Ho imparato a conoscere l'ambiente universitario, quale luogo di conoscenza continua e di nuovi incontri, grazie anche a professori di una certa importanza.

Sicuramente questo è il raggiungimento di una tappa importante di cui essere soddisfatti.