DIPARTIMENTO DI GIURISPRUDENZA

Cattedra di Diritto Penale 2

FAKE NEWS, DISINFORMAZIONE E DIRITTO PENALE NELL'ERA DELLA POST-VERITÀ

RELATORE
Chiar.mo Prof.
Antonino Gullo

CANDIDATA
Giorgia Bizzarri
Matr. 153053

CORRELATORE
Chiar.mo Prof.
Maurizio Bellacosa

ANNO ACCADEMICO 2020/2021

A Colei che mi ha reso una brava studentessa,

e non una studentessa brava.

INDICE

INTRODUZIONE 4

I. LE MANIPOLAZIONI DELL'INFORMAZIONE NELL'ERA DELLA POST-VERITÀ 6

1. Le manipolazioni dell'informazione nell'era della Post-Verità: *Fake News*, Disinformazione e *Misinformation* 6

1.1 *Fake news* definizione e ontologia 9

1.1.1 Le categorie della disinformazione e della misinformation 12

1.2 Libertà di espressione e *fake news* 17

1.2.1 Fake news nel costituzionalismo italiano: tra libertà di espressione e libertà di informazione 18

1.2.2 Fake news nel costituzionalismo statunitense: il Primo Emendamento tra limiti e tutele 22

1.2.3 Tutela internazionale ed europea della libertà di espressione 27

1.3 La qualità delle notizie nell'era del 4.0 33

1.3.1 I fattori che hanno determinato l'incremento delle fake news 34

1.3.2 La formazione mediale della realtà: il caso Blue Whale 36

II. *FAKE NEWS* E DIRITTO PENALE ITALIANO 41

2. *Fake News* e i Reati astrattamente configurabili 41

2.1. Il reato di pubblicazione o diffusione di notizie false, esagerate o tendenziose, atte a turbare l'ordine pubblico 42

2.2. Il reato di diffamazione 45

2.2.1. Il reato di diffamazione on-line 46

2.2.2. La non applicabilità della disciplina della diffamazione a mezzo stampa alle fake news diffuse su sulle piattaforme on-line diverse dai periodici telematici registrati 54

2.3. La responsabilità penale ex. art. 57 c.p. del direttore di una testata telematica 57

2.4. Il reato di procurato allarme presso l'Autorità 64

2.5. La non configurabilità dei reati elettorali per le *fake news on-line* e l'assenza di una disciplina sul silenzio elettorale sui *social media* 66

2.6. Il reato di sostituzione di persona e *identity theft* 68

III. LA RESPONSABILITÀ DEGLI *INTERNET SERVICE PROVIDERS* 74

3. Gli *Internet Service Providers*: definizione e ontologia 74

3.1. La Responsabilità degli *Internet Service Providers*: l'esperienza Statunitense 77

3.2. La Responsabilità degli *Internet Service Providers*: l'esperienza Europea dalla Direttiva 31/2000 al *Digital Service Act* 90

3.3. La Responsabilità degli *Internet Service Providers*: l'esperienza italiana 106

IV. L'IMPATTO DELLE *FAKE NEWS* SULLA DEMOCRAZIA 116

4. Processi democratici e *social network*: la "*Bubble Democracy*" 116

4.1. Alcuni esempi di campagne di disinformazione nel corso di processi elettorali 122

4.1.1. Le elezioni presidenziali americane del 2016: la Internet Research Agency (IRA) 122

4.1.2. Le elezioni presidenziali americane del 2020 127

4.1.3. Fake news e referendum 129

4.1.3.1. Il *referendum* sulla *Brexit* 129

4.1.3.2. Il *referendum* costituzionale del 2016 sulla riforma Renzi-Boschi 132

4.2. Cornice regolatoria e potenziali violazioni 135

4.3. Possibili soluzioni regolatorie 144

CONCLUSIONI 149

INDICE BIBLIOGRAFICO 156

INTRODUZIONE

L'era della Post-Verità si caratterizza per l'avvento di tecnologie innovative e lo sviluppo di nuove piattaforme digitali. Tale scenario, se da un lato ha consentito l'instaurazione di una connessione permanente degli utenti su Internet, dall'altro ha anche portato con sé un aumento vertiginoso non solo della quantità di *fake news* diffuse su Internet, ma anche, e soprattutto, dalla velocità della loro propagazione.
Come sarà esposto nel dettaglio nel primo capitolo, ciò è conseguenza necessaria del fenomeno della polarizzazione presente sul *web*, meccanismo che fa sì che gli utenti vengano inconsapevolmente chiusi nelle cosiddette "camere d'eco" o bolle virtuali, entrando a contatto solo con le informazioni conformi alle proprie idee e opinioni.
Il presente elaborato si aprirà, dunque, con l'analisi della definizione e dell'ontologia delle categorie delle *fake news*, della disinformazione e della *misinformation.*
A ciò seguirà la trattazione del tema della necessità di individuare un bilanciamento tra l'esigenza di incrementare la lotta contro fenomeni manipolativi dell'informazione e l'importanza di assicurare una tutela effettiva della libertà di espressione. A tale fine, dopo una presentazione delle nozioni di libertà di manifestazione del pensiero in senso attivo e passivo, verranno illustrate le soluzioni giurisprudenziali e dottrinali adottate in Italia, negli Stati Uniti, a livello europeo ed internazionale; rispettivamente con riferimento all'art. 21 Cost., al I emendamento americano, all'art. 10 CEDU e all'art. 19 dell'*International Covenant on Civil and Political Rights.*
Il secondo capitolo sarà, poi, dedicato alle ipotesi dei reati astrattamente configurabili nell'ordinamento giuridico italiano da parte degli individui che diffondono notizie false sul *web*. Nello specifico verranno trattati i seguenti illeciti penali: il reato di pubblicazione o diffusione di notizie false, esagerate o tendenziose, atte turbare l'ordine pubblico; il reato di diffamazione *on-line* e la non applicabilità della disciplina della diffamazione a mezzo stampa alle *fake news* diffuse su Internet; il reato di procurato allarme presso l'Autorità; la non

configurabilità dei reati elettorali e l'assenza di una disciplina sul silenzio elettorale sui *social media*; il reato di sostituzione di persona e la *identity theft.*

All'analisi delle suddette fattispecie criminose seguirà, nel terzo capitolo, una trattazione dei regimi di responsabilità applicabili agli *Internet Service Providers*, mediante lo svolgimento di un confronto tra le soluzioni adottate nel paradigma regolatorio statunitense e in quello europeo, nell'ambito del quale saranno oggetto di approfondimento le risposte fornite dalla giurisprudenza italiana.

Infine, il quarto capitolo sarà dedicato alla tematica delle campagne di disinformazione nel corso delle elezioni, argomento che sarà affrontato anche alla luce dell'analisi di alcuni tra gli esempi storici maggiormente rilevanti, come le *disinformation operations* condotte nel corso delle elezioni presidenziali statunitensi de 2016. La sezione in questione, si concluderà, poi, con l'illustrazione del quadro regolatorio internazionale esistente, e delle proposte di *soft* e *hard* law prospettate in dottrina e giurisprudenza negli anni più recenti.

Il presente elaborato si pone, dunque, l'obiettivo di mostrare la necessità dell'introduzione di una disciplina, tanto nazionale quanto internazionale, che, tenendo conto delle evoluzioni tecnologiche e digitali che hanno caratterizzato l'ultimo secolo e che continueranno a dominare il prossimo futuro, preveda un regime di responsabilità *ad hoc* non solo per gli utenti che diffondono notizie false, ma anche, e soprattutto, per le piattaforme digitali che ospitano i cosiddetti *user generated contents.*

Nello specifico, come verrà argomentato più nel dettaglio nelle conclusioni, a parere della scrivente la soluzione maggiormente efficace risiederebbe nell'adottare un paradigma che contemperi soluzioni fondate su meccanismi di autoregolazione con strumenti di eteroregolazione.

CAPITOLO I

I. LE MANIPOLAZIONI DELL'INFORMAZIONE NELL'ERA DELLA POST-VERITÀ

1. Le manipolazioni dell'informazione nell'era della Post-Verità: *Fake News,* Disinformazione e *Misinformation*

La ricerca della verità, di ciò che gli antichi Grechi chiamavano *l'aletheia*, è sempre stata al centro del dibattito filosofico-giuridico sin dalle origini della democrazia. Parmenide nella sua opera *Sulla Natura* scriveva: «la via della verità è insegnata al filosofo da Dike, Dea della Giustizia»[1].

Nel corso del tempo si sono alternate diverse visioni del concetto di verità, ora interpretandola come corrispondenza tra un fatto e uno stato oggettivo delle cose (c.d. teoria della corrispondenza), ora facendola coincidere con un sistema coerente, non contraddittorio e complessivo di convinzioni (c.d. teoria della coerenza).

Il dibattito sulla verità si accentuò, poi, con la nascita dello Stato Costituzionale. Questo, infatti, è stato descritto come intrinsecamente «consegnato a una perpetua ricerca della verità» [2], alla quale nel tempo sono stati attribuiti significati diversi, ma che è sempre stata profondamente legata alla tutela costituzionale delle libertà fondamentali.

A tal riguardo, Kant, con la sua teoria sul *divieto di menzogna*, si è posto, forse, come il più grande garante dello Stato Costituzionale. Egli, infatti, riteneva che la menzogna fosse una violazione della «dignità dell'uomo nella sua propria persona», una violazione che non poteva in nessun caso essere considerata necessaria o giustificabile[3].

Ma cosa segna il confine tra menzogna e verità? Sussiste solo un divieto per lo Stato Costituzionale di mentire consapevolmente, o, invece, esiste anche un vero e proprio diritto alla verità per il cittadino?

---

[1] PARMENIDE, *Sulla Natura,* frammento 1.
[2] SPADARO, *Contributo per una teoria della Costituzione,* 1994, p 123.
[3] HABERLE, *Diritto e Verità,* 200, p. 45.

Ci troviamo oggi in quella che è stata definita da molti come *l'epoca della Post-Verità* [4].

Nello specifico, nel 2016 questo termine è stato dichiarato parola dell'anno dall'*Oxford Dictionary*.

Quest'ultimo definiva la *Post-Truth* come aggettivo «relativo e denotante circostanze in cui i fatti oggettivi hanno minore influsso nel disegnare l'opinione pubblica che non gli appelli alle emozioni o a credenze personali»[5]. In realtà, il termine Post-verità oggi va inteso non come aggettivo relativo, bensì come sostantivo, che si riferisce all'atteggiamento culturale post-moderno, che ha segnato l'unione tra nichilismo, svalutazione della verità e le nuove forme di comunicazione tramite Internet[6].

Nonostante questa precisazione, la definizione dell'*Oxford Dictionary* assume una grande rilevanza per diversi fattori.

Anzitutto, è lo stesso *Oxford Dictionary* a chiarire il significato del prefisso "post" del termine post-verità: esso non fa riferimento a un evento temporalmente successivo ad un altro – come ad esempio nel caso di post-guerra o post-rivoluzione – bensì, sta ad indicare che il concetto che segue il prefisso è ormai superato. In altre parole, il prefisso "post" suggerisce l'attuale irrilevanza e anacronismo del concetto stesso di "verità", fa riferimento a un mondo in cui la verità oggettiva e materiale cede il passo a un profondo relativismo.

In secondo luogo, non appare casuale la scelta dell'*Oxford Dictionary* di eleggere la *Post-Truth* come parola dell'anno proprio nel 2016. È, infatti, interessante notare che nello stesso anno la parola *fake news* entrò a far parte del linguaggio comune a seguito delle elezioni presidenziali americane, divenendo parola dell'anno per il *Collins Dictionary* nel 2017.

Evitando di entrare nel dettaglio delle elezioni americane di cui si tratterà in seguito[7], il rapporto tra *fake news* e Post-Verità può essere facilmente compreso analizzando le dinamiche dell'informazione nell'ambito di Internet.

---

[4] FERRARIS, *Postverità e altri enigmi*, Bologna, 2017, pp. 72-76; SAVARESE, *Dalla bugia alla menzogna: la postverità e l'impossibilità del diritto,* in *Nomos le attualità nel diritto*, 2018, 2, pp. 1-21.

[5] SAVARESE, *Dalla Bugia alla Menzogna: la Postverità e l'impossibilità del Diritto,* in *Nomos le attualità nel diritto*, 2018, 2, p. 1.

[6] MAGNANI, *Libertà di espressione e fake news, il difficile rapporto tra verità e diritto. Una prospettiva teorica,* in *Costituzionalismo.it*, 2018, 3.

[7] V. *infra* Cap. IV.

Paolo Savarese definiva la Post-Verità come *un carcere immaginario.*[8] Il carcere immaginario di Savarese altro non è che la rappresentazione figurativa del fenomeno della polarizzazione che avviene su Internet[9], anche detto fenomeno della *filter bubble.*[10]

È proprio qui che risiede il grande paradosso dell'era della Post-Verità: se l'avvento di Internet da una parte ha reso le persone sempre più connesse tra di loro, facilitando e velocizzando la circolazione di informazioni, dall'altra non ha fatto altro che alimentare il fenomeno della *filter bubble*.

Infatti, pur avendo gli utenti potenzialmente accesso a fonti infinite di informazioni, in realtà questi tendono a chiudersi in comunità virtuali in cui ciascuno si confronta solo con persone che condividono le proprie opinioni. La naturale conseguenza di ciò è non solo che i pregiudizi si acuiscono e si consolidano, ma anche che gli utenti divengono sempre meno propensi a credere alle idee che non circolano nella loro bolla.

Questi fenomeni sono terreno fertile per le *fake news*, per la disinformazione e per la *misinformation*. Infatti, tali manipolazioni del linguaggio, facendo leva sulla polarizzazione che connota il consumo di informazioni su Internet, riescono ad avere una propagazione più ampia e rapida e ad accrescere la propria credibilità; conseguentemente allungando il ciclo di vita della notizia falsa.

A tal riguardo, è interessante notare che, come esposto in un rapporto del 2018 dell'AGCOM[11], il ciclo di vita di una notizia falsa è tendenzialmente più breve rispetto a quello di una notizia vera.

Da questo dato discende, come conseguenza naturale, che più una *fake news*, grazie al suo circolare in specifiche comunità, diviene credibile per l'utente, più lunga sarà la durata della vita della notizia stessa.

Prima di passare alla definizione delle diverse tipologie di manipolazione dell'informazione – vale a dire *fake news*, disinformazione e *misinformation* – è importante chiarire che a livello internazionale non vi è un *mutuo consenso* sul significato da attribuire a questi termini. Tuttavia, in questa sede si tenterà di fornire

[8] SAVARESE, *Dalla Bugia alla Menzogna: la Postverità e l'impossibilità del Diritto,* cit., p. 19
[9] AGCOM, *News vs. Fake nel Sistema dell'informazione,* 2018, p. 3
[10]. PITRUZZELLA, POLLICINO, QUINTARELLI, *Parole e Potere, Libertà di Espressione, Hate Speech e Fake News,* Egea, 2017, pp. 67-69.
[11] AGCOM, *New vs. Fake nel Sistema dell'informazione,* Interim Report, Indagine Conoscitiva, Del. 309/16/Cons, novembre 2018.

una panoramica quanto più ampia possibile di tali concetti, soffermandosi, in conclusione, su una visione penalisticamente orientata.

1.1 *Fake news* definizione e ontologia

La nascita del termine *fake news* si fa risalire convenzionalmente alle elezioni presidenziali americane del 2016, occasione durante la quale il Presidente Americano Trump lo utilizzò con riferimento a notizie invise alla sua amministrazione.

In realtà, le elezioni americane del 2016 segnano soltanto il momento dopo il quale l'attenzione mediatica si è concentrata sull'utilizzo del termine *fake news*, dando avvio a un processo che ha portato a una più compiuta delineazione dei confini di tale concetto; al contrario, la propagazione di notizie false o ingannevoli è, ovviamente, ben più risalente nel tempo.

A tal riguardo, basti pensare che fu proprio una notizia falsa che diciotto anni fa diede avvio all'invasione dell'Iraq. Nello specifico, l'allora segretario di Stato degli USA Colin Powell tenne un discorso di fronte al Consiglio di Sicurezza dell'ONU il 5 febbraio del 2003 mostrando immagini satellitari, foto e grafici al fine di provare l'esistenza di un programma iracheno di armi batteriologiche e chimiche. Niente di tutto ciò era vero, tuttavia, questa messa in scena convinse l'allora presidente americano Bush a superare le opinioni contrarie della comunità internazionale, e dare avvio all'invasione dell'Iraq[12].

E ancora, una notizia falsa di una certa rilevanza si fa risalire addirittura al 1814, durante le guerre Napoleoniche. Si narra, infatti, che un uomo vestito in uniforme britannica, spacciandosi per il Colonnello du Bourg, diffuse la notizia dell'uccisione di Napoleone e della conseguente vittoria della guerra da parte degli Alleati. Nella realtà, Napoleone era ancora in vita e la guerra non si era conclusa; tuttavia, la propagazione di tale notizia mandò in *tilt* la borsa di Londra, dove, ritenendo che il tiranno fosse defunto, la maggior parte degli azionisti si affrettò a investire[13].

[12] RAITANO, *Le notizie false che cambiano il mondo,* in *Altraeconomia.it,* 1 aprile 2018.
[13] DALLA CASA, *Napoleone è Morto! La Fake News che mandò in tilt la borsa di Londra,* in *Wired.it,* 28 luglio 2017; DALE, *Napoleon is Dead,* 2006.

Sebbene, dunque, la tendenza a creare notizie false possa considerarsi una costante nel modo di agire dell'Uomo di ogni tempo, sarebbe, tuttavia, erroneo e riduttivo far coincidere il concetto di notizia falsa con quello di *fake news*.

Come si accennava sopra, il termine *fake news* venne eletto parola dell'anno dal *Collins Dictionary* nel 2017. Secondo tale autorevole fonte con *fake news* si intende «*false, often sensational, information disseminated under the guise of news reporting*».[14]

Dunque, il *Collins Dictionary* parla di informazioni false, spesso sensazionali, diffuse come fossero vere notizie giornalistiche.

Da questa definizione, apparentemente banale, si può in realtà desumere una caratteristica fondamentale delle *fake news*: esse raccolgono in sé tanto il falso oggettivo, quanto il falso soggettivo.

Con l'espressione falso oggettivo si identifica la «non verità della notizia in sé, quale non corrispondenza della stessa alla realtà fattuale concretamente verificabile secondo parametri accettati dalla comunità di riferimento». Al contrario, il profilo soggettivo del falso attiene «alla convinzione di tale corrispondenza da parte del soggetto che divulga la notizia».[15]

In altre parole, le *fake news* racchiudono in sé sia la disinformazione che la *misinformation*, concetti che si distinguono a seconda che vi sia o meno la consapevolezza della falsità della notizia e un intento ingannatorio da parte di chi la diffonde.

Rimandando al paragrafo successivo[16] un'analisi più approfondita di tali concetti, appare a questo punto necessario fornire una definizione compiuta e penalisticamente orientata di *fake news*.

Ai fini del presente elaborato, con il termine *fake news* si intenderà «un'informazione in parte o del tutto non corrispondente al vero, prodotta e divulgata intenzionalmente o inintenzionalmente attraverso il Web, i media o le tecnologie digitali di comunicazione, e caratterizzata da un'apparente plausibilità, quest'ultima alimentata da un sistema distorto di aspettative dell'opinione pubblica e da un'amplificazione dei pregiudizi che ne sono alla base, che ne agevola la

[14] Collins Dictionary: fake news, << https://www.collinsdictionary.com/it/dizionario/inglese/fake-news>>.

[15] PERRONE, *Fake news e libertà di manifestazione del pensiero: brevi coordinate in tema di tutela costituzionale del falso,* in *Nomos le attualità nel diritto*, 2018, pp. 3 e ss.

[16] V. *infra* § 1.1.1.

condivisione e la diffusione pur in assenza di una verifica delle fonti, tale da ledere beni giuridici individuali, come l'onore e la reputazione, ovvero finalizzata a incidere, direttamente o indirettamente, sulla libertà dei cittadini di esercitare il diritto di voto e ad incidere sul corretto funzionamento delle istituzioni democratiche».[17]

Vediamo, dunque, come appaia lampante dalla lettura di tale definizione che il significato del termine *fake news* non può essere ridotto al tradizionale concetto di notizie false o di "bufale".

Infatti, se da un lato l'espressione in questione evoca l'idea di un prodotto elaborato da esperti di comunicazione che operano sul *surplus* di informazioni su Internet, dall'altro esso ricomprende anche quell'insieme di informazioni diffuse da persone inconsapevoli della falsità delle stesse, in quanto soggette al fenomeno della polarizzazione in rete.

Riprendendo la tassonomia di Guerini,[18] nell'ambito della generale suddivisione tra disinformazione e *misinformation*, possiamo distinguere le seguenti specifiche tipologie di *fake news*:

- *Satiry and Parody*: si tratta di notizie false, diffuse con uno scopo satirico o parodico e caratterizzate dall'assenza di uno scopo offensivo o ingannatorio;
- *Misleading Content*: si fa qui riferimento a contenuti la cui ingannevolezza deriva dalla semplificazione da parte dell'autore di un concetto complesso, che comporta un'alterazione della percezione dei lettori;
- *Imposter Content, False Connection e False Context*: in tutti questi casi sussiste un nucleo di verità, il quale tuttavia viene fraudolentemente alterato rispettivamente attraverso la manipolazione della fonte della notizia, corredando l'articolo di titoli e immagini che non corrispondono all'effettivo contenuto dello stesso, o, infine, aggiungendo a una notizia di per sé vera informazioni false di minore importanza;
- *Manipulated Content* e *Fabricated Content*: si tratta di due casi limite che si riferiscono ad ipotesi in cui il contenuto di un articolo, immagine o filmato

[17] GUERINI, Fake News *e Diritto Penale, La Manipolazione Digitale del Consenso nelle Democrazie Liberali,* Torino, 2020, pp. 28-29.

[18] GUERINI, *Fake News e Diritto Penale, La Manipolazione Digitale del Consenso nelle Democrazie Liberali* cit., pp 35-38.

viene intenzionalmente ed espressamente alterato, o addirittura fabbricato, al fine di ingannare i destinatari dell'informazione stessa;

Tutte le tipologie di *fake news* sopra citate hanno certamente un'incidenza a livello di comunicazione e rilevanza mediatica, tuttavia, soltanto alcune di esse assurgono a violazioni penalmente rilevanti.

Come sarà meglio analizzato[19], da un punto di vista penalistico possiamo distinguere le *fake news*, e soprattutto le ipotesi di disinformazione, a seconda che queste siano di carattere cosiddetto *neutro*, e quindi non lesivo di specifici interessi giuridici, o che queste integrino ipotesi di reato, come ad esempio la diffamazione.

Appare, infine, necessario dare conto di un'ulteriore tipologia di *fake news*, poco trattata ma oggi quanto mai attuale. Si tratta di contenuti falsi a stampo antiscientifico, creati al fine di sostenere tesi scientifiche minoritarie o contrarie alla letteratura prevalente. A tal riguardo, basti pensare alla molteplicità di *fake news* riguardanti l'epidemia Covid-19, che nell'ultimo anno hanno invaso il *web*.[20]

1.1.1 Le categorie della disinformazione e della *misinformation*

Passando ora all'analisi delle due macro-categorie di *fake news*, è fondamentale distinguere la fattispecie della disinformazione da quella della semplice *misinformation*.

Per quanto concerne la prima categoria, la Commissione Europea nel 2018 ha fornito una definizione di disinformazione in termini di «*verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm. Public harm comprises threats to democratic political and policymaking processes as well as*

[19] V. *infra* Cap. II.

[20] Lewis Hamilton ha diffuso notizie affermando che dietro la diffusione del Covid ci sarebbe Bill Gates, il cui intento sarebbe di impiantare *microchip* nel corpo delle persone; il rapper Wiz Khalifa ha sostenuto che il Corona Virus è legato alla tecnologia del 5G (per ulteriori riferimenti v. https://www.quotidiano.net/magazine/coronavirus-madonna-vaccino-1.5381343); Facebook e Twitter hanno rimosso post del Presidente americano Donald Trump, classificandole come *news* sul Corona Virus. Nello specifico il Premier statunitense affermava sui suoi profili social "la quasi immunità dei bimbi": v. l'articolo reperibile su << https://www.lastampa.it/esteri/2020/08/06/news/trump-vaccino-prima-di-fine-2020-ma-twitter-gli-blocca-l-account-per-fake-news-sul-covid-1.39165225 >>.

public goods such as the protection of EU citizens' health, the environment or security»[21] .

Vediamo, dunque, come qui ci troviamo nell'ambito di quel profilo oggettivo del falso, che si riferisce a ipotesi in cui colui che crea, presenta o diffonde la notizia è pienamente consapevole della falsità della stessa.

In questi contesti, il soggetto agisce con uno scopo preciso e può causare danni non solo ai lettori, in quanto singoli individui, ma più in generale all'istituzione democratica nel suo complesso.

Ma qual è lo scopo con cui agiscono i creatori della disinformazione?

Anche con riferimento alla definizione della Commissione Europea, possiamo individuare tre tipologie di motivazioni fondamentali che si celano dietro la consapevole manipolazione di notizie: commerciale, politica e sociologica.

Per quanto concerne la prima, un esempio lampante di una motivazione di stampo commerciale che ha dato luogo alla creazione di una grande quantità di *fake news* intenzionali ci è fornita dai siti *pro-Trump* creati durante le lezioni presidenziali americane del 2016.

Tali siti vennero progettati e utilizzati in maniera ingente in quanto costituivano fonti di guadagno economico immediato per i creatori di notizie false grazie al cosiddetto *Clickbaiting.*[22]

Per *Clickbaiting* si intende quel meccanismo incentrato su contenuti *web* la cui funzione principale è di attirare il maggior numero possibile di utenti, al fine di generare rendite pubblicitarie *on-line*.

Dunque, mentre generalmente condividere contenuti sulle piattaforme dei *social media* è privo di costi, esistono siti Internet dedicati alla creazione e diffusione di disinformazione.

Tali siti *web* utilizzano la pubblicità *on-line* per ottenere un profitto senza dover sopportare i costi necessari alle ordinarie verifiche di veridicità e affidabilità dei contenuti effettuate dalle agenzie professionali di informazioni. [23]

---

[21] COMMISSIONE EUROPEA, *Commission Communication for tackling online Disinformation: a European approach*, COM, 2018, paragrafo 2.1.

[22] GUERINI, *Fake News e Diritto Penale, La Manipolazione Digitale del Consenso nelle Democrazie Liberali*, cit., p. 40.

[23] DUFFY, *Websites that paddles disinformation make millions of dollars in Ads*, in *New Study Fields, CNN*, <<https://222.cnn.com/2019/08/18/tech/adsvertising-disinformation-money-reliable-sources/index.html>> [https://perma.cc/R7KY-28FF].

Anche in questo caso, tali siti al fine di massimizzare il loro guadagno sfruttavano la polarizzazione di Internet.

Risulta, infatti, dai sondaggi che i Repubblicani fossero più polarizzati, alludendosi con tale termine alla loro maggiore propensione, da una parte, a credere alle notizie che circolavano nella loro bolla virtuale e, dall'altra, a rifiutare notizie contrarie alle proprie convinzioni. [24]

Questa condizione ha generato quella che gli americani definirebbero una *Slippery Slope*, ossia letteralmente un pendio scivoloso: più gli utenti di una comunità virtuale che ricevono notizie false sono polarizzati, più saranno propensi a ritenerle vere. La naturale conseguenza di ciò è che tali utenti ri-condivideranno su Internet quelle notizie, accrescendo, così, la credibilità delle stesse per altri lettori.

Spostandoci ora al secondo scopo della disinformazione, la motivazione politica è forse il principale motore che dà propulsione alla creazione di *fake news* intenzionali e consapevoli.

È, infatti, molto frequente che un candidato diffonda personalmente o per il tramite di intermediari contenuti falsi, manipolati o infondati al fine di alterare il dibattito politico e aumentare le sue probabilità di vittoria.

A tal riguardo, è interessante notare che la politica rientra tra le aree tematiche maggiormente colpite da disinformazione secondo il sondaggio dell'AGCOM del 2018. [25]

La motivazione che risiede dietro la concentrazione di disinformazione su tale materia consiste nel fatto che la politica rientra tra quelle che l'Agenzia definisce *Hard News.* Si tratta di tematiche, per così dire *sensational*, [26] ovverosia argomenti che lasciano ampio spazio al dibattito e suscitano stati emotivi negli utenti.

Infine, la terza spinta che può portare alla creazione e diffusione di disinformazione è costituita da una ragione di stampo sociologico. Questo è il caso degli *influencer* su Internet che possono generare disinformazione al fine di ottenere elevati numeri di visualizzazioni o, più in generale, per accrescere la loro rilevanza mediatica.

---

[24] EUROPEAN COMMISSION, *JRC Technical Reports, JRC Digital Economy Working Paper 2018-02, the digital transformation of news media and the rise of disinformation and fake news,* aprile 2018, p. 32.

[25] AGCOM, *News vs. Fake nel Sistema dell'informazione*, 2018, pp. 33 – 37.

[26] Collins Dictionary: fake news, << https://www.collinsdictionary.com/it/dizionario/inglese/fake-news>>.

È interessante notare che il fenomeno è diventato così diffuso che nel 2019 che un gruppo di giovani programmatori e informatici italiani ha elaborato un'apposita *App* chiamata "*Power Board".*

Si tratta di un'applicazione per *smartphone* che ha lo scopo di «facilitare e ottimizzare l'utilizzo del social in maniera etica, per analisi di contenuti e audience e, quindi per allontanare fake e falsi profili, trovare, gestire e verificare *Influencer*».[27]

Un'esemplificazione perfetta di un contesto in cui si possono rintracciare tutte e tre gli scopi sopra menzionati ci è fornita dalle campagne di disinformazione.

Si tratta contesti in cui vi è una diffusione di notizie false o manipolate da parte di esperti di comunicazioni e *digital marketing* appositamente assunti da candidati politici.

Vediamo, infatti, come se da una parte abbiamo il cliente che persegue uno scopo puramente politico, dall'altra abbiamo gli esperti da lui assunti che agiscono al fine di ottenere una remunerazione economica. Infine, il quadro viene completato dagli *influencer* che partecipano alla campagna con un duplice scopo: aumentare la propria rilevanza mediatica e, al contempo, ottenere un ritorno economico.

In conclusione, dunque, possiamo riassumere il concetto di disinformazione come la «divulgazione di contenuti informativi falsi, infondati, manipolati o riportati in maniera non veritiera, creati ad arte in modo da risultare verosimili nel contesto mediatico»[28], sfruttando a tal fine la polarizzazione di Internet.

Agli antipodi della disinformazione si colloca la *misinformation*.

In questo caso, ci troviamo nell'ambito soggettivo del falso: ossia la diffusione inconsapevole di *fake news*.

Nello specifico, riprendendo le parole del Rapporto del 2018 del Gruppo di Esperti sulle *Fake News e la Disinformazione Online* creato dalla Commissione Europea (HLEG), per *misinformation* si intende «*misleading or inaccurate information shared by people who do not recognize it as such*». [29]

---

[27] *Stop alle Fake News su Intagram. Ci pensa una Startup italiana*, in *CORCOM*, 29 agosto 2019, <<https://www.corrierecomunicazioni.it/digital-economy/instagram-piu-trasparente-ci-pensa-una-startup-italiana/>>.

[28] AGCOM, *News vs. Fake nel Sistema dell'informazione*, 2018, paragrafo 2.1

[29] COMMISSIONE EUROPEA, *Final report of the High-Level Expert Group on Fake News and Online Disinformation*, 12 marzo 2018, p. 10.

Dunque, a differenza di quanto avviene nella disinformazione, chi causa *misinformation* si limita a condividere informazioni senza rendersi conto che queste sono inaccurate o fuorvianti.

Ma cosa spinge un utente a credere alla veridicità di una notizia o un'informazione, senza averla preliminarmente verificata?

Ancora una volta la risposta ci riporta al fenomeno della polarizzazione su Internet, o più precisamente al *bias dello struzzo* di Guerini. [30]

Tale meccanismo psicologico si fonda sulla sensazione di sicurezza e stabilità che gli utenti percepiscono nel vedere confermate le proprie idee e, al contrario, nella precarietà e confusione che gli individui provano quando le proprie convinzioni vengono smentite.

Tali processi socio-psicologici fanno sì che gli utenti agiscano come degli struzzi di fronte a informazioni che non condividono: infilano la testa sotto la sabbia.

Fuor di metafora, il *bias dello struzzo* descrive la tendenza dei lettori a rifiutare le informazioni che confliggono con le proprie idee, e conseguentemente, a ritenere vere, senza necessità di una previa verifica, le notizie che, al contrario, confermano i propri pensieri.

In conclusione, è interessante notare che negli ultimi anni si è diffusa una tipologia di manipolazione dell'informazione che si pone a cavallo tra la disinformazione e la *misinformation*: il *deepfake.*

Quest'ultimo è stato definito come la tecnologia che consente di creare contenuti audiovisivi in cui persone vere dicono e fanno cose che, nella realtà, non hanno mai detto o fatto. [31]

Più precisamente, si tratta di una tecnologia che utilizza algoritmi di nuova generazione al fine di scambiare i volti di due persone e sincronizzarne il labiale con un'altissima precisione.

Ancora una volta, un esempio di tale manipolazione dell'informazione ci è fornito dall'ambite politico americano.

Nel 2019 è stato messo in rete un video che ritraeva la Speaker della *United States House of Representatives*, Nancy Pelosi, in uno stato di ubriachezza. La gravità di

---

[30] GUERINI, *Fake News e Diritto Penale, La Manipolazione Digitale del Consenso nelle Democrazie Liberali,* cit., p. 44

[31] CHESNEY, CITRON, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 14 luglio 2018, in *University of California Berkeley School of Law*, p. 1753.

tale *fake news* è stata ulteriormente accresciuta dal fatto che anche il Presidente Americano Donald Trump ha ri-condiviso tale contenuto sul proprio profilo *Twitter*, ottenendo oltre tre milioni e mezzo di visualizzazioni.

Nel caso di specie, la volontà di credere alla veridicità del video è probabilmente stata alimentata dal cosiddetto *bias di conferma*, [32] ossia dalla necessità degli utenti di prendere *scorciatoie mentali*, classificando come veri i contenuti che confermano le proprie opinioni.

Appare, dunque, evidente che il rischio generato da questa tipologia di tecnologia manipolativa dell'informazione è superiore a quello di qualsiasi altro *fake*.

Infatti, l'innestarsi della profonda verosimiglianza di tali contenuti audiovisivi su una consolidata polarizzazione di Internet, determina una elevatissima potenzialità dannosa del *deepfake.*

Dunque, in conclusione, se dal punto di vista degli utenti inconsapevoli il *deepfake* può essere considerato come l'*ultima frontiera della misinformation*, probabilmente, dal lato dei creatori di tali video, sarebbe più corretto considerarlo *l'ultimo confine della disinformazione*.

1.2 Libertà di espressione e *fake news*

La libertà di espressione costituisce la *pietra angolare dell'ordinamento democratico*,[33] il principio fondamentale su cui poggia l'idea stessa del pluralismo. Tale libertà ricopre un ruolo fondamentale in tutti gli ordinamenti di matrice liberale; tuttavia, i vari Stati ne articolano la tutela in maniera diversa a seconda della propria tradizione giuridica.

In via preliminare, possiamo tracciare una distinzione tra *Democrazia Militante* e la *Democrazia Tollerante*.[34]

Per quanto concerne la prima tipologia, con il termine Democrazia Militante si fa riferimento a uno Stato incentrato sulla difesa assoluta di un sistema di valori, contro eventuali pericoli derivanti dall'esercizio di diritti riconosciuti dalla costituzione stessa. [35]

---

[32] GUERINI, *Fake News e Diritto Penale, La Manipolazione Digitale del Consenso nelle Democrazie Liberali,* cit., p. 44.

[33] Corte Cost., 2 aprile 1969, n. 84, in *consultaonline*, paragrafo 5.

[34] PITRUZZELLA, POLLICINO, QUINTARELLI, *Parole e Potere, Libertà di Espressione, Hate Speech e Fake News,* cit., pp. 1-3.

[35] LOEWENSTEIN, *Militant Democracy and Fundamental Rights,* in *American Political Science Review,* 1937, pp. 31, 417 e ss.

Nella democrazia tollerante, al contrario, viene meno l'idea stessa di un controllo statale sull'esercizio dei diritti da parte dei cittadini.

Dunque, risulta sin da qui evidente che tali diversità hanno un inevitabile riflesso anche sulle modalità che i singoli Stati possono adottare al fine di regolamentare e contenere la diffusione di *fake news*.

Infatti, mentre in un sistema giuridico con una maggiore propensione all'intrusione dello Stato nell'ambito della tutela della libertà di espressione, quale quello Europeo, sarà più semplice anche prevedere l'intervento di questo sulla circolazione di contenuti non veritieri; diversamente, in un paradigma costituzionale, quale quello degli Stati Uniti d'America, in cui la tutela della libertà di espressione sembra non lasciare spazio a limitazioni, sarà certamente più complesso consentire un intervento statale nella lotta contro le *fake news*[36].

In altre parole, la regolamentazione delle *fake news* deve trovare un bilanciamento con la tutela costituzionale della libertà di espressione, bilanciamento che inevitabilmente giunge a risultati diversi a seconda della modalità con cui la libertà di manifestazione del pensiero viene sancita nei vari ordinamenti.

1.2.1 *Fake news* nel costituzionalismo italiano: tra libertà di espressione e libertà di informazione

Nell'ordinamento italiano la libertà di espressione viene tutelata dall'art. 21 della Costituzione, ai sensi del quale «tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione».

L'avvento di Internet ha profondamente modificato le modalità di comunicazione, espressione e informazione, ampliando in maniera significativa la parte di popolazione a cui l'aggettivo "tutti" fa riferimento.

Se, infatti, un tempo erano pochi coloro che concretamente avevano accesso ai costosi e limitati mezzi di comunicazione, oggi la totalità degli utenti ha la possibilità di condividere con il resto del *web* il proprio pensiero in ogni momento.

[36] PITRUZZELLA, POLLICINO, QUINTARELLI, *Parole e Potere, Libertà di Espressione, Hate Speech e Fake News,* cit., p 46.

Dunque, leggendo l'art. 21 alla luce dei predetti cambiamenti tecnologici e sociali, appare inevitabile domandarsi se la tutela assicurata da questa disposizione si estenda anche alla diffusione di *fake news* su Internet.

La risposta fornita dal costituzionalismo italiano sembra essere negativa: il diritto alla libertà di espressione non può essere invocato come giustificazione per la creazione e diffusione di *fake news*.

L'orientamento maggiormente risalente nel tempo a sostegno di tale posizione vede nel falso un *limite logico* alla tutela delle manifestazioni del pensiero. [37]

Il punto di partenza di tale teoria è l'analisi letterale del testo del primo comma dell'art. 21, e nello specifico l'esegesi del termine *proprio.*

La circostanza che il pensiero venga qualificato come "proprio" indurrebbe a ritenere che la disposizione in esame protegga esclusivamente il pensiero appartenente a colui che lo esprime.

Dunque, se l'autore della notizia è consapevole della falsità della stessa, essa non rappresenta realmente un suo *proprio* pensiero, e quindi, non gode della tutela assicurata dall'art. 21. [38]

Si tratta di un'interpretazione in cui viene posto l'accento sull'interesse individuale; per cui, se le idee espresse non sono proprie del creatore o diffusore delle stesse, anche l'interesse individuale alla base della tutela viene meno.

Un approccio più recente, invece, ritiene che l'incostituzionalità delle *fake news* derivi dal fatto che l'art. 21 non tutela solo la libertà di espressione in quanto diritto di esprimere attivamente il proprio pensiero, ma anche in senso passivo, come diritto di essere informati.

In questa ottica, la disposizione in questione fornirebbe una tutela contro informazioni false che minano la corretta formazione dell'opinione pubblica, privando i cittadini di informazioni veritiere, e, quindi, impedendogli di formarsi un giudizio critico. [39]

Tale interpretazione è stata accolta in numerose pronunce della Corte Costituzionale[40].

---

[37] PERRONE, *Fake news e libertà di manifestazione del pensiero: brevi coordinate in tema di tutela costituzionale del falso*, in *Nomos le attualità nel diritto*, 2/2018, p. 9.

[38] ESPOSITO, *La libertà di manifestazione del pensiero*, Milano, 1958, p. 36.

[39] BASSINI, *Primi appunti su* fake news *e dintorni*, in *Media Laws*, 11 ottobre 2017, pp. 18 e ss.

[40]Corte Cost., 9 giugno 1972, n. 105 in *consultaonline;* Corte Cost.,9 luglio 1974, n. 225, in *consultaonline*; Corte Cost., 13 maggio 1987, n. 153 in *consultaonline;* Corte Cost., 24 marzo 1993,

Nello specifico, il percorso che ha portato il Giudice delle leggi a riconoscere esplicitamente il profilo passivo del diritto all'informazione ha avuto inizio con la sentenza n. 105 del 1972, in materia di riposo settimanale per gli addetti delle aziende editrici e stampatrici.

In questa pronuncia la Corte riconobbe l'importanza dell'informazione al fine di consentire la formazione di una pubblica opinione avvertita e consapevole.

Questo primo riconoscimento dell'importanza per i cittadini di potersi formare un'opinione critica fu poi ripreso dalla Corte in maniera più compiuta nella sentenza n. 94 del 1977, quando questa affermò che l'interesse generale della collettività all'informazione gode di una tutela implicita ed esplicita da parte dell'art. 21 della Costituzione.

Successivamente, con la sentenza n. 153 del 1987, in materia di trasmissioni radiotelevisive trasmesse su scala nazionale e gestite in regime di monopolio statale, la Corte pervenne a sostenere l'esistenza di un diritto all'informazione, affermando che nei confronti dei cittadini-utenti «lo Stato deve assicurare il diritto alla informazione, promuovendo appunto […] lo sviluppo sociale e culturale della collettività».[41]

Queste pronunce hanno, in sostanza, aperto la strada al riconoscimento espresso, da parte della Consulta nella sentenza n. 112 del 1993, del profilo passivo del diritto all'informazione come facente parte dell'alea di tutela assicurata dall'art. 21.

In quest'ultima pronuncia, infatti, la Corte Costituzionale affermò che «la Costituzione, all'art. 21, riconosce e garantisce a tutti la libertà di manifestare il proprio pensiero con qualsiasi mezzo di diffusione e che tale libertà ricomprende tanto il diritto di informare, quanto il diritto di essere informati».[42]

Tale interpretazione dell'articolo in questione è stata avallata anche da autorevole dottrina.[43]

Oreste Pollicino, nel suo scritto *La prospettiva costituzionale nell'era di Internet*, sostiene che il diritto di essere informati, ancorché non esplicitamente sancito

n. 112 in *consultaonline;* Corte Cost., 15 luglio 1976, n. 202 in *consultaonline;* Corte Cost., 14 luglio 1981, n. 148, in *consultaonline;* Corte Cost., 13 luglio 1988, n. 826 in *consultaonline*.

[41] Corte Cost., 13 maggio 1987, n. 153 in *consultaonline*, paragrafo 5.

[42] Corte cost., 24 marzo 1993, n. 112, in *consultaonline,* paragrafo 7.

[43] LOIODICE, voce *L'informazione (diritto alla)*, in *Enc. dir.*, XXI, Milano, m 1971, p. 472 e ss; POLLICINO, *La prospettiva costituzionale*, cit., p. 46 e ss.

dall'art. 21 della Costituzione italiana, entri a farne parte per il tramite dell'art. 11 della stessa.

Infatti, secondo l'Autore, essendo il diritto di essere informati sancito dall'art. 10 della CEDU, [44] esso forma implicitamente parte integrante dell'apparato costituzionale italiano.

In altre parole, tale orientamento, largamente prevalente in dottrina e in giurisprudenza, sostiene l'esistenza di un interesse costituzionalmente protetto a che le informazioni che circolano siano trasparenti e veritiere, donde la possibilità di intervenire sulle notizie che non presentano tali caratteristiche e che, quindi, non godono della tutela costituzionale.

Ancora, nel costituzionalismo italiano si è sviluppata una terza teoria a sostegno dell'esistenza di un profilo passivo della libertà di espressione nell'alea dell'art. 21. Si tratta di un filone di pensiero dottrinale che qualifica il diritto di essere informati come un "diritto aletico".

L'espressione diritti aletici deriva dal greco *aletheia*[45] e fa riferimento a quella categoria di diritti che concerne la verità, a un insieme di pretese che sono funzionali alla tenuta del sistema democratico.[46]

Nello specifico, con riferimento all'art. 21, autorevole dottrina[47] parla di un risvolto passivo della libertà di manifestazione del pensiero, in termini del diritto aletico di *essere informati in modo veritiero e di non essere ingannati o fuorviati.*[48]

Si ritiene dunque, che non solo il diritto di informare, ma anche il diritto di essere informati siano corollari dei valori propri dell'ordinamento democratico, in quanto la tenuta di tale regime dipende in larga parte dall'esistenza di un'opinione pubblica consapevole e informata.[49]

In conclusione, quale che sia l'approccio scelto, il testo dell'art. 21 della Costituzione italiana, se da una parte riconosce e tutela la libertà di espressione, dall'altra consente l'introduzione di forme di limitazione statuale della libertà di manifestazione del pensiero e di repressione dell'abuso di tale diritto.

---

[44] V. *infra* § 1.2.3.
[45] V. *infra* § 1.
[46] RODOTÀ, *Il diritto alla verità,* in Il diritto di avere diritti, Bari-Roma, 2012, pp. 211 e ss.
[47] MORTATI, *Istituzioni di diritto pubblico,* vol. II, Padova, 1976, p. 1069.
[48] FOÀ, *Pubblici poteri e contrasto alle fake news. Verso l'effettività dei diritti aletici?,* in *federalismi.it rivista di diritto pubblico italiano, comparato, europeo*, n 11/2020, p. 249.
[49] ZENCOVICH, *Il diritto di essere informati quale elemento del rapporto di cittadinanza, in il diritto dell'informazione e dell'informatica*, n. 22/2006, pp. 1 e ss.

Queste limitazioni trovano una giustificazione nella necessità di tutelare beni giuridici che siano parimenti garantiti dal testo costituzionale.
Nel caso di specie, il bene giuridico la cui tutela autorizza la limitazione della libertà di espressione, altro non è che l'interesse garantito dal profilo passivo del medesimo articolo.
Si tratta del diritto a un'informazione veritiera e non manipolata che consenta agli utenti di formarsi un pensiero critico; un diritto che deve essere soddisfatto con interventi positivi a opera dello Stato.[50]

1.2.2 *Fake news* nel costituzionalismo statunitense: il Primo Emendamento tra limiti e tutele

Passando ora all'analisi della tutela della libertà di espressione nel costituzionalismo americano, il primo emendamento stabilisce che «*Congress shall make no law […] abridging the freedom of speech, or of the press […]*».
Vediamo, dunque, come venga sancito in maniera quasi lapidaria il divieto per il Congresso di creare qualsiasi legge che limiti la libertà di parola o di stampa.
Si tratta di una disposizione eccezionale nel panorama delle democrazie liberali, in quanto essa fornisce alla libertà di parola una protezione così ampia da apparire quasi assoluta.
Nell'ordinamento costituzionale americano, infatti, il *freedom of speech* gode di una protezione cosiddetta *rafforzata*,[51] la quale si sostanzia nel divieto dei pubblici poteri di interferire con la libertà di parola in ogni sua declinazione.
Sin da qui, dunque, emerge la prima fondamentale differenza tra il primo emendamento e l'ordinamento costituzionale italiano.
Se, infatti, l'art. 21 consente allo Stato di bilanciare la tutela della libertà in esame con la protezione di altri beni giuridici parimenti costituzionalmente rilevanti, diversamente, il primo emendamento sembra escludere *a priori* la legittimità di qualsiasi intervento dei pubblici poteri sull'esercizio della libertà di espressione da parte dei cittadini.

[50] NICASTRO, *Libertà Di Manifestazione del Pensiero e tutela della personalità nella giurisprudenza della Corte Costituzionale*, in *CorteCostituzionale.it,* 2015, p. 4.
[51] PITRUZZELLA, POLLICINO, *Disinformation and Hate Speech a European Constitutial Perspective*, 2020 pp. 71-74.

In altre parole, il primo emendamento sembra far riferimento esclusivamente alla dimensione attiva del *freedom of speech*, mentre la tutela dell'art. 21 ricomprende anche il profilo passivo della libertà di manifestazione del pensiero.

L'ideologia alla base della concezione statunitense è perfettamente racchiusa dalla metafora del *free marketplace of ideas*, coniata dal giudice Holmes e poi ripresa dalla *Supreme Court* americana in molteplici pronunce. [52]

Il *free marketplace of ideas* è un libero mercato delle idee in cui ognuna di queste, per quanto scorretta o poco popolare, deve godere di pari tutela rispetto alle altre.

Tale paradigma poggia sull'assunto secondo cui la capacità di discernimento degli utenti li porta a sottoporre a giudizio critico i contenuti informativi, così che dal confronto delle idee sopravvivranno solo quelle realmente corrette e veritiere, senza necessità di un intervento esterno che impedisca la loro diffusione.

Dunque, l'intervento statale è visto non solo come superfluo, ma anche come profondamente dannoso per la tutela della libertà di manifestazione del pensiero.

Attualmente la possibilità per lo Stato di limitare la libertà di parola è circoscritta a pochi casi tassativi: frode, *obscenity*, diffamazione e incitamento all'odio.[53]

Nella specifica ipotesi della *defamation*, per altro, si applica la cosiddetta *Republican Rule*, la quale prevede che «*one who republishes a defamatory statements adopts it as his own, and is liable in equal measure to the original defamer*».[54]

Di conseguenza, qualora una *fake news* integrasse gli estremi della fattispecie della diffamazione, la responsabilità si estenderebbe non solo al creatore della stessa, ma anche a coloro che ri-condividerebbero tale informazione.

In altre parole, quindi, qualora una *fake news* integri gli estremi del reato di diffamazione, la *Republican Rule* punisce sia la disinformazione che la *misinformation*.

Infatti, la ri-condivisione di un contenuto altrui viene vista come un atto mediante il quale colui che agisce fa proprio il contenuto che pubblica sul *web*, a prescindere dalla sua consapevolezza o ignoranza della falsità della notizia.

---

[52] Dissenting opinion del Giudice Holmes al primo Emendamento; US SUPREME COURT, *Reno, attorney general of the united states, et al. v. American Civil Liberties Union et al*., 1997

[53] US SUPREME COURT, *United States v Alvarez*, 576 U.S., 2012, pp. 709,712.

[54] PARK, YOUM, F*ake news from a legal perspective: The United States and South Korea compared*, in *Southwestern Journal of International Law*, vol XXI, n. 1, 2019, p. 107; US COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT, *Liberty Lobby, Inc. v. Dow Jones e Co*., 823 F.2d (1988) pp. 1287, 1289.

Al di fuori del *numerus clausus* di ipotesi sopra menzionate, tuttavia, l'introduzione di nuove limitazioni della libertà di espressione è assai complessa e deve passare il cosiddetto *test* dello *strict scrutiny*.

Si tratta di un vaglio costituzionale in base al quale le limitazioni del *freedom of speech* saranno considerate legittime solo se tutelano un interesse fondamentale dello Stato e se sono strettamente necessarie allo scopo perseguito.[55]

Nel corso del tempo, soprattutto con riferimento a informazioni che circolano su Internet, vi sono stati dei tentativi di "comprimere" la tutela assicurata dal primo emendamento, come ad esempio il *Communication Decency Act* (CDA) del 1996 sui contenuti indecenti o manifestatamente offensivi.

Tuttavia, i vari tentativi non hanno mai superato lo *strict scrutiny test*.

Nel caso di specie, la *Supreme Court* affermò che la compressione del CDA del diritto alla libertà di espressione non era contenuta entro i margini di stretta necessità, in quanto le restrizioni imposte erano eccessivamente vaghe.

In generale, il costituzionalismo americano si è mostrato sempre poco propenso a una modifica, anche solo interpretativa, del primo emendamento.

Emblematiche, in tal senso, le parole del Professor Richard Haesen, il quale, in riferimento alla possibilità di una revisione della disposizione in questione, ha affermato: «*we do not want the cure to be wors than the disease*» [56].

L'affermazione secondo cui una modifica, anche meramente interpretativa, del primo emendamento costituirebbe una cura peggiore della "malattia", ossia della circolazione di *fake news* su Internet, fa immediatamente comprendere la rigidità del costituzionalismo americano nei confronti della libertà di espressione.

Ovviamente, anche nel panorama statunitense non mancano opinioni contrarie all'assolutezza della tutela del primo emendamento.

Coloro che abbracciano questa visione ritengono che la pressoché libera circolazione di *fake news*, e in particolare di disinformazione, su Internet lungi dal tutelare il libero scambio di idee, mini l'essenza stessa del *free marketplace of ideas*.

Nello specifico, tale corrente di pensiero, dopo aver definito i tre pilastri fondamentali del libero mercato, afferma che questi vengano sovvertiti dalla disinformazione.

---

[55] V. *infra* § 1.

[56] HASEN, *Cheap Speech and What it has done (to american democracy)*, vol. 16, in *first emendament, law Review*, 2017 pp. 200,202.

Per quanto concerne i tre principi fondanti del libero mercato delle idee,[57] questi sono descritti come:

1. Un costante confronto delle idee tra di loro;
2. La capacità e la volontà dei partecipanti al mercato di distinguere la verità dal *fake*;
3. La accidentalità della falsità.

Ebbene, analizzando tali pilastri, i sostenitori di un maggiore intervento statale a tutela del diritto alla verità sostengono che:

1. la polarizzazione impedisca agli utenti di beneficiare del costante confronto delle idee, in quanto questi recepiscono solo le informazioni provenienti dalla propria comunità virtuale e non quelle esterne e contrarie;
2. la capacità dei partecipanti al mercato di riconoscere il *fake* sia limitata dalla disinformazione, in quanto una volta che gli utenti ritengono vera una notizia falsa, è molto complesso dimostrare il contrario;
3. l'accidentalità della falsità sia smentita dal recente "*disinformation business*"[58], ossia un intero *business* di attori sul mercato che guadagno dalla creazione di *fake news*, che, ovviamente, diffondono volontariamente.[59]

Dunque, riassumendo, l'opinione minoritaria ritiene che, essendo la determinazione della verità l'obiettivo primario dell'intero *free marketplace of ideas*, non vi è motivo di permettere la circolazione di notizie false.[60]

Tuttavia, la Corte Suprema statunitense sembra abbracciare un'interpretazione decisamente rigorosa del primo emendamento, lasciando poco spazio a limitazioni della libertà di espressione e, conseguentemente, a divieti di circolazione di informazioni.

Vediamo, infatti, come già nel 1974,[61] la *Supreme Court*, dopo aver affermato che ai sensi del primo emendamento non esistono false idee, sostenne che a prescindere da quanto perniciosa possa essere un'idea, per la sua correzione bisogna fare

---

[57] NUÑEZ, *Disinformation legislation and freedom of expression*, in *UC Irvine Law Review*, vol. 10, issue 2, 2020, pp.787, 788.

[58] SOARES, *The fake news machine: inside a town gearing up for 2020*, in *cnn*, <https://money.cnn.com/interactive/media/the-macedonia-story/> [https;//perma.cc/VW93-G6AF].

[59] V. *infra* § 1.1.1.

[60] GREY, *The first amendment and the dissemination of socially worthless untruths*, in *Florida State University Law Review*, vol. 36, issue 1, 2008, p. 8.

[61] U.S. SUPREME COURT, *Gertz v Robert Welch*, Inc., 418 U.S (1974) pp. 323, 339-340.

affidamento non sulla coscienza dei giudici e delle giurie ma sul confronto con altre idee. In conclusione, la Corte sancì il principio per cui non vi è alcun valore costituzionale nelle affermazioni false.

L'importanza della tutela del primo emendamento fu poi rimarcata, nel medesimo caso, specificatamente anche dal giudice Justice Powell, il quale scandì a chiare lettere che il primo emendamento richiede la protezione di alcune falsità al fine di proteggere i discorsi che contano.[62]

Ancora, nel 1997, la Corte, dopo aver sostenuto che una regolazione statale della libera espressione del pensiero è più probabile che interferisca con il libero scambio di idee, piuttosto che lo incoraggi, sancì che l'interesse a incoraggiare la libertà di espressione in una società democratica prevale su qualsiasi beneficio teorico ma non provato della censura.[63]

Tale visione è stata poi confermata nel 2017 nel caso *Packingham v. North Carolina*.[64]

In questa pronuncia la Corte affermò molto chiaramente che la dottrina contenuta nel primo emendamento la guiderà nell'affrontare questioni attinenti alla libertà di espressione su Internet, consentendo, così, agli americani di sperimentare un democratico e libero scambio di idee anche in rete.

In conclusione, la risposta degli Stati Uniti alla creazione e diffusione capillare di *fake news* non sembra essere l'introduzione di limiti da parte dei pubblici poteri, in quanto questi vengono visti come l'inizio di un processo che porta alla *censorship*, ossia alla censura.

Infatti, l'opinione prevalente, tanto in dottrina quanto in giurisprudenza, ritiene che una compressione a livello statale della libertà di manifestazione del pensiero, trasformerebbe i cittadini in ricettori passivi di informazione, in quanto attribuirebbe al governo il ruolo di arbitro della verità, consentendogli di dare alle persone la propria ufficiale versione della verità. [65]

---

[62] *Ivi* p. 341.

[63] *Reno, attorney general of the united states, et al. v. American Civil Liberties Union et al*., 521 U.S., 1997, p. 844.

[64] U.S. SUPREME COURT, *Packingham v North Carolina*, 582 U.S., 2017, pp. 1730, 1736.

[65] CALVERT, VINING, *Filtering fake news through a lens of the supreme Court observations and adages*, in *UF Law Faculty Publications*, 2018, p. 174.

Piuttosto, il costituzionalismo americano propende per l'incoraggiamento all'utilizzo di siti creati appositamente al fine di confutare le *fake news*, come ad esempio *Polifact*.

1.2.3 Tutela internazionale ed europea della libertà di espressione

Nell'ambito del costituzionalismo europeo e internazionale, la libertà di manifestazione del pensiero ricopre una posizione centrale, assurgendo a baluardo di una società pluralistica e democratica.

Il riconoscimento della libertà di espressione, infatti, garantisce la tutela di molti altri diritti e libertà propri di ogni democrazia liberale; ad esempio il diritto alla partecipazione politica dei cittadini.

Tale garanzia trova il proprio presupposto fondamentale non solo nel diritto di esercitare attivamente la libertà di parola, ma anche nel diritto dei cittadini di ricevere informazioni veritiere che gli consentano di formarsi una opinione libera e informata.

Per quanto attiene all'ambito puramente internazionale, l'art. 19 *dell'International Convenant on Civil and Political Rights* (ICCPR) al secondo comma stabilisce che tutti hanno diritto alla libertà di espressione; questo diritto include la libertà di cercare, ricevere e diffondere informazioni e idee di ogni genere, sia oralmente che in forma scritta o per il tramite della stampa, in forma artistica o attraverso qualsiasi *media* a sua scelta, senza limiti di frontiera.

La precisazione secondo cui il diritto di espressione include tanto la libertà di ricevere informazioni, quanto quella di diffonderle rende immediatamente chiaro che la disposizione in esame tutela non solo il profilo attivo della libertà di manifestazione del pensiero, ma anche quello passivo.

In quest'ottica, in prima battuta si può già affermare che il costituzionalismo internazionale si avvicina maggiormente all'impostazione fornita dall'art. 21 della Costituzione italiana, come interpretato dalla dottrina e dalla giurisprudenza prevalenti, piuttosto che al primo emendamento americano.

La disposizione è, poi, completata dall'affermazione secondo cui l'esercizio del diritto previsto dal secondo comma porta con sé doveri e responsabilità speciali. Proprio alla luce di ciò, il terzo comma continua prevedendo la possibilità di

imporre delle restrizioni alla tutela della libertà di espressione, purché queste superino gli S*trict Tests of Proportionality and of Necessity*. [66]

In altre parole, le limitazioni della libertà di manifestazione del pensiero devono essere non solo previste dalla legge, ma anche proporzionali e necessarie alla protezione dei diritti e della reputazione altrui o alla tutela della sicurezza nazionale, dell'ordine pubblico, ovvero della salute e della morale pubblica.

Il requisito della proporzionalità richiede che le restrizioni riguardino un obiettivo specifico, non dovendo trattarsi solamente di un intervento indebito sui diritti altrui, e che vengano utilizzati gli strumenti meno invasivi tra quelli idonei a raggiungere l'obiettivo. [67]

Per quanto attiene al requisito della necessità, invece, questo viene considerato violato da una misura limitativa della libertà di espressione se sarebbe stato possibile proteggere il medesimo interesse senza imporre restrizioni della libertà in esame.[68]

Il tema della possibilità di limitare la libertà di manifestazione del pensiero al fine di contenere i fenomeni di manipolazione dell'informazione su Internet è stato oggetto specifico di una dichiarazione congiunta del Relatore Speciale delle Nazioni Unite per la libertà di opinione ed espressione, dell'OCSE e di un gruppo di esperti in materia nel 2017.

La *Joint Declaration on Freedom of Expression and Fake News, Disinformation and Propaganda*, conferma che, anche nell'ambito della lotta contro le *fake news*, la compressione del diritto di espressione è considerata legittima purché superi gli *strict tests* di *Proportionality* and *Necessity*. Al contrario, qualsiasi divieto generico, legge o regolamento basato su idee vaghe o ambigue deve essere abolito.[69]

È stato lo stesso David Kaye, nominato Relatore Speciale delle Nazioni Unite per la promozione e la protezione della libertà di opinione ed espressione nel 2014, ad affermare che le *fake news* sono diventate un problema globale e che è proprio la

[66] HUMAN RIGHTS COMMITTEE, *art 19: freedom of opinion and expression*, general comment n. 34, 12 settembre 2011, paragrafo 22.
[67] *Ivi*, paragrafo 34-35.
[68] *Ivi*, paragrafo 33.
[69] *Joint Declaration on Freedom of Expression and Fake News, Disinformation and propaganda*, Org. Sec and Co-operation Eur, 3 marzo 2017, paragrafo 2 (a) e ss.

dichiarazione congiunta in questione a identificare i principi generali che dovrebbero essere applicati nel fronteggiare tale problematica. [70]

Il perfetto anello di collegamento tra l'ottica internazionale e l'approccio europeo della libertà di manifestazione del pensiero è costituito dalla Convenzione Europea dei diritti dell'Uomo (CEDU).

L'art. 10, paragrafo 1, della CEDU prevede che «ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza considerazione di frontiera».

La concezione della libertà di manifestazione del pensiero cristallizzata in tale disposizione è stata oggetto di grande dibattito nel corso degli anni, sia a livello dottrinale che giurisprudenziale.

Invero, se da un lato la Convenzione riconosce espressamente sia il diritto di informare che il diritto di essere informati, avvicinandosi così al modello della democrazia militante, nonché all'approccio proprio dell'ICCPR; dall'altro, il prevedere il divieto di ingerenza da parte delle autorità pubbliche, sembrerebbe trasformare l'art. in questione in una consacrazione di un approccio proprio delle democrazie tolleranti.

Una prima interpretazione dell'art. 10 della CEDU è stata fornita dalla Corte stessa nel 1976 nel caso *Handyside v. Regno Unito*.

Secondo quanto affermato in tale pronuncia, la tutela assicurata dalla Convenzione alla libertà di espressione si estenderebbe non solo alle idee accolte in modo favorevole dalla collettività, ma anche a quelle espressioni che sono generalmente reputate offensive o scioccanti.

Dunque, la Corte Europea dei Diritti dell'Uomo in prima battuta ha ritenuto necessario interpretare la garanzia assicurata dall'art. 10 come pressoché "assoluta", al fine di tutelare i principi fondanti della democrazia, quali la libertà del dibattito politico, il pluralismo e la tolleranza.

Tuttavia, essendo la finalità primaria dell'art. 10 proprio la tutela dell'ordinamento democratico, appare inevitabile domandarsi come si collochi questa interpretazione estensiva rispetto al fenomeno delle *fake news*, che non comporta in alcun modo gli

[70] OHCHR, *Freedom of Expression Monitors Issue Joint Declaration on 'Fake News', Disinformation and Propaganda*, 2017.

effetti favorevoli propri della libertà di espressione né, tantomeno, giova alla democrazia liberale.

A tal riguardo, è fondamentale leggere l'art. 10 della CEDU in combinato disposto con l'art. 17, il quale vieta l'abuso dei diritti sanciti dalla Convenzione in funzione strumentale alla distruzione degli stessi. Il costituzionalismo internazionale ed europeo, quindi, richiede che si trovi un bilanciamento tra la tutela della libertà di espressione in senso ampio, e il divieto di abusare di questo diritto a scapito di altre libertà riconosciute dalla Convenzione.

Emerge, dunque, un'apertura verso la possibilità di limitare la libertà di espressione, oltre che nei casi espressamente indicati dal paragrafo 2 dell'art. 10, anche quando le modalità di manifestazione del pensiero integrano gli estremi di un abuso di tale libertà al fine di danneggiare diritti altrui.

Nello specifico, come anticipato, nel caso delle *fake news* il primo diritto danneggiato dall'abuso della libertà di espressione è il diritto all'informazione, ossia nient'altro che il profilo passivo dello stesso art. 10.

La preoccupazione della Corte per gli abusi di tale diritto è emersa per la prima volta nel 2007 con particolare riferimento ai contenuti giornalistici pubblicati su Internet. [71]

Nel caso di specie, la Corte fornì una prima risposta alle criticità che derivano dall'uso di Internet imponendo obblighi aggiuntivi per i giornali *on-line* e affermando che, in un mondo dove un numero sempre crescente di individui si confronta con grandi quantità di informazioni veicolate tanto per via tradizionali quanto attraverso i *media*, i controlli sul rispetto da parte dei giornalisti dei principi etici acquisisce una rinnovata importanza. [72]

La medesima preoccupazione fu poi specificata nella sentenza *Editorial board of Pravoye Delo e Shtekel c. Ucraina* del 2011.

In questa pronuncia la Corte EDU, affermando che «*the Internet might adversely affect other rights, freedoms and values*»,[73] mostrò esplicitamente il proprio timore

[71] Corte Europea dei Diritti dell'Uomo, *Stoll v Svizzera*, nr. 69698/01, 10 dicembre 2007.

[72] *Ivi*, paragrafo 104: "in a world where the individual is confronted with vast quantities of information circulated via traditional and electronic media and involving an ever-growing number of players, monitoring compliance with journalistic ethics take on added importance"

[73] Corte Europea dei Diritti dell'Uomo, *Editorial board of Pravoye Delo e Shtekel v Ukraina*, nr. 33014/05, 4 maggio 2011, paragrafo 30

per le violazioni di diritti fondamentali che posso derivare dalla condivisione di contenuti su piattaforme Internet.

Ecco, quindi, che l'approccio europeo si allontana dal paradigma statunitense del *free marketplace of ideas*, ritenendo necessaria la compressione della libertà di manifestazione del pensiero in un bilanciamento con la tutela di altri diritti parimenti garantiti dalla Convenzione.

Infatti, se il caso in questione può essere visto come il riconoscimento ufficiale da parte della Corte EDU dei danni che possono derivare dall'attribuzione alla libertà di espressione di una tutela assoluta, al contrario il caso statunitense sopra menzionato *ACLU v. Reno*[74] costituisce la più compiuta cristallizzazione del paradigma statunitense del *free marketplace of ideas*.

In conclusione, il convincimento della Corte EDU del maggiore grado di offensività delle tecnologie digitali rispetto ai mezzi di comunicazione tradizionali e della non assolutezza della libertà di manifestazione del pensiero, fa sì che il diritto in esame possa essere compresso genericamente quando il suo esercizio integra abusi, e più specificamente quando tali abusi si concretizzano in fenomeni manipolativi dell'informazione su Internet. [75]

La prospettiva non muta a livello dell'Unione Europea, dove la libertà di manifestazione del pensiero è sancita dall'art. 11 della Carta dei diritti fondamentali, con un testo molto simile a quello dell'art. 10 della CEDU.

Ai sensi della disposizione in questione, infatti, «ogni individuo ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera».

Ancora una volta, dunque, siamo di fronte a una disposizione che estende la tutela della libertà di espressione anche al profilo passivo di questa.

Per quanto attiene più specificamente alle *fake news*, l'Unione Europea negli ultimi anni ha elaborato numerosi documenti e rapporti in cui affronta il problema della

[74] V. *infra* § 1.2.2.

[75] FLAUSS, *The European Court of Human Rights and the Freedom of Expression*, in Indiana law journal, vol. 84, issue 3, 2009, p. 809.

disinformazione, e più genericamente dei fenomeni manipolativi del linguaggio, ipotizzando delle possibili soluzioni. [76]

Rimandando al capitolo 4 un'analisi approfondita di tali proposte, per quel che concerne la libertà di espressione, tali *Report* fanno emergere con chiarezza la propensione dell'Unione Europea a consentire una compressione del diritto in questione nel bilanciamento con la necessità di contrastare la circolazione di *fake news*.

Ancora, la preoccupazione dell'Unione per le violazioni dei diritti fondamentali che possono verificarsi su Internet emerge chiaramente dalla pronuncia sul caso *Google Spain*.[77]

Nella sentenza in questione, infatti, il fatto che la Corte abbia riconosciuto l'applicabilità degli obblighi previsti per chi tratta per proprio conto dati personali ai motori di ricerca, altro non è che una conferma della necessità di una regolamentazione della diffusione dei contenuti su Internet.

Dunque, l'Unione Europea integra perfettamente il paradigma delle democrazie militanti, abbracciando un approccio non dissimile a quello adottato dalla Corte Europea dei Diritti dell'uomo.

Mentre gli Stati Uniti d'America mantengono un approccio *sui generis*, tutelando esclusivamente il profilo attivo della libertà di espressione, diversamente le istituzioni europee ed internazionali adottano un paradigma piuttosto omogeneo e uniforme di tutela, bilanciando le esigenze di garanzia del profilo attivo e di quello passivo.

In conclusione, in ottica riassuntiva si può affermare che se da una parte il costituzionalismo europeo e internazionale elevano la libertà di espressione a baluardo dei valori propri della democrazia e del pluralismo, dall'altro essi riconoscono che è necessario consentire limitazioni del diritto in questione proprio al fine di assicurare lo sviluppo dello stesso ordinamento democratico.

---

[76] COMMISSIONE EUROPEA, *A multi-dimensional approach to disinformation, Report of the independent High-level Group on fake news and online disinformation,* 2018; COMMISSIONE EUROPEA, *Tackling online disinformation,* 7 luglio 2020.

[77] Corte di Giustizia dell'Unione Europea, *Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, Grande Sezione, 13 maggio 2014.

1.3 La qualità delle notizie nell'era del 4.0

Lo sviluppo di nuove tecnologie digitali ha dato origine alla cosiddetta *quarta rivoluzione industriale.*[78]

Tale espressione fa riferimento a un processo di compenetrazione del mondo fisico con quello digitale; all'insieme di progressi in materia di intelligenza artificiale, tecnologie computazionali, robotica, Internet delle cose e altre innovazioni.[79]

Con specifico riferimento all'industria dell'informazione, le tecnologie del 4.0 costituiscono *un'arma a doppio taglio* comportando tanti benefici quante criticità.

Partendo dai benefici, le innovazioni degli ultimi anni, l'avvento degli *smartphone* e dei *tablet*, così come l'incremento della capacità dei microprocessori sono tutti fattori che hanno contribuito a instaurare una connessione permanente tra utenti sul *web*, a ridurre i costi necessari per diffondere informazioni e ad aumentare vertiginosamente la quantità di dati che possono essere raccolti e immagazzinati.

Tuttavia, le nuove tecnologie portano con sé anche nuovi rischi: esse hanno aumentato la diffusione e l'efficacia delle *fake news*, comportando una conseguente riduzione nella qualità dell'informazione.

A tal proposito, prima di passare a un'analisi delle ragioni che motivano tale incremento appare necessario fornire una definizione di "qualità dell'informazione".

Secondo il paradigma fornito da Reuters nel 2017 la "qualità dell'informazione" si fonda su quattro direttrici: (1) l'accuratezza e l'affidabilità dei contenuti, (2) la capacità di essere d'ausilio per l'utente nella comprensione di argomenti complessi, (3) il potere di comunicare opinioni forti, e (4) l'abilità di trasmettere un contenuto accattivante. [80]

Appare, dunque, evidente che la qualità dell'informazione, intesa come il prodotto dell'intersezione di tali caratteristiche, e la diffusione di *fake news* non possono che essere inversamente proporzionali: all'aumentare dell'uno diminuisce l'altro, e viceversa.

---

[78] SCHWAB, *The fourth industrial revolution*, in world economic forum, Ginevra, 2016.
[79] *Ibidem*.
[80] NEWMAN,FLETCHER, KALOGEROPOULOS, LEVY, KLEIS NIELSEN, *Reuters Institute Digital News Report 2017*, in *Reuters institute for the study of journalism*, p. 22-23.

1.3.1 I fattori che hanno determinato l'incremento delle *fake news*

Passando ora all'analisi dei fattori che hanno determinato la nuova efficacia acquisita dalle *fake news,* sussistono tre ragioni fondamentali che spiegano tale fenomeno.

Anzitutto, poiché con l'avvento di Internet chiunque può facilmente inserire informazioni in rete, si è venuto a creare un sistema di produzione dell'informazione radicalmente decentralizzato; a tal riguardo, basti pensare alla rapidità di condivisione consentita dai *social media* attraverso i meccanismi del *retweet e repost.* [81]

Di conseguenza, essendo venute meno le barriere all'ingresso proprie dell'industria dell'informazione tradizionale, l'assenza di meccanismi di controllo aumenta le probabilità che le *fake news* vengano create e diffuse in rete.

Gli effetti di questa mancanza di supervisione sono ulteriormente aggravati dal fatto che, mentre un tempo i quotidiani seguivano dei cicli di 24 ore producendo una nuova versione ogni giorno, oggi Internet consente un ciclo di produzione senza soluzione di continuità.

Di conseguenza, non solo gli articoli possono essere pubblicati e modificati continuamente nel corso della giornata, ma è anche aumentata la competizione tra le singole testate giornalistiche; invero, nessun giornale o sito può attendere 24 ore per pubblicare una notizia.

Uno studio dimostra che una notizia pubblicata *online* da una testata giornalista in media viene ripubblicata da altri siti entro 2 ore, ma nella metà dei casi ciò avviene in meno di 45 minuti, e nel 25% dei casi in meno di 5. [82]

È evidente, dunque, che la rapidità con cui si muove il sistema di produzione dell'informazione lascia decisamente poco spazio per il controllo di qualità e per il cosiddetto *fact-checking*.

Da ciò discende che, non solo è più probabile che una *fake news* sfugga al controllo e venga pubblicata, ma, poiché una volta pubblicata questa sarà ri-condivisa da altri giornali, aumenta anche la sua credibilità agli occhi dei lettori.

---

[81] NUÑEZ, *Disinformation legislation and freedom of expression*, cit., p. 786.

[82] CAGE, HERVE, VIAUD, *The Production of Information in an Online World*, in *NetInstitute.org*, working paper n. 2015/05.

La seconda ragione che motiva l'incremento della diffusione di *fake news* risiede nel ruolo ricoperto dai *social media*.

Infatti, grazie a questi i siti *web* riescono a incrementare il proprio traffico e a diffondere notizie senza dover sopportare i costi propri dei media tradizionali.

Nello specifico, per i siti, anche *fake,* è sufficiente che una piccola parte degli utenti che leggono l'articolo su un *social* clicchino su questo e accedano al loro sito.

Mediante tale meccanismo, dunque, si crea un rapporto di dipendenza del sito nei confronti del *social media*.

Prendendo a esempio *Facebook,* in prima battuta questa piattaforma fornisce a tutti i siti la possibilità di espandere il proprio raggio d'azione rinviando a questi il proprio traffico *web*.

In tal modo, si crea il meccanismo di dipendenza sopra menzionato: da una parte i siti forniscono al *social media* un flusso di informazioni che interessa gli utenti, dall'altra *Facebook* incrementa notevolmente il loro traffico.

Dunque, grazie a tale meccanismo, gli articoli pubblicati dai siti acquistano una risonanza infintamente più elevata in un lasso di tempo molto ridotto.

A tal riguardo è interessante notare che uno studio del 2018 dimostra che attraverso i *social media* una notizia *fake* si diffonde addirittura fino a sei volte più velocemente di un contenuto vero.[83]

Da ciò discende che, grazie al ruolo ricoperto dai *social media* non solo è più facile diffondere *fake news*, ma, non essendoci un vero e proprio un controllo della fonte da parte degli utenti, è anche più probabile che queste siano reputate come informazioni attendibili.

Infine, l'efficacia delle *fake news* viene amplificata dal fatto che gli algoritmi utilizzati dai motori di ricerca e dalle piattaforme *social* consentono di personalizzare le ricerche che gli utenti effettuano sul *web*.[84]

Di conseguenza, gli utenti pur avendo in linea teorica accesso a una quantità pressoché infinita di fonti di informazione, in realtà visualizzano quasi esclusivamente *post* e articoli conformi alle proprie opinioni e credenze.

---

[83] DIZIKES, *study: on twitter, false news travels faster than true stories*, in *MIT News*, 2018; VOSOUGHI, ROY, ARAL, *the spread of true and false news online*, in *Science*, 2018, pp. 1146 e ss.

[84] PRAISER, *Filter Bubble: how the new personalized web is changing what we read and we think*, New York, 2011

Per effetto di questo, gli utenti, chiusi nella loro bolla virtuale, sono sempre più propensi a credere ai contenuti che circolano all'interno di questa, anche qualora questi fossero *fake*. In altre parole, si tratta del sopra citato fenomeno della *filter bubble*.[85]

A tal riguardo, è interessante notare che, a seguito delle elezioni americane del 2016, il grado di compatibilità delle notizie condivisa su Internet con le opinioni e le preferenze dell'utente è stato considerato indice della qualità delle notizie stesse[86].

Vediamo, dunque, come la personalizzazione dei contenuti venga vista sempre di più come una caratteristica fondamentale dell'industria dell'informazione.

Tuttavia, se da un lato questo meccanismo porta con sé dei vantaggi evidenti, consentendo agli utenti di visualizzare contenuti che reputano interessanti con maggiore agilità, dall'altro esso rende molto più complesso non solo contenere il dilagare delle *fake news*, ma anche dimostrare la non veridicità di una notizia una volta che questa è stata messo in rete.

In conclusione, se è vero che le "bufale" non sono nate in anni recenti, nondimeno è innegabile che l'avvento di Internet ha innescato una crescita esponenziale del fenomeno delle *fake news*, comportando una consequenziale drastica diminuzione della qualità dell'informazione.

Alla luce di ciò, risulta quanto mai attuale l'affermazione della Corte Europea dei Diritti dell'Uomo secondo cui «*the risk of harm posed by the content and communications on the internet to the exercise and enjoyment of human rights and freedoms, […] is certainly higher than that posed by the press*».[87]

1.3.2 La formazione mediale della realtà: il caso *Blue Whale*

Una volta analizzati i motivi che determinano l'incremento dell'efficacia delle *fake news*, risulta interessante indagare gli effetti provocati da tale incremento.

I *media* ricoprono da sempre un ruolo decisivo nella formazione mediale della realtà.

---

[85] V. *infra* § 1.

[86] Gentzkow et al. (2016)

[87] Corte Europea dei Diritti dell'Uomo, *Editorial board of Pravoye Delo e Shtekel v Ukraina*, n. 33014/05, 4 maggio 2011, par. 63.

Essi, infatti, non si limitano a selezionare e "raccontare" temi di interesse, bensì svolgono un contributo determinate nella creazione di quell'insieme di contenuti, immagini, forme di interazione tra utenti e credenze comuni sulla base dei quali prende forma il sistema sociale;[88] in altre parole, i *media* plasmano la realtà sociale in cui viviamo.

A tal riguardo, un caso emblematico di formazione mediale della realtà è costituito dalla vicenda della Guerra dei Mondi del 1938.

Con questa espressione si fa riferimento al panico collettivo che si generò negli Stati Uniti a seguito di un episodio della trasmissione radiofonica *Mercury Theatre on the Air*. La puntata in questione, basandosi sull'omonimo romanzo di W. G. Wells, narrava in forma romanzata l'invasione della terra da parte dei marziani. Il racconto fu così realistico che fu stimato che il 28 % degli ascoltatori pensò che fosse un programma di informazione giornalistica.[89]

Da ciò derivò il panico generalizzato che si diffuse tra quella parte della popolazione che era convinta che l'invasione aliena fosse un reale e imminente pericolo.

Questo fenomeno venne studiato dal celebre psicologo H. Cantril nel 1940, il quale condusse la propria analisi prendendo come punto di partenza il controllo delle fonti da parte degli ascoltatori.

Da tale ricerca emerse che la porzione di *audience* tra cui si generò il panico era formata in gran parte da coloro che non avevano svolto un controllo né sulla coerenza interna né su quella esterna del contenuto della trasmissione[90]. In altre parole, si trattava di quella parte degli ascoltatori che si era affidata ciecamente a quanto raccontato, ignorando la credenza comune circa l'inesistenza dei marziani così come l'assenza di prove a sostegno della loro esistenza e dell'imminente invasione.

Riportando tale studio all'epoca moderna, o più precisamente all'era del 4.0, il processo di formazione mediale della realtà diviene ancora più reale e preoccupante.

---

[88] GIACCARDI, *Media, Significato e Realtà Sociale: per un approccio comparativo all'analisi dei testi pubblicitari,* in *Vita e Pensiero*, 1993, pp. 283-297.

[89] CANTRIL, *The Invasion from Mars*, in *Princeton Legacy Library*, 1982.

[90] BENNATO, *L'emergere della disinformazione come processo socio-computazionale, Il caso Blue Whale*, in *Problemi dell'Informazione*, dicembre 2018, pp. 394-398.

Uno studio condotto da Reuters nel 2017, infatti, mostra che meno della metà degli utenti intervistati sono stati in grado di ricordare la fonte originaria da cui derivava l'articolo che avevano letto su un *social media*[91].

Dunque, se all'incremento nell'efficacia delle *fake news* si aggiunge anche un bassissimo livello di controllo delle fonti, non può che generarsi un reale rischio che notizie manipolate diventino parte integrante dell'opinione pubblica e si trasformino, così, in realtà.

Un perfetto esempio di creazione mediale della realtà ci è fornita dal caso noto come *Blue Whale.*

Si tratta di un *reportage* pubblicato sul giornale russo Novaya Gazeta che racconta di 130 suicidi avvenuti tra novembre 2015 e aprile 2016 in numerose città russe. Si parla di un "curatore" che contattando gli adolescenti sui *social media* li guida attraverso 50 prove, l'ultima delle quali è lanciarsi dal tetto di un grattacielo.

Il primo giornale italiano a riprendere l'inchiesta russa fu La Stampa il 3 giugno 2016[92]; successivamente tra febbraio e marzo del medesimo anno la notizia venne pubblicata anche da numerosi altri giornali italiani tra cui la Repubblica e il Messaggero.

In sostanza, però, si può affermare che il caso in questione entrò a far parte dell'opinione pubblica italiana con l'inchiesta giornalistica di Matteo Viviani per conto di Le Iene il 14 maggio del 2016.

Il *reportage* riguardava il suicidio di un adolescente avvenuto a Livorno, e lo ricollegava allo schema del *Blue Whale.*

Questa inchiesta poi si rivelò una "bufala" basata su informazioni di seconda mano, racconti dei genitori dei ragazzi, video manipolati e un'intervista a un tale "Filip Liss", successivamente identificato come Philip Budeikin, ossia uno dei presunti curatori.

Lo stesso giornalista si corresse qualche tempo dopo affermando che i video erano falsi[93]; purtroppo, però, nel frattempo quella che era nata come una *fake news* era diventata realtà.

---

[91] NEWMAN, FLETCHER, KALOGEROPOULOS, LEVY, NIELSEN, *Reuters Institute Digital News Report 2017*, cit., pp. 22-23.

[92] ZAFESOVA, *Istigazioni 'social' al suicidio, panico in Russia per le chat della morte. Ma è solo un brutto scherzo*, in *LaStampa*, 4 giugno 2016.

[93] LUCARELLI, *Blue Whale, parla Matteo Viviani de Le Iene: "Sì, i video russi sono falsi ma il pericolo c'è"*, in *il fatto quotidiano*, 7 giugno 2018.

Nell'intervista di Selvaggia Lucarelli per il Fatto Quotidiano si legge «prima del servizio zero casi dopo forse sì. Soltanto emulazione?», e ancora «La sera in cui il servizio è andato in onda, sul web c'è stata una reazione forte. Da quel momento, caso strano, sono cominciati casi su casi di Blue Whale in Italia».

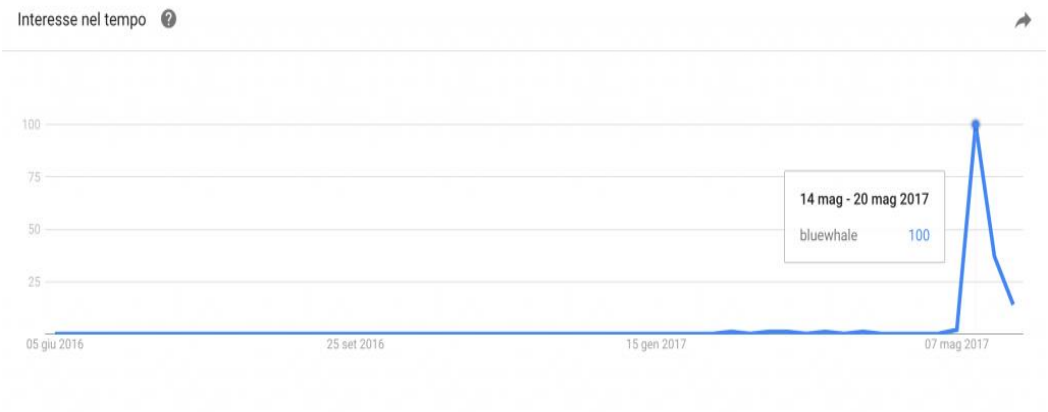
Addirittura il dirigente polizia di Stato della direzione Anticrimine Mancini ha affermato che dopo il video de Le Iene sono arrivate segnalazioni riguardanti adolescenti irretiti dal presunto *gioco* della *Blue Whale*.[94]

Dunque, siamo di fronte a un caso in cui una *fake news* che ha inciso a tal punto sulla formazione della realtà, da divenire essa stessa reale.

Il concretizzarsi di tale fenomeno può essere spiegato prendendo in considerazione il combinato disposto dell'inchiesta di Viviani con la personalizzazione del *web*.

Il funzionamento degli algoritmi alla base dei motori di ricerca e delle piattaforme *social* si fonda sul meccanismo della *filter bubble,* per cui l'utente che cerca un'informazione vede tendenzialmente confermata la propria opinione. Ad esempio, nei giorni successivi cercando sul motore Google i termini *Blue Whale* automaticamente uscivano parole quali: regole, gioco, regole del gioco, sfide.[95]

Inoltre, a tal riguardo è interessante notare come dopo il 14 maggio 2016, vi è stato un picco dell'uso dell'espressione *Blue Whale* nelle ricerche di Google.[96]



Lo stesso è accaduto sui *social media*, dove a partire dalla metà di maggio 2016 vi è stata un'esplosione nell'utilizzo dell'*hashtag* #curatorfindme.

[94]TORRISI, ZITELLI, *Blue Whale: la leggenda urbana, gli errori delle Iene e come i media dovrebbero parlare di suicidio,* in *Valigia Blu,* 3 giugno 2017.
[95] Secondo il servizio Google *autocomplete* in lingua italiana a maggio 2017.
[96] TORRISI, ZITELLI, *Blue Whale: la leggenda urbana, gli errori delle Iene e come i media dovrebbero parlare di suicidio,* cit.

Dunque, il *reportage* basato su fonti non attendibili unito ai meccanismi della *filter bubble* e alla personalizzazione delle ricerche ha generato un'ondata di comunicazione ed emulazioni, trasformando una *fake news* in realtà. [97]

Concludendo, appare evidente come divenga progressivamente più complesso distinguere una notizia vera da una falsa e come, al contempo, le notizie manipolate si diffondano sempre di più e sempre più rapidamente, diminuendo la qualità dell'informazione.

L'effetto generato da questi meccanismi è che vi è una sempre maggiore formazione mediale della realtà, spesso generata da *fake news*.

Alla luce del panorama sopradescritto, appare, dunque, opportuno analizzare le fattispecie di reato astrattamente integrabili nel nostro ordinamento dalla diffusione di *fake news on-line.*

[97] PITRUZZELLA, POLLICINO, QUINTARELLI, *Parole e Potere, Libertà di Espressione, Hate Speech e Fake News,* cit., p. 128.

CAPITOLO II

II. *FAKE NEWS* E DIRITTO PENALE ITALIANO

2. *Fake News* e i Reati astrattamente configurabili

Nell'approccio alla trattazione della regolamentazione dei fenomeni manipolativi dell'informazione, è preliminarmente necessario affrontare la problematica relativa alla concezione della verità quale possibile oggetto di tutela penale.

Come analizzato nel capitolo precedente[98], la nozione stessa di verità si è evoluta nel corso del tempo: il concetto di "verità oggettiva" proprio degli anni '80, si è tramutato in un'idea di "verità relativa" quale corrispondenza tra accaduto e narrato, fino a giungere, nell'attuale era della Post-Verità, a una nozione di verità quale rispetto del «nucleo essenziale del fatto» [99].

Con riferimento all'attuale sistema punitivo italiano, uno specifico obbligo di verità può configurarsi solamente rispetto a fattispecie che incriminano espressamente una condotta di falso. Di conseguenza, l'incriminazione della diffusione di *fake news* è necessariamente correlata all'idoneità della condotta dell'agente a ingannare o a causare l'inganno. In altre parole, nel vigente codice penale italiano la verità non viene mai tutelata in quanto bene giuridico protetto in via diretta, bensì sempre in quanto strumentale rispetto alla tutela di quegli interessi ulteriori che possono essere lesi dalla condotta di falso tipizzata nella norma[100].

Come sarà affrontato più nel dettaglio nei paragrafi successivi, sarebbe tuttavia erroneo ritenere che l'avvento di Internet e dei *social media* abbia reso gli strumenti tradizionali del diritto penale inidonei a fronteggiare le nuove istanze di tutela. Al contrario, la pressoché totalità dei casi di diffusione di notizie false o manipolate ad oggi può essere ricompresa in una delle fattispecie tipizzate dal nostro codice penale. Semmai, con riferimento a tali previsioni, il problema che si pone è la necessità di adeguarle alle peculiarità di quelli che sono stati definiti i nuovi reati di «comunicazione orizzontale» (ossia della *mass self-comunication*)[101], ad

---

[98] V. *supra* Cap. I

[99] FUMO, *Bufale elettroniche, repressione penale e democrazia*, in *Media Laws*, 2018, 87.

[100] PERINI, *Fake news e Post-Verità tra diritto penale e politica criminale*, in *Dir. pen. cont.*, 20 dicembre 2017.

[101] CASTELLS, *Comunicazione, potere e contro-potere nella network society* in <http://www.caffeuropa.it/socinrete/castells.pdf>, p. 2.

esempio inasprendo le sanzioni al fine di aumentarne la capacità dissuasiva delle stesse,[102] ovvero fornendone un'interpretazione evolutiva.

Ciò detto, nei paragrafi successivi verranno analizzate alcune tra le fattispecie penali astrattamente configurabili in ipotesi di diffusione di *fake news on-line*, nello specifico saranno affrontati: il reato di pubblicazione o diffusione di notizie false, esagerate o tendenziose, atte a turbare l'ordine pubblico; il reato di diffamazione; il reato di procurato allarme presso l'autorità e il reato di sostituzione di persona.

2.1. Il reato di pubblicazione o diffusione di notizie false, esagerate o tendenziose, atte a turbare l'ordine pubblico

Lo studio delle fattispecie integrabili dalla creazione e diffusione di *fake news on-line* non può che partire dalla norma di carattere generale contenuta nell'art. 656 c.p., rubricato «Pubblicazione o diffusione di notizie false, esagerate o tendenziose, atte a turbare l'ordine pubblico».

Ai sensi di tale disposizione «chiunque pubblica o diffonde notizie false, esagerate o tendenziose, per le quali possa essere turbato l'ordine pubblico, è punito, se il fatto non costituisce un più grave reato, con l'arresto fino a tre mesi o con l'ammenda fino a euro 309».

Da una prima analisi letterale del testo della disposizione appare immediatamente evidente come questa norma rientri tra quell'insieme di disposizioni in cui il bene giuridico tutelato non è la verità della notizia in quanto tale, bensì un interesse ulteriore, che, nel caso di specie, è rappresentato dall'ordine pubblico.

Nella formulazione originaria del codice Rocco, l'art 656 c.p. era volto a criminalizzare l'espressione di pensieri politici contrari al regime fascista[103], assumendo così i tratti di una disposizione limitativa della libertà di manifestazione del pensiero.

In ragione di tale natura, la Corte Costituzionale, chiamata a più riprese a pronunciarsi sulla legittimità di tale norma, ha sempre confermato la costituzionalità della disposizione, fornendone un'interpretazione evolutiva diretta a rendere il reato in questione compatibile con l'impianto democratico e pluralistico

[102] COSTANTINI, *Diritto penale e libertà di espressione in Internet*, in *Dir. pen. cont. – Riv. Trim*, 2/2019, p. 70.
[103] COSTANTINI, *Diritto penale e libertà di espressione in Internet*, cit., p. 64.

proprio del nostro ordinamento giuridico. Nello specifico, nella sentenza n. 19 del 1962 la Corte, dopo aver definito l'espressione notizie false, esagerate e tendenziose come «una forma di endiadi, con la quale il legislatore si è proposto di abbracciare ogni specie di notizie che, in qualche modo, rappresentino la realtà del mondo alterato», ha precisato che il termine tendenziose fa riferimento a quelle notizie «che, pur riferendosi a cose vere, le presentino tuttavia in modo che chi le apprende possa avere una rappresentazione alterata della realtà»[104].

Alla luce di tale affermazione si può, dunque, dedurre che la ampia nozione di diffusione di notizie false, esagerate o tendenziose, almeno in astratto, non ponga ostacoli all'applicazione dell'art. 656 c.p. alla propagazione di *fake news on-line*, purché, ovviamente, queste integrino una minaccia all'ordine pubblico.

Infatti, come affermato dalla stessa Corte Costituzionale, nell'ambito della disposizione in esame, la diffusione di notizie false assume il connotato di elemento giustificativo della limitazione della libertà di espressione solamente qualora questa si identifichi con una minaccia all'ordine pubblico, inteso quale «ordine legale su cui poggia la convivenza sociale»[105].

Sulla medesima scia di pensiero, con riferimento alle possibili limitazioni del diritto di cui all'art. 21 della Costituzione, la Corte ha inoltre statuito che «la garanzia dei diritti inviolabili dell'uomo diventerebbe illusoria per tutti, se ciascuno potesse esercitarli fuori dell'ambito delle leggi, della civile regolamentazione, del ragionevole costume. Anche diritti primari e fondamentali […] debbono venir contemperati con le esigenze di una tollerabile convivenza». In questo senso, la tutela dell'ordine pubblico assurge a legittima limitazione della libertà di pensiero, dovendo questo essere inteso quale «ordine pubblico costituzionale […] che deve essere assicurato appunto per consentire a tutti il godimento effettivo dei diritti inviolabili dell'uomo»[106].

Ne consegue che, qualora le *fake news* diffuse *on-line* siano idonee a turbare l'ordine pubblico, integrando gli estremi di notizie false, esagerate o tendenziose, nulla impedisce l'applicazione della fattispecie incriminatrice di cui all'art. 656 c.p.

---

[104] Corte cost., 16 marzo 1962, n. 19, in *giurcost.org.*

[105] Corte cost., 23 giugno 1956, n. 2, in *giurcost.org;* Corte cost., 18 marzo 1962, n. 19, in *giurcost.org.*

[106] Corte Cost., 8 luglio 1971, n. 168, *giurcost.org.*

Con specifico riferimento alla diffusione di *fake news*, inoltre, assume particolare rilevanza la circostanza che la disposizione in esame integri un reato contravvenzionale, che, quindi, potrà essere punito sia a titolo di dolo che a titolo di colpa. Nel secondo caso, dunque, non avrà rilevanza né l'errore sulla veridicità della notizia diffusa – eccezion fatta per le ipotesi di errore scusabile – né le motivazioni che hanno indotto il soggetto a diffondere la notizia.

Di conseguenza, in tema di fenomeni manipolativi dell'informazione, risulta indifferente quale tra gli scopi astrattamente perseguibili mediante la diffusione e pubblicazione di *fake news* stesse perseguendo l'utente[107], purché sia integrato il requisito della minaccia al turbamento dell'ordine pubblico.

Appare, inoltre, opportuno sottolineare che, essendo l'art 656 c.p. un reato di pericolo, ai fini della sua configurazione è sufficiente un'astratta possibilità che si verifichi un turbamento dell'ordine pubblico; non assumendo, al contrario, rilevanza che di fatto non si sia verificato alcun turbamento[108].

Ciò detto, il primo limite alla perseguibilità penale della diffusione *di fake news* ai sensi dell'art. 656 c.p. è costituito proprio dalla difficoltà dell'accertamento della effettiva, se pur astratta, idoneità della notizia falsa o manipolata a causare un turbamento dell'ordine pubblico.

A tale criticità si aggiunge una seconda problematica che deriva dalla necessità di escludere dalla tutela fornita dall'art. 656 c.p. le «interpretazioni, valutazioni, commenti, ideologicamente qualificati, e persino tendenziosi, relativi a cose vere»[109]. Se pur in un'ottica di bilanciamento tra tutela dell'ordine pubblico e la garanzia della libertà di pensiero tale esclusione appare legittima e ragionevole, tuttavia l'opinabile discrezionalità del confine tra mere interpretazioni tendenziose e vere e proprie *fake news*, genera una situazione di incertezza giuridica[110], minando così l'efficacia della tutela assicurata dall'articolo in esame. Questo appare quanto mai vero e preoccupante con riguardo alla diffusione di *fake news on-line*, dove il confine tra commenti, opinioni e 'bufale' è sempre più labile e dubbio.

In conclusione, pur essendo la tutela assicurata dalla fattispecie di cui all'art. 656 c.p. astrattamente e potenzialmente idonea a ricomprendere il fenomeno della

---

[107] V. *supra* Cap. I § 1.1.1.

[108] Cass. pen, Sez. I, 7 novembre 1996, n. 9475, in *Pluris*; Cass, pen., 4. Febbraio 1976, in *Cass. Pen. Mass.ann*., con nota di MULLIRI, p. 735.

[109] Cass. pen, Sez IV, 11 gennaio 1977, n. 3967, in *riv. En*, p. 463.

[110] FUMO, *Bufale elettroniche, diritto penale e democrazia,* cit., p. 88.

diffusione di *fake news* sul *web*, nella pratica il testo della norma presenta evidenti problematiche che la rendono facile oggetto di abusi limitativi della libertà di pensiero[111].

2.2. Il reato di diffamazione

Ai sensi del primo comma dell'art. 595 c.p. «chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a euro 1.032».

Anche in questo caso, la disposizione in esame rientra tra quelle norme che tutelano la verità solo in quanto strumentale alla protezione di un bene giuridico ulteriore, vale a dire, in questo caso, la reputazione, intesa quale dignità della persona in un determinato ambito sociale[112].

In particolare, il concetto di offesa richiamato dalla norma in esame comprende qualsiasi espressione infamante, considerata tale tenuto conto non soltanto del suo significato esplicito, ma anche del contesto in cui viene diffusa. In tal senso si è pronunciata la Corte di Cassazione affermando che «*integra la lesione della reputazione altrui non solo l'attribuzione di un fatto illecito, perché posto in essere contro il divieto imposto da norme giuridiche, assistite o meno da sanzione, ma anche la divulgazione di comportamenti che, alla luce dei canoni etici condivisi dalla generalità dei consociati, siano suscettibili di incontrare la riprovazione della communis opinio*»[113].

Infatti, ai fini della integrazione del reato di diffamazione risulta irrilevante che l'espressione offensiva sia veritiera o meno[114], rilevando esclusivamente l'idoneità di questa a ledere la reputazione del soggetto passivo. Al contrario, la falsità della notizia, tutto al più, preclude all'autore del reato la possibilità di avvalersi della *exceptio veritatis*, nelle circostanze in cui è ammessa la prova liberatoria basata sulla verità del fatto, *ex.* art. 596 c.p., nonché di invocare la scriminante di cui all'art. 51 c.p., in particolare per quel che concerne l'esimente del diritto di cronaca.

---

[111] COSTANTINI, *Diritto penale e libertà di espressione in Internet*, cit., p. 65

[112] GULLO, *Diffamazione e legittimazione all'intervento penale, Contributo a una riforma dei delitti conto l'onore,* Roma, 2013, pp. 11 e ss; GULLO, *Delitti contro l'onore,* in PIERGALLINI-VIGANÒ, (a cura di), *Reati contro la persona*, Estratto dal VII volume del *Trattato teorico-pratico di diritto penale*, diretto da PALAZZO-PALIERO, Torino, 2015, pp. 189 e ss.

[113] Cass. pen., Sez. V, 29 ottobre 2008, n. 40359, in *www.pluris.it.*

[114] PADOVANI, *Menzogna e diritto penale,* Pisa, 2014, p. 273.

2.2.1. Il reato di diffamazione *on-line*

Tanto premesso in via generale, occorre precisare che l'applicabilità dell'art. 595 c.p. alla diffusione e pubblicazione su Internet di contenuti diffamatori è stata ampiamente riconosciuta dalla giurisprudenza.

Nello specifico, recente giurisprudenza ha ritenuto che la pubblicazione di offese personali su articoli *web* o *social network* integri l'aggravante dell'uso di un qualunque altro mezzo di pubblicità diverso dalla stampa, di cui all'art. 595 comma III[115]. Costituisce, infatti, ormai *ius receptum*[116] l'impostazione stabilita dalla giurisprudenza di merito, e avallata dalla giurisprudenza di legittimità, secondo cui una notizia pubblicata o diffusa su Internet possiede intrinsecamente quella potenziale capacità di raggiungere un numero indeterminato o quantitativamente elevato di persone, richiesta dalla norma per la configurazione dell'aggravante in esame[117].

Sul tema la Corte di Cassazione ha affermato che nell'ipotesi di diffamazione commessa tramite internet, la particolare capacità diffusiva del mezzo utilizzato per far circolare il messaggio denigratorio renda l'autore meritevole di un trattamento sanzionatorio più severo, e, quindi, che si possa configurare il delitto di diffamazione aggravata di cui al terzo comma dell'art. 595 c. p[118].

Inoltre, secondo quanto affermato dal Tribunale di Pescara nel 2018 «La pubblicazione di frasi o immagini diffamatorie sulla piattaforma *social* "Facebook" costituisce un ambito quantitativamente apprezzabile ed ampiamente sufficiente ad integrare l'elemento oggettivo del reato di diffamazione, il che vale configurare l'ipotesi aggravata di cui al comma terzo dell'art. 595 c.p. poiché trattasi di condotta potenzialmente idonea a raggiungere un numero indeterminato o comunque quantitativamente apprezzabile di persone»[119].

---

[115] V *infra* Cap II § 2.2.2.

[116] Cass., Sez. I, 22 gennaio 2014 n. 16712, con nota di TURCHETTI, *Diffamazione su Facebook: comunicazione con più persone e individuabilità della vittima*, in *Dir. pen. cont.*, 8 maggio 2014.

[117] Cass. pen. Sez. I, 28 aprile 2015, n. 24431, in *www.pluris.it*

[118] Cass. pen. Sez. V. 11 giugno 2010, n. 30065, in *www.dejure.it.*

[119] Tribunale Pescara, 5 marzo 2018, n. 652, in *www.dejure.it.*

D'altronde è la stessa definizione di *social network* che suggerisce, quale caratteristica intrinseca e necessaria di queste piattaforme, proprio l'instaurazione di «una trama di relazioni tra più persone all'interno dello stesso sistema»[120].

E ancora, il Tribunale di Bari ha ritenuto che costituisse reato *ex.* art. 595 comma III c.p. la creazione di un sito internet di fantasia contenente immagini di stampo erotico, al quale venga associato il nome e il numero telefonico di una persona realmente esistente[121].

Dunque, appare evidente che la *ratio* alla base dell'estensione della tutela accordata dall'art. 595 c.p. alla diffamazione *on-line* risieda proprio nella maggiore capacità di diffusione dei mezzi di comunicazione dell'era della Post-Verità, e quindi nel maggiore pericolo a cui è esposto il bene giuridico della reputazione[122].

Inoltre, essendo la diffamazione un reato di evento che si consuma nel momento e nel luogo in cui terze persone percepiscono l'offesa, la giurisprudenza più recente[123] ha stabilito che la sussistenza del requisito della pluralità dei percettori di messaggi diffamatori sia da ritenersi presunta qualora le espressioni siano pubblicate su un *sito web*. Infatti, essendo quest'ultimo per propria natura intrinseca destinato ad essere visitato da un numero indeterminato di utenti, in maniera non dissimile dal caso di un tradizionale giornale cartaceo, a nulla rileva la possibilità astratta che la conoscenza dell'espressione lesiva sfugga a tutti o a parte degli utenti-percettori.

Le medesime conclusioni sono applicabili anche alle *fake news* diffamatorie diffuse sui *social network*. A titolo esemplificativo, il Tribunale di Monza, dopo aver affermato che è da ritenersi che coloro che si iscrivono a una piattaforma *social* abbiano, almeno in una certa misura, consapevolmente accettato il rischio delle «potenziali esondazioni dei contenuti che vi inseriscono»[124], ha concluso che postare un messaggio diffamatorio sulla bacheca di un *social network* costituisce dimostrazione del «carattere pubblico delle offese arrecate, riconducibili in modo diretto ed immediato» all'utente[125].

---

[120] Cass. pen, Sez. V, 14 novembre 2016, n. 4873, in *Dir. pen. cont*., 20 aprile 2017, con nota di BIRRITTERI, *Diffamazione e facebook: la cassazione conferma il suo indirizzo ma apre un'estensione analogica in malam partem delle norme sulla stampa;* Cass. pen, Sez. V, sent. n. 4873, de 1 febbraio 2017, in *www.dejure.it.*

[121] Tribunale Bari, Sez. Molfetta, 18 febbraio 2003, n. 23, in *Dir. Giust*., 14 giugno 2003, pp. 23-83.

[122] MANZINI, *Trattato di diritto penale italiano*, Vol. VIII, UTET, p. 340.

[123] Cass. pen., Sez. V, 22 aprile 2010, n. 34916, in *www.dejure.it*.

[124] Tribunale Monza, Sez. IV civ., 2 marzo 2010, n. 770, in *www.dejure.it.*

[125] Tribunale Monza, 2 marzo 2010, cit., pp.1566-1567.

È proprio in riferimento alla riconducibilità all'utente delle offese diffuse su Internet che si pone uno dei principali problemi di applicabilità dell'art. 595 c.p. alla pubblicazione di *fake news on-line.*

Infatti, mentre non sussistono particolari problematiche in relazione all'identificazione del soggetto passivo di diffamazione dal momento che non è necessario che questo sia identificato per nome e per cognome, purché sia identificabile tramite altri elementi indiziari, lo stesso non può dirsi sull'identificazione dell'autore del reato[126].

Sul tema prevalente giurisprudenza ritiene che al fine di poter applicare l'incriminazione di cui all'art. 595 comma III a un'offesa diffusa *on-line* sia imprescindibile l'accertamento da parte dell'autorità giudiziaria dell'indirizzo IP.

Infatti, poiché è non è complesso clonare o utilizzare l'altrui *account* su Internet, la mera circostanza che il *post* discriminatorio sia stato diffuso da uno specifico *account* non può costituire una prova sufficiente ad attribuire la commissione del reato al titolare di quel dato *account*[127].

Al contrario, risulta imprescindibile l'individuazione del sopramenzionato indirizzo IP, ossia di quel codice numerico assegnato esclusivamente a un dispositivo elettronico nel momento della connessione a una data postazione del servizio telefonico[128].

In ragione di tale considerazione, la Corte di Cassazione ha stabilito la necessità dell'accertamento dell'indirizzo IP a cui riferire il messaggio diffamatorio al fine di poter dichiarare la condanna ai sensi del terzo comma dell'art. 595 c.p.[129].

Passando ai requisiti cui la giurisprudenza subordina il diritto costituzionalmente tutelato di diffondere informazioni potenzialmente diffamatorie, vale a dire la continenza, la pertinenza e la verità putativa dei fatti divulgati, questi devono essere rispettati anche da chi, pur non essendo un giornalista, diffonde una notizia sul *web*[130].

---

[126] LONGO, *Diffamazione via mass media e social network, tutele e risarcimenti,* in *Altalex.*, 2020, <https://www.altalex.com/documents/news/2020/02/28/diffamazione-via-mass-media-social-network-tutele-risarcimenti>.

[127] Tribunale Pescara, 5 marzo 2018, n. 652, in *www.dejure.it.*

[128] LONGO, *Diffamazione via mass media e social network, tutele e risarcimenti,* cit.

[129] Cass. pen. Sez. V, 22 novembre 2017, n. 5352, in *www.dejure.it.*

[130] Cass. pen. Sez., V, 1 luglio 2008, n. 31392, in *Dir. Inf.,* 2008, p. 808.

Anzitutto, con il termine pertinenza si fa riferimento al requisito dell'utilità sociale della notizia[131], vale a dire all'idoneità di questa a contribuire alla formazione dell'opinione pubblica in un dato ambito di interesse generale[132]; la continenza, al contrario, indica una forma e un'esposizione dei fatti che siano obiettivi, non denigratori e che non travalichino lo scopo informativo.

E', dunque, proprio in relazione all'interesse generale al contenuto divulgato che i requisiti della pertinenza e della continenza trovano la propria fusione.

Infatti, la stessa Corte di Cassazione ha statuito che, al fine di scriminare affermazioni diffamatorie, il limite della continenza deve essere analizzato non soltanto sotto l'aspetto formale della correttezza dell'esposizione, bensì anche sotto il profilo sostanziale del contenuto potenzialmente diffamatorio che viene divulgato. In altre parole, il requisito della continenza da un punto di vista sostanziale, si concretizza in un divieto di travalicare i limiti di quanto strettamente necessario a soddisfare l'interesse collettivo. Ne consegue che solo l'esigenza di assecondare l'interesse collettivo all'informazione su specifici fatti di rilievo generale, e quindi l'utilità sociale della notizia, può dare luogo a una legittima prevalenza della tutela del diritto alla libertà di espressione, *ex.* art. 21 Cost., sull'integrità dell'onore e sulla reputazione del singolo cittadino[133].

E ancora, al fine di poter considerare legittima la divulgazione di un contenuto lesivo dell'onore o della reputazione altrui è necessario che questo non sia espresso in termini assoluti o assiomatici, ma che, al contrario, la sua diffusione sia accompagnata da una motivazione concreta[134].

Ne deriva, che per quanto concerne la pertinenza, e quindi dell'utilità sociale, tale requisito impone a colui che diffonde la notizia l'obbligo di verifica non solo della verità dei fatti, ma anche dell'esistenza di un effettivo interesse pubblico circa quella determinata notizia. Tale ultima verifica deve essere svolta non in termini soggettivi, quale volontà di soddisfare una propria curiosità, bensì in termini oggettivi: è necessario che la divulgazione dei fatti oggetto della notizia

---

[131] REDAZIONE DI DIRITTO.IT, *Oblio: informazione, verità, pertinenza e continenza*, in *Diritto.it*, 2019, <https://www.diritto.it/oblio-informazione-verita-pertinenza-e-continenza/>.

[132] CASCELLA, *Le condizioni per il legittimo esercizio del diritto di cronaca*, in *diritto.it*, 2012, paragrafo 2.2.

[133] Cass. civ., sez. I, 6 aprile 1993, n. 4109, in *Corr. giur*., 1993, nota ZENCOVICH.

[134] Cass. civ., Sez. III, 15 gennaio 2002, n. 370, in *Foro it*, Rep., 2002, voce Responsabilità civile, n. 197.

contribuisca allo sviluppo della "coscienza sociale" degli individui, consentendo alla collettività di trarre un beneficio dall'apprendimento di quei fatti[135].

Appare, inoltre, opportuno sottolineare che la Suprema Corte ha di recente posto l'attenzione sullo stretto collegamento che intercorre tra l'utilità sociale dell'informazione e il perseguimento del diritto alla libertà di espressione *ex.* art. 21 Cost. A titolo esemplificativo, nella sentenza n. 482 del 2009, la Corte, riconoscendo il diritto alla libertà di manifestazione del pensiero in capo a un'associazione di consumatori ha statuito che «*Il diritto di informazione, garantito dall'art. 21 cost., sussiste in capo ad un'associazione di consumatori ogni qual volta risulti evidente l'utilità sociale della conoscenza dei fatti e delle opinioni, trasmessi con comunicati, perché diretti a contribuire alla formazione della pubblica opinione in materia di interesse generale, correlata alle finalità istituzionali di tale associazione; i «comunicati stampa» di quest'ultima rientrano, pertanto, nella nozione di «stampato» disciplinato dagli art. 1 e 2 l. n. 47 del 1948, trattandosi di attività di soggetto che svolge anche funzione di agenzia, in senso lato, di informazione, sia pure nel più ristretto ambito delle materie connesse alle finalità istituzionali sue proprie, in quanto le notizie diffuse dalle agenzie di informazione mediante comunicati o dispacci sono destinate alla pubblicazione, così come richiesto dal cit. art. 1, e l'eventuale diffamazione consumata attraverso tali comunicati integra l'illecito di diffamazione a mezzo stampa*»[136].

Continuando, ora, l'analisi del requisito della continenza, in una pronuncia del 2011 la Corte di Cassazione ha, poi, esplicitamente ribadito che tale requisito debba ritenersi integrato ogniqualvolta le modalità espressive con cui una vicenda viene narrata rispettino i canoni della moderazione, della misura e della proporzione, non trascendendo in attacchi personali volti a ledere l'altrui dignità morale e professionale. A tal fine, continua la Corte, è necessario prendere in considerazione non solo il contenuto della notizia in senso stretto, ma l'intero contesto espressivo in cui questo è inserito; vale a dire tutti gli elementi che siano utili ad esplicitare il significato del contenuto divulgato, risultando di conseguenza idonei a suggestionare i lettori[137].

---

[135] SICA, D'ANTONIO, *Professioni e responsabilità civile*, Bologna, 2006, pp. 844 e ss.

[136] Cass. civ., sez. III, 13 gennaio 2009, n. 482, in *Foro it*., Mass., 2009, p. 31.

[137] Cass. civ., sez. III, 7 ottobre 2011, n. 20608, in *Foro it.*, Mass., 2011, p. 842.

Passando ora al terzo e ultimo requisito cui la giurisprudenza subordina il diritto di divulgare informazioni lesive dell'altrui onore e reputazione[138], il canone della verità putativa è forse quello che assume maggiore rilevanza con specifico riferimento alle *fake-news* diffuse *on-line*.

Infatti, da questo deriva un onere di verifica delle fonti[139], che, come affermato dal Tribunale di Torino nel 2020, non può considerarsi assolto «nel caso in cui la notizia sia già stata pubblicata da altri, qualora la fonte non dia garanzie di certezza e quindi, a maggior ragione, non può dirsi adempiuto […] laddove la notizia era stata acquisita da internet, dal passaggio sui telefonini e dalle voci che su di essa circolavano»[140].

D'altronde, già ne 1996 la Corte di Cassazione, aveva affermato che si può parlare di verità della notizia quando il fatto narrato corrisponde alla vicenda accaduta; al contrario, non si potrà parlare di verità dell'informazione nell'ipotesi in cui il racconto di fatti veri si affianchi all'omissione di altri avvenimenti la cui inclusone nella narrazione stravolgerebbe il senso della notizia stessa, essendo i secondi inscindibilmente, o quasi, legati ai primi[141].

La Suprema Corte ha, poi, ripreso e approfondito tale filone di pensiero in una pronuncia recente, affermando che «l'esimente della verità putativa dei fatti narrati, idonea ad escludere la responsabilità dell'autore d'uno scritto offensivo dell'altrui reputazione, sussiste solo a condizione che: a) l'autore abbia compiuto ogni diligente accertamento per verificare la verosimiglianza dei fatti riferiti; b) l'autore abbia dato conto con chiarezza e trasparenza della fonte da cui ha tratto le sue informazione, e del contesto in cui, in quella fonte, esse erano inserite; c) l'autore non ha sottaciuto fatti collaterali idonei a privare di senso o modificare il senso dei fatti narrati; d) l'autore, nel riferire fatti pur veri, non abbia usato toni allusivi, insinuanti, decettivi»[142].

Un'ulteriore problematica affrontata dalla recente giurisprudenza in tema di diffamazione *on-line* concerne la responsabilità penale del gestore di un sito

---

[138] GULLO, *Diffamazione e legittimazione all'intervento penale, Contributo a una riforma dei delitti conto l'onore,* cit., p. 32.

[139] SICA, D'ANTONIO, *Professioni e responsabilità civile*, cit., p. 839; Cass. civ., sez. III, 3 marzo 2010, n. 5081, in *La responsabilità civile*, 2011, 442, nota BALLERINI.

[140] Tribunale Torino, 11 giugno 2020.

[141] Cass. civ., Sez. III, 7 febbraio 1996, n. 982, in *Danno e resp.*, 1996, 456, nota CHIAROLLA.

[142] Cass., civ., Sez. III, 29 ottobre 2019, n. 27592, in *www.dejure.it*.

Internet o di un *blog* per i contenuti offensivi dell'altrui reputazione diffusi sullo stesso.

A tal riguardo la Corte di Cassazione nel 2018[143] ha ritenuto che il gestore di un sito o di un *blog* possa rispondere dei contenuti denigratori pubblicati su di esso da terzi solamente quando, essendo a conoscenza della lesività di questi, non li abbia rimossi consapevolmente. Di conseguenza, risulta necessaria una verifica della consapevole adesione del *blogger* o gestore del sito *web* al messaggio diffamatorio, adesione che può essere desunta dalla decisione di questo di non eliminare il contenuto in questione dal proprio *blog.*

Con riferimento a ciò, appare opportuno richiamare la sentenza della Corte di Cassazione penale n. 54946 del 2016, e che ha aperto ha strada alla pronuncia del 2018 sopramenzionata.

Il caso di specie riguardava un commento diffamatorio pubblicato da un utente su un sito *web* nei confronti di Carlo Tavecchio, ex presidente della Federazione Italiana Gioco Calcio, allegando al commento il certificato penale del soggetto offeso. Nei giorni successivi, il gestore del sito in questione aveva pubblicato sullo stesso un articolo che richiamava il commento diffamatorio, così al contempo diffondendolo e pubblicamente definendolo non discriminatorio.

Ebbene, la Corte di Cassazione, allineandosi alla pronuncia della Corte d'Appello, ha ritenuto la conoscenza da parte del gestore del sito del messaggio diffamatorio pubblicato dall'utente e la scelta di questo di non rimuoverlo, elementi sufficienti per far scattare la condanna *ex.* terzo comma dell'art. 595 c.p.

Tale ultima pronuncia ha seguito un altro caso in materia di responsabilità dei gestori di piattaforme *social* che ha suscitato grande scalpore nell'opinione pubblica italiana.

Si tratta del caso del 2006 in cui una ragazza si è tolta la vita dopo che sono state diffuse sulla piattaforma *social Facebook* sue *immagini* e suoi video intimi. Nel caso di specie, il tribunale di Napoli[144] ha affermato che sussiste in capo all'*hosting provider* (ossia in questo caso *Facebook)* un «obbligo di successiva attivazione», in base al quale la responsabilità di questo sorge qualora non ottemperi alla richiesta

[143] Cass. pen., Sez. V, 8 novembre 2018, n. 12546 in *www.dejure.it*.
[144] Tribunale Napoli, Sez. II, civ., ord., 4 novembre 2016, n. 9799.

del soggetto passivo di rimuovere il contenuto lesivo, ovvero all'ordine di un'autorità giurisdizionale o amministrativa[145].

In definitiva, non in maniera dissimile da quanto affermato in passato dalla Corte Suprema in relazione a una trasmissione televisiva in cui il conduttore aveva aderito alle affermazioni discriminatorie di uno degli ospiti[146], qualora un gestore di un sito Internet o un *blogger* non rimuova un commento diffamatorio e dimostri una sua consapevole adesione a questo, egli sarà ritenuto corresponsabile *ex.* art. 110 c.p. di diffamazione aggravata di cui all'art. 595 comma III c.p.

E ancora, sempre in relazione alla pubblicazione di contenuti su Internet, è importante sottolineare che, come affermato dalla Corte di Cassazione[147], anche l'aver prestato il consenso alla diffusione di un determinato contenuto non esclude la responsabilità per diffamazione, nell'ipotesi in cui quel contenuto venga poi pubblicato per scopi o in contesti assolutamente diversi rispetto a quelli per cui era stato concesso il consenso.

Un'altra questione di cui si è occupata la giurisprudenza negli ultimi anni riguarda la possibilità che si configuri il reato di diffamazione in relazione a opinioni e commenti pubblicati dagli utenti su siti di recensioni *on-line*.

In materia si è pronunciato il Tribunale di Pistoia nel 2015 escludendo la configurabilità del reato in esame, ritenendo che il gestore di un locale pubblico implicitamente si assuma il rischio che i propri servizi non vengano graditi e conseguentemente siano oggetto di critiche[148].

Per quanto concerne la possibilità di configurare la reiterazione del reato di diffamazione mediante diffusione di *fake news on-line,* il Tribunale di Milano[149], già nel 2004, ha statuito che costituisce reiterazione via internet del delitto di diffamazione la divulgazione sull'archivio *on-line* del sito di un giornale di un articolo che, dopo essere stato pubblicato sull'edizione cartacea del medesimo giornale, era già stato giudicato diffamatorio da una precedente sentenza; non

[145] PITRUZZELLA, POLLICINO, QUINTARELLI, *Potere e parole, libertà di espressione, hate speech e fake news*, cit., pp. 80-81.
[146] Cass. pen., Sez. V, n. 24727, del 21 gennaio 2016.
[147] Cass. pen., Sez. V, 19 giugno 2008, n. 30664, in *www.dejure.it.*
[148] Tribunale Pistoia, 16 dicembre 2015, n. 5665, in *www.dejure.it.*
[149] Tribunale Milano, Sez. civ.,16 ottobre 2004, n. 11848, in *Dir. Inf.*, 2004, pp. 855 e ss.

assumendo rilevanza che l'accesso all'archivio fosse riservato solo agli abbonati e a fronte del pagamento di un corrispettivo in denaro[150].

In conclusione, per quel che concerne gli ostacoli alla repressione di offese *on-line***,** come sarà meglio analizzato nel paragrafo successivo, è importante sottolineare l'inapplicabilità alle *fake news* diffuse su Internet dell'aggravante di cui all'art. 13 della legge 47/1948, nonché della responsabilità dei direttori delle testate telematiche per omesso controllo *ex.* art 57 c.p.[151], dovuta alla non estendibilità della nozione di stampa di cui all'art. 1 della medesima legge alle piattaforme *on-line* diverse dai periodici telematici registrati.

2.2.2. La non applicabilità della disciplina della diffamazione a mezzo stampa alle *fake news* diffuse su sulle piattaforme *on-line* diverse dai periodici telematici registrati

Entrando più nello specifico della non applicabilità della disciplina della diffamazione a mezzo stampa alle *fake news* diffuse su Internet, occorre anzitutto analizzare la nozione di stampa e la relativa disciplina in caso di diffamazione.

Ai sensi del III comma dell'art. 595 c.p. «se l'offesa è recata col mezzo della stampa o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico, la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a euro 516».

Per quanto concerne la definizione di stampa, secondo l'art. 1 della legge 47/1948 «sono considerati stampa o stampati […] tutte le riproduzioni tipografiche comunque ottenute con mezzi meccanici o fisico-chimici, in qualsiasi modo destinati alla pubblicazione».

Sulla base di tale disposizione, la Corte di Cassazione ha individuato due elementi da rispettare per poter parlare di stampa in senso giuridico, uno obiettivo o statico, l'altro teleologico o dinamico[152]: che vi sia una riproduzione tipografica; che il prodotto di tale attività sia destinato alla pubblicazione e quindi debba essere effettivamente distribuito tra il pubblico[153].

---

[150] PERON, *Internet, regime applicabile per i casi di diffamazione e responsabilità del Direttore,* in *Responsabilità civile e previdenza,* n. 1, 2011, p. 91.

[151] V. *infra* Cap. II § 2.3.

[152] SCOPINARO, *Diffamazione via Internet: applicabilità della circostanza aggravante relativa all'uso del mezzo della pubblicità,* in *Riv. It. Dir. proc.,* 2001, p. 1413.

[153] Cass. pen., Sez. V, 16 luglio 2010, n. 35511, in *penale.it.*

Di conseguenza, nella medesima pronuncia la Corte ha precisato la non applicabilità della disciplina della diffamazione a mezzo stampa alle *fake news* diffuse *on-line,* statuendo che «il fatto che il messaggio internet (e dunque anche la pagina del giornale telematico) si possa stampare non appare circostanza determinante, in ragione della mera eventualità, sia oggettiva, che soggettiva. Sotto il primo aspetto, si osserva che non tutti i messaggi trasmessi via internet sono "stampabili": sì pensi ai video, magari corredati di audio; sotto il secondo, basta riflettere sulla circostanza che, in realtà, è il destinatario colui che, selettivamente ed eventualmente, decide di riprodurre a stampa la schermata. E se è pur vero che la "stampa" – normativamente intesa – ha certamente a oggetto, come si è premesso, messaggi destinati alla pubblicazione, è altrettanto vero che deve trattarsi […] di comunicazioni che abbiano veste di riproduzione tipografica. Se pur, dunque, le comunicazioni telematiche sono, a volte, stampabili, esse certamente non riproducono stampati […]. Bisogna pertanto riconoscere la assoluta eterogeneità della telematica rispetto agli altri media, sinora conosciuti e, per quel che qui interessa, rispetto alla stampa».

In una pronuncia precedente, peraltro, la Cassazione aveva già esplicitamente affermato che i cosiddetti *forum online* non possono essere qualificati come prodotto editoriale, giornale *on-line,* o testata telematica, ritenendoli, al contrario, «una semplice area di discussione dove qualsiasi utente, o gli utenti registrati, sono liberi di esprimere il proprio pensiero, ma non per questo il *forum* resta sottoposto alle regole e agli obblighi cui è soggetta la stampa, come indicare un direttore responsabile per registrare la testata»[154].

Vi è, tuttavia, una parte della giurisprudenza più recente che ha adottato una prospettiva differente. Ad esempio, il Tribunale di Milano ha ritenuto possibile l'equiparazione tra articoli su supporto cartaceo e articoli su supporto telematico nell'ipotesi in cui «un sito sia destinato a contenere pubblicazioni giornalistiche concernenti notizie, comunicati e orientamenti finalizzati a formare l'opinione pubblica». Questa affermazione assume una grande rilevanza, in quanto da questa conseguirebbe che sarebbe possibile estendere ai prodotti editoriali pubblicati *online* le garanzie costituzionali in materia di sequestro di stampa[155].

---

[154] Cass. pen. Sez. III, 11 dicembre 2008, n. 10535, in *Foro it.,* 2010, p. 95, con nota di CHIAROLLA, *Riflessioni introno al concetto di produzione editoriale digitale.*

[155] Tribunale Milano Sez. XI, pen., ord. 21 giugno 2010, n. 157, in *Guida, dir*., 2010, n. 44, p. 24.

La medesima prospettiva è stata accolta anche dal Tribunale di Padova[156], il quale ha ricompreso i prodotti su supporto informatico destinati alla pubblicazione o alla diffusione di informazioni presso il pubblico nella nozione di stampa, ritenendoli parte della nozione di prodotto editoriale. Ciò è stato affermato in particolare con riferimento alle testate telematiche per le quali venga richiesta e ottenuta la registrazione, adempimento che è espressamente richiesto per i periodici cartacei. Il Tribunale ha quindi concluso affermando che l'obbligo di riportare le indicazioni di cui al II comma dell'art. 2 l. n. 47/1948, e di depositare i documenti di cui al successivo comma 5, non può che comportare l'assimilazione tra giornale cartaceo e telematico sotto il punto di vista del contenuto e della destinazione al pubblico.

Contro tali interpretazioni evolutive si è pronunciata, tuttavia, una parte della dottrina sostenendo che, seguendo l'impostazione della sopra citata giurisprudenza, le testate *on-line* non registrate finirebbero per godere di una tutela addirittura maggiore rispetto a quella assicurata ai giornali cartacei, regolarmente iscritti nel registro della stampa[157].

Infatti, come sarà esaminato nel dettaglio nel paragrafo successivo, la più recente giurisprudenza della Corte di Cassazione ha esteso la nozione di stampa alle testate telematiche con una periodicità regolare, ma non alle altre piattaforme *on-line.* Ne consegue che solo le prime, al pari dei giornali cartacei, sono legalmente obbligate ad avere un direttore responsabile che, se del caso, risponde del reato di omesso controllo di cui all'art. 57 c.p; al contrario, ad oggi non è prevista l'applicabilità della disciplina in esame alle altre piattaforme digitali, quali *blog* o *forum.*

In conclusione, nonostante gli orientamenti della dottrina e della giurisprudenza minoritarie, e l'ormai pacifica l'applicabilità dell'aggravante dell'uso di un qualunque altro mezzo di pubblicità diverso dalla stampa di cui al terzo comma dell'art. 595 c.p. alla diffamazione *on-line,* prevalente giurisprudenza e dottrina continuano a essere restii sul legittimare la comprensione nella nozione di stampa dei contenuti pubblicati su piattaforme *on-line* diverse dai periodici telematici registrati.

---

[156] Tribunale Padova, ord., 1 ottobre 2009, in *Foro.it*., 2009, I, p. 3225.

[157] CIMINO, *Art. 21 Costituzione ed i limiti a sequestro dei contenuti (multimediali) nelle pubblicazioni telematiche e nei prodotti editoriali*, in *Dir. inf*., 2009, p. 772.

2.3. La responsabilità penale ex. art. 57 c.p. del direttore di una testata telematica

L'art. 3 della legge n. 47 del 1948 prevede che ogni giornale o periodico debba avere un direttore responsabile, il quale deve essere un cittadino italiano o comunitario[158], in possesso dei requisiti per l'iscrizione nelle liste elettorali politiche.

Ciò posto, l'art. 57 c.p. sui reati commessi col mezzo della stampa periodica sancisce che «salva la responsabilità dell'autore della pubblicazione e fuori dei casi di concorso, il direttore o il vice-direttore responsabile, il quale omette di esercitare sul contenuto del periodico da lui diretto il controllo necessario ad impedire che col mezzo della pubblicazione siano commessi reati, è punito, a titolo di colpa, se un reato è commesso, con la pena stabilita per tale reato, diminuita in misura non eccedente un terzo».

La Corte di Cassazione ha, poi, precisato che il controllo sul contenuto del giornale, unitamente considerato, spetta in via esclusiva al direttore responsabile. Di conseguenza, ai fini della configurabilità del reato, è da escludere che abbia qualsiasi tipo di rilevanza il conferimento al redattore capo delle edizioni decentrate delle funzioni di controllo che, al contrario, gli articoli 57 c.p. e 3 della l. n. 47/1948 demandano direttamente alla posizione di garanzia del direttore responsabile, non sussistendo possibilità di delega ad altri soggetti del potere-dovere di controllo[159].

A tal riguardo, è bene ricordare anche che il direttore che si affianca al direttore responsabile senza sostituirlo o assumerne le funzioni, non essendo titolare dei sopramenzionati poteri di controllo, non può essere ritenuto responsabile per i danni derivanti dalla pubblicazione di articoli diffamatori[160].

Prima di passare all'analisi della possibile estensione dell'art. 57 c.p. ai periodici telematici, risulta opportuno affrontare le problematiche sulla natura e il contenuto dell'obbligo che la disposizione in esame pone in capo al direttore responsabile,

---

[158] ai sensi dell'art. 9 l. 52/1996 il cittadino italiano è stato equiparato a quello comunitario ai fini degli artt. 3 e 4 l. n. 47/1948.

[159] Cass. pen. Sez., V, 11 novembre 2009 n. 7407, in *www.dejure.it*.

[160] Cass. pen., Sez. V, 2 dicembre 2004, n. 46786, in *www.dejure.it*; Cass. pen., Sez. V, 14 agosto 2008n. 33472, in *www.dejure.it*.

tema che ad oggi continua a formare oggetto di dibattito dottrinale e giurisprudenziale[161].

Vi è, infatti, un filone di pensiero secondo cui l'inciso "a titolo di colpa" definirebbe esclusivamente il titolo del reato, e non la natura della stessa, descrivendo, dunque, una forma di responsabilità oggettiva[162].

Altri autori, al contrario, hanno affermato che l'inciso in questione dimostrerebbe la natura colposa dell'illecito, andando così a incidere sulla natura e sul fondamento stesso dell'incriminazione, nella quale la sanzione riguarderebbe l'omissione di controllo da parte del direttore responsabile[163].

Ciò detto, per quanto concerne l'applicabilità dell'art. 57 c.p. ai direttori di giornali telematici, ha assunto un ruolo determinante l'introduzione della definizione di "prodotto editoriale" nell'art. 1 della legge 62 del 2001, cosiddetta "terza legge sull'editoria"[164]. Infatti, non solo la nozione di prodotto editoriale, a differenza di quella di stampa sopramenzionata, comprende anche le pubblicazioni *on-line*, ma a questa si applicano anche le disposizioni di cui all'art. 2 della legge 47/1948 in virtù del rimando previsto nell'art. 3 della medesima legge del 2001. Ne consegue che trova applicazione anche per i periodici telematici la normativa sull'inserimento obbligatorio dell'indicazione del luogo e della data della pubblicazione; del nome e del domicilio dello stampatore; del nome del proprietario e del direttore o vice direttore responsabile. Inoltre, qualora il giornale sia diffuso al pubblico con cadenza regolare e sia contraddistinto da una testata identificativa del prodotto, il periodico è sottoposto, anche agli obblighi previsti *ex.* art. 5 della medesima legge, ossia alla registrazione della testata telematica presso la cancelleria del tribunale.

Tale equiparazione sul piano amministrativo tra periodico telematico e periodico cartaceo ha sollevato una questione circa la possibilità di un'estensione anche sul piano penale. Tuttavia, come dimostrato dalla pronuncia della Corte di Cassazione

---

[161] GUERINI, Fake News *e Diritto Penale, la mnipolazione digitale del consenso nelle democrazie liberali,* cit. p. 139

[162] PISAPIA, *La nuova disciplina della responsabilità per i reati commessi a mezzo della stampa*, in *Riv. It. Dir. proc. pen*., 1958, p. 318.

[163] GROSSO, *Responsabilità penale per i reati commessi col mezzo della stampa*, Milano, 1969, p. 88.

[164] BASSINI, *La disciplina penale della stampa alla prova di internet: avanzamenti e arresti nella dialettica giurisprudenziale da una prospettiva costituzionale,* in FLOR, FALCINELLI, MARCOLINI (a cura di), *La giustizia penale nella "rete" Le nuove sfide della società dell'informazione nell'epoca di Internet,* 2015, p. 13.

nel *leading case* Brambilla[165] , almeno in un primo momento, l'eventualità di tale equiparazione sul fronte penale è stata rigettata dalla Corte, la quale ha escluso ogni forma di coinvolgimento del direttore di un periodico telematico, sul presupposto che il reato di omesso controllo *ex.* art. 57 c.p. «non è realizzabile da chi non sia direttore di un giornale cartaceo».

Nello specifico, nel caso in esame la Suprema Corte ha definito come forma di analogia *in malam partem* l'equiparazione di un periodico *on-line* a una testata telematica, osservando come il codice penale, nell'attribuire un rilievo particolare alla stampa rispetto agli altri mezzi di informazione, si riferisca «specificatamente all'informazione diffusa tramite "carta stampata"». In conclusione della citata pronuncia, la Corte ha escluso anche un'autonoma responsabilità del giornale *on-line,* dal momento che tale reato non è previsto dal codice penale italiano, non essendo l'art. 57 c.p. applicabile a questa fattispecie.

Inoltre, la Corte, facendo riferimento alla disciplina del d.lgs 70/2003 in tema di Internet *service provider,* sostanzialmente ha equiparato il direttore di una testata telematica a un gestore di un *blog,* sottolineando che in capo a questi non sussiste alcun obbligo generale di sorveglianza o responsabilità per omesso controllo, bensì la responsabilità del prestatore è circoscritta alla rimozione di contenuti illeciti specificamente e previamente segnalatigli[166].

Tale orientamento è poi stato ulteriormente confermato in una sentenza del 2011, in occasione della quale la Corte ha chiarito che la *ratio* dietro l'inammissibilità dell'equiparazione consiste nella «diversità strutturale tra i due mezzi di comunicazione»[167].

Se, dunque, fino al 2011 l'orientamento della giurisprudenza sembrava saldo nel rigettare l'estendibilità ai periodici *on-line* della disciplina sulla stampa, con la celebre sentenza n. 31022 del 2015 la Corte ha avuto una netta inversione di tendenza. In tale pronuncia, infatti, le Sezioni Unite hanno esteso le garanzie previste dal terzo comma dell'art. 21 Cost., in tema di sequestro della stampa cartacea, anche a quella diffusa *on-line* tramite il mezzo di Internet. La Corte è dunque giunta a un'equiparazione tra stampa periodica cartacea e stampa

[165] Cass. pen. Sez. V, 16 luglio 2010, n. 35511, in *www.dejure.it.*

[166] BASSINI, *La disciplina penale della stampa alla prova di internet: avanzamenti e arresti nella dialettica giurisprudenziale da una prospettiva costituzionale,* cit., pp. 16-17.

[167] Cass. pen. Sez. V, 29 novembre 2011, n. 44126, in *www.dejure.it.*

telematica, affermando che: «la testata giornalistica telematica, funzionalmente assimilabile a quella tradizionale in formato cartaceo, rientra nella nozione di "stampa" di cui alla L. 8 febbraio 1948, n. 47, art. 1, in quanto si tratta di prodotto editoriale sottoposto alla normativa di rango costituzionale e di livello ordinario, che disciplina l'attività di informazione professionale diretta al pubblico»[168].

Nello statuire ciò, tuttavia, la Corte di Cassazione in composizione plenaria ha sottolineato la distinzione tra testata di un giornale telematico e le altre piattaforme su Internet - tra cui *Blog*, *social network e forum* - ribadendo che la sopramenzionata equiparazione sussiste solo per i periodici telematici.

La Corte ha raggiunto tale adattamento in *bonam partem* abbandonando la tradizionale nozione di "stampa" prevista dal dato letterale della legge n. 47 del 1948, al fine di accogliere un concetto di stampa più moderno e meno rigido, legato alla "professionalità dell'informazione" che rimane tale a prescindere dalla forma cartacea o telematica in cui si sostanzia.

Dunque, la Corte ha statuito che «in realtà, lo scopo informativo è il vero elemento caratterizzante l'attività giornalistica e un giornale può ritenersi tale se ha i requisiti, strutturale e finalistico, di cui si è detto sopra, anche se la tecnica di diffusione al pubblico sia diversa dalla riproduzione tipografica o ottenuta con mezzi meccanici o fisico-chimici. Ma anche a prescindere da tali considerazioni, è il caso di aggiungere che non è certamente dirimente la tesi, secondo cui il giornale telematico non rispecchierebbe le due condizioni ritenute essenziali ai fini della sussistenza del prodotto stampa come definito dalla legge n. 47 del 1948, vale a dire un'attività di riproduzione e la destinazione alla pubblicazione. L'informazione professionale, pertanto, può essere espressa non solo attraverso lo scritto (giornale cartaceo), ma anche attraverso la parola unita eventualmente all'immagine (telegiornale, giornale radio) o altro mezzo di diffusione, qual è internet (giornale telematico); e tutte queste forme espressive, ove dotate dei requisiti richiesti, non possono essere sottratte alle garanzie e alle responsabilità previste dalla normativa sulla stampa».

In altre parole, la Corte ha attuato un'interpretazione estensiva in chiave evolutiva della nozione di stampa, così da rendere questa conforme e coerente con il progresso tecnologico e con l'era della Post-Verità, ma rimanendo sempre fedele

[168] Cass. pen. Sez. U.U., 17 luglio 2015, n. 31022, in www.dejure.it; GULLO, *Diffamazione e pena detentiva*, in *Diritto penale contemporaneo* (online), 2016, pp. 1-12.

all'ordinamento giuridico positivo. E, infatti, la stessa Corte che ha proseguito affermando che «l'interpretazione estensiva, se coerente con la mens legis - nel senso che ne rispetta lo scopo oggettivamente inteso, senza porsi in conflitto con il sistema giuridico che regola il settore d'interesse - consente di discostarsi dalle definizioni legali, le quali sono semplici generalizzazioni destinate ad agevolare l'applicazione della legge in un determinato momento storico, e di accreditare al dato normativo un senso e una portata corrispondenti alla coscienza giuridica e alle necessità sociali del momento attuale».

In questo specifico caso, la pronuncia della Corte era limitata al tema del sequestro preventivo, e dunque l'intervento delle Sezioni Unite si è risolto in un'estensione in *bonam partem* delle tutele costituzionali volte a impedire un'illegittima compressione della libertà di manifestazione del pensiero[169].

Tuttavia, la rilevanza di tale pronuncia non è circoscritta al *thema decidendum* di quella specifica vicenda, al contrario è stata proprio la sentenza n. 31022 del 2015 ad aprire la strada alle innumerevoli altre decisioni in tema di responsabilità dei direttori di periodici telematici, e non solo, che si sono succedute negli anni.

Anzitutto, appare opportuno ricordare la sentenza n. 13398 del 2017[170], con la quale la Corte di Cassazione ha fornito un'interpretazione della nozione di stampa in chiave ancora più evolutiva prevedendo l'applicabilità dell'art. 57 c.p. al direttore responsabile di testate telematiche registrate.

In tale occasione, la Suprema Corte ha affermato che «dalla riconducibilità della testata giornalistica telematica alla nozione di "stampa", consegue la sottoposizione di tale particolare forma di "giornale" alla relativa disciplina di rango costituzionale e di livello ordinario.

Ad essa, pertanto, si estendono non solo le garanzie costituzionali a tutela della stampa e della libera manifestazione del pensiero previste dall'art. 21 Cost., ma anche le disposizioni volte ad impedire che con il mezzo della stampa si commettano reati, tra le quali particolare rilievo assume il disposto del citato art. 57 c.p., che, secondo il costante insegnamento della giurisprudenza di legittimità, estende la sua portata anche ai casi di pubblicazione di un articolo non firmato, da

[169] PISA, *La responsabilità del direttore di periodico on line tra vincoli normativi e discutibili novità giurisprudenziali*, in *Dir. pen. proc*., 3, 2019.
[170] Cass. pen., sez. V, 11 dicembre 2017, n. 13398, in *Foro it*., 5, 2018, II.

ritenersi, in assenza di diversa allegazione, di produzione redazionale, dunque, riconducibile al direttore responsabile.

Risulta, pertanto, superato il contrario orientamento della giurisprudenza di legittimità, che escludeva la responsabilità del direttore di un periodico *on-line* per il reato di omesso controllo, ex art. 57 c.p […]».

A supporto di tale piena estensione, la Corte ha richiamato la sostanziale assimilabilità tra testata telematica registrata e giornale cartaceo, sia da un punto di vista ontologico che sotto il profilo funzionale, sottolineando che tale equiparazione sussiste a prescindere dalla materiale possibilità per il direttore del periodico di svolgere un controllo e una vigilanza sugli articoli pubblicati. Sul punto la Corte di Cassazione ha affermato esplicitamente che anche nell'ipotesi in cui si accertasse l'impossibilità per il direttore di prevenire la commissione dei reati a mezzo stampa, ciò comunque non sarebbe sufficiente per escludere la responsabilità di questo con riferimento a un articolo pubblicato, che egli avrebbe dovuto o potuto rimuovere e rispetto al quale potrebbe comunque essere incriminato a titolo di colpa *ex.* art. 57 c.p. - ovviamente nell'eventualità in cui fosse possibile raggiungere la prova della sua adesione al contenuto diffamatorio.

È inoltre importante sottolineare che, anche in questa pronuncia la Corte di Cassazione, riprendendo quanto statuito dalle Sezioni Unite nel 2015, ha ribadito la netta distinzione tra i periodici telematici e le altre piattaforme *on-line*, confermando la non applicabilità dell'art. 57c.p. a queste ultime.

Tale argomentazione è stata ulteriormente confermata da una pronuncia del 2018[171], in cui la Corte ha previsto espressamente che «in tema di diffamazione, l'amministratore di un sito internet non è responsabile ai sensi dell'art. 57 c.p., in quanto tale norma è applicabile alle sole testate giornalistiche telematiche e non anche ai diversi mezzi informatici di manifestazione del pensiero (forum, blog, newsletter, newsgroup, mailing list, Facebook)».

E ancora, questo nuovo orientamento è stato ulteriormente ribadito e confermato dalla Corte nella recente sentenza 1275 del 2018[172], in cui questa ha riconosciuto la responsabilità per omesso controllo in capo al direttore di un quotidiano *on-line*,

[171] Cass. pen., Sez. V, 19 febbraio 2018, n. 16751, in *Cass. pen*., 11, 2018, 3743 ss., con nota di PEDULLÀ.

[172] Cass., Pen., 23 ottobre 2018, n. 1275, in *Dir. pen. cont. (online),* 28 febbraio 2019, con nota di MAURI.

affermando che, data la nozione evolutiva e costituzionalmente orientata del termine "stampa", sarebbe irragionevole e illegittimo per violazione del principio di uguaglianza *ex.* art. 3 della Costituzione, ritenere che alle due fattispecie non sia applicabile la medesima disciplina.

Appare a questo punto opportuno ricordare che, nonostante l'uniformità di pensiero che caratterizza tale nuovo filone giurisprudenziale, questo è stato aspramente criticato in dottrina[173]. A titolo esemplificativo, è stato affermato che «l'estensione della portata dell'art. 57 c.p. non è frutto di una semplice interpretazione estensiva, ma rappresenta un'applicazione analogica in malam partem: un overruling in contrasto con i principi costituzionali che strumentalizza, paradossalmente, l'apertura "garantista" delle Sezioni Unite in tema di sequestro preventivo del periodico telematico»[174].

Più nello specifico, i sostenitori della corrente dottrinale in esame ritengono che il dettato normativo dell'art. 1 della legge numero 47 del 1948 non consenta di estendere il conetto di "stampa" oltre quanto ivi espressamente stabilito, nonostante l'interpretazione evolutiva fornita dalla Corte di Cassazione appaia astrattamente condivisibile, in quanto volta a porre fine alla disparità di trattamento tra i periodici telematici e quelli cartacei[175].

Ad ogni modo, dalle recenti pronunce della Corte di Cassazione risulta ormai chiara l'estensione della nozione di "stampa" ai periodici telematici registrati, con la conseguente applicabilità dell'art. 57 c.p., ma non alle altre piattaforme *on-line*, tra cui i *social network e i blog.*

Proprio con riferimento ai *blog*, risulta opportuno fare una considerazione conclusiva sull'ipotesi in cui venga pubblicato un contenuto lesivo su di essi in assenza di controllo da parte del gestore dello stesso. Anzitutto, con il termine *blog* si indica una «pagina internet personale, aperta ai commenti dei lettori, di norma

---

[173] PAOLONI, *Le Sezioni Unite si pronunciano per l'applicabilità alle testate telematiche delle garanzie costituzionali sul sequestro della stampa: ubi commoda, ibi et incommoda?*, in *Cass. pen.*, 10, 2015, pp. 3454 ss; MAURI, *Applicabile l'art. 57 c.p. al direttore del quotidiano online: un revirement giurisprudenziale della Cassazione, di problematica compatibilità con il divieto di analogia*, in *DPC*, 2019; PETRINI, *Diffamazione on line: offesa recata "con altro mezzo di pubblicità" o col mezzo della stampa?*, in *Dir. pen. proc*., 1, 2017, pp. 1485 ss.

[174] PISA, *La responsabilità del direttore di periodico on line tra vincoli normativi e discutibili novità giurisprudenziali*, cit., p. 408.

[175] AMERIO, *La responsabilità ex. art. 57 c.p. del direttore di testate telematiche: tra estensione interpretativa ed analogia in malam partem*, in *media laws*, 2019, pp. 291 e ss

organizzata in ordine cronologico e arricchita con link ad altri siti, articoli, immagini, video disponibili in rete»[176].

Ebbene, con riferimento a questa specifica categoria di piattaforma *on-line*, in una pronuncia recente la Corte ha riaperto la questione della responsabilità dell'amministratore statuendo che, a prescindere dall'applicabilità dell'art. 57 c.p. al gestore di un *blog*, in ogni caso quest'ultimo è responsabile dei contenuti lesivi pubblicati sul suo diario da terzi se, presa cognizione dell'offensività di tali contenuti, decide consapevolmente di mantenerli[177]. In particolare la non tempestiva rimozione da parte del *blogger* dei contenuti offensivi pubblicati da soggetti terzi equivale alla consapevole adesione e condivisione del commento diffamatorio, con ulteriore riproduzione della lesività dei contenuti pubblicati sul diario digitale che è gestito dal *blogger* stesso.

In conclusione, negli ultimi anni si è assistito a una sorprendente inversione di tendenza in giurisprudenza, la quale si è mossa sempre di più verso una responsabilizzazione dei gestori e dei direttori delle piattaforme *web.* Infatti, se da un lato è stata esplicitamente riconosciuta l'applicabilità dell'art. 57 c.p. alle testate telematiche, dall'altra, pur non essendo stato ancora esteso l'alveo di tutela di tale disposizione alle altre piattaforme *on-line,* come abbiamo visto per il caso del *blog,* la tendenza della Corte di Cassazione è quella di andare verso l'attribuzione di una responsabilità di rimozione di contenuti lesivi ivi pubblicati in capo al gestore delle stesse.

2.4. Il reato di procurato allarme presso l'Autorità

Tra i reati astrattamente configurabili dalla diffusione di *fake news* su Internet, bisogna sicuramente annoverare l'art. 658 c.p., ai sensi del quale «chiunque, annunziando disastri, infortuni o pericoli inesistenti, suscita allarme presso l'Autorità, o presso enti o persone che esercitano un pubblico servizio, è punito con l'arresto fino a sei mesi o con l'ammenda da euro 10 a euro 516».

Si tratta di un reato comune, di evento e a forma vincolata, il cui oggetto consiste nella tutela dell'ordine pubblico. Dunque, ancora una volta, siamo in presenza di una norma che tutela la verità solamente in quanto funzionale alla protezione

[176] Enciclopedia Treccani, <<https://www.treccani.it/enciclopedia/blog/ >>.
[177] Cass. pen, Sez. V, 8 novembre 2018, n.12546, in *www.dejure.it* .

dell'ulteriore bene giuridico dell'ordine pubblico, in questo caso *sub* forma della tranquillità dei cittadini.

Ciò detto, per quel che concerne le *fake news*, il fatto che l'oggetto della sanzione sia una particolare forma di notizia che, per il proprio contenuto allarmante, è idonea a turbare la pubblica tranquillità, fa sì che la tutela assicurata dalla previsione in esame si possa facilmente estendere ai fenomeni manipolativi dell'informazione su Internet.

D'altra parte, non è irragionevole pensare che la diffusione di una notizia falsa o manipolata da parte di un utente tramite il *web* possa comportare l'attivazione della pubblica Autorità preposta al monitoraggio di quella determinata piattaforma.

Una perfetta esemplificazione di questa circostanza ci è fornita proprio dalle notizie false diffuse su piattaforme *social* in relazione alla pandemia Covid-19.

Negli ultimi mesi sono state numerose le denunce per il reato di procurato allarme presso l'Autorità *ex.* art. 658 c.p., nei confronti di coloro che hanno diffuso notizie false su situazioni di pericolo in relazione al contagio da Coronavirus mediante *Whatsapp o* piattaforme *social,* così generando un ingiustificato e infondato allarme sociale, e di riflesso presso l'Autorità.

Infatti, come affermato dalla Corte di Cassazione nel 2018, condotte di questo genere configurano il reato in esame anche se l'annuncio del pericolo non sia effettuato direttamente all'Autorità, ma solamente in via mediata tramite la creazione di un allarme in un qualsiasi privato cittadino e nella collettività[178].

A titolo esemplificativo, dalle notizie di cronaca si è appreso che l'11 marzo 2020 a Milano, la polizia di stato ha trasmesso all'Autorità Giudiziaria l'esposto dell'ospedale di Niguarda di Milano. Questo riguardava un messaggio vocale inviato via *Whatsapp* registrato da una cardiologa presso il reparto di terapia intensiva dell'ospedale milanese che riportava *fake news* sulla gestione dell'emergenza sanitaria idonee a destare allarme sociale nei destinatari.

In conclusione, appare, dunque, evidente che l'art. 658 c.p. rientra tra quelle disposizioni incriminatrici che forniscono una tutela pienamente idonea ad essere estesa alle istanze sorte con l'avvento di Internet nell'era della Post-Verità.

Tuttavia, è altrettanto importante ricordare che a parare della dottrina prevalente solamente un pericolo prossimo è idoneo a far scattare l'incriminazione per

[178] Cass. pen., Sez. I, 9 febbraio 2018, n. 26897, in *www.dejure.it.*

procurato allarme presso l'Autorità, stante l'inidoneità di un pericolo meramente remoto a determinare l'attivazione della pubblica Autorità[179]. Ad esempio, riprendendo il caso della *Blue Whale*[180], difficilmente un pericolo generico di un suicidio di massa di adolescenti potrebbe essere ricompreso nella fattispecie in esame[181].

2.5. La non configurabilità dei reati elettorali per le *fake news on-line* e l'assenza di una disciplina sul silenzio elettorale sui *social media*

Come sarà affrontato nel capitolo successivo[182], il problema delle *fake news* va necessariamente inquadrato nell'ambito di una dimensione politica, essendo le manipolazioni dell'informazione spesso uno strumento utilizzato nell'ambito della propaganda politica.

Per tale ragione, nell'analisi dei reati astrattamente configurabili mediante la diffusione di *fake news* è opportuno affrontare i reati elettorali, nonostante si giungerà a riconoscere la non configurabilità di tali illeciti penali nell'ipotesi di manipolazioni dell'informazione *on-line.*

Si tratta di una categoria di reati volti a tutelare il libero esercizio da parte dei cittadini dei diritti politici, nonché la regolarità e la genuinità delle consultazioni e della propaganda elettorale[183].

Tra le norme penali in materia di propaganda elettorale vanno sicuramente annoverati gli articoli 8 e 9 della legge 212 del 1956, i quali riguardano rispettivamente la sottrazione o distruzione di stampati, giornali murali o altri o manifesti di propaganda elettorale, e la violazione del silenzio elettorale.

Per quanto attiene, invece, strettamente al codice penale assumo rilievo gli articoli 294 e 416 *ter* c.p., i quali tuttavia, non trovano applicazione nell'ambito di *fake news* diffuse *on-line.*

Partendo dal primo, il reato di cui all'art. 294 c.p. si sostanzia nell'impedimento mediante violenza, minaccia o inganno dell'esercizio di un diritto politico, ovvero nella determinazione, con i medesimi mezzi di taluno a esercitarlo in senso difforme

---

[179] MANZINI, *Trattato di diritto penale italiano*, V ed., Torino, 1986 pp. 149-150.
[180] V. *supra* Cap. I, § 1.3.2.
[181] PUENTE, *Il grande inganno di internet*, Milano, 2019, pp. 165-170; GUERINI, *Fake News e Diritto Penale, la manipolazione digitale del consenso nelle democrazie liberali*, cit. pp. 150-151.
[182] V. *infra* Cap. III.
[183] MAZZANTI, *Reati elettorali*, (voce), in *Enc. Dir.*, XIV vol., Milano, 1965, p. 806.

dalla sua volontà. Tuttavia, alcune precisazioni della Corte di Cassazione hanno confermato la non configurabilità della disposizione in esame nell'ipotesi di *fake news* sul *web*. Nello specifico la Corte, ribadendo quanto affermato in una pronuncia del 1989 secondo cui la mera suggestione non è sufficiente a integrare il reato in questione[184], con la sentenza numero 16381 del 2018 ha chiarito che per integrare l'inganno è necessaria una condotta che faccia uso di qualsiasi mezzo fraudolento idoneo ad esercitare sull'elettore una pressione di una intensità tale da indurlo ad esercitare un proprio diritto politico in maniera differente alla sua reale volontà[185]. Appare, dunque, evidente che tale precisazione esclude le *fake news* dall'insieme dei mezzi fraudolenti idonei a far scattare la condanna ai sensi dell'art. 294 c.p.[186].

Per quel che concerne la seconda disposizione, ossia l'art. 416 *ter* c.p., tale reato si configura nelle ipotesi di accordi tra esponenti mafiosi e candidati alle elezioni tali da alterare lo svolgimento delle elezioni, andando così a ledere la tutela dell'ordine pubblico e lo stesso principio democratico. Anche in questo caso, la natura stessa della norma esclude la possibilità di applicare la tutela da questo assicurata alla fattispecie delle *fake news on-line.*

Ciò che, al contrario, si configura nell'ambito delle *fake news* su Internet in relazione alla propaganda elettorale, è il mancato rispetto da parte dei candidati della disciplina del silenzio elettorale sui *social network.*

La disciplina del silenzio elettorale è contenuta nell'art. 9 comma I della legge 212/1956, ai sensi del quale «nel giorno precedente ed in quelli stabiliti per le elezioni sono vietati i comizi, le riunioni di propaganda elettorale diretta o indiretta, in luoghi pubblici o aperti al pubblico, la nuova affissione di stampati, giornali murali o altri e manifesti di propaganda».

Tale normativa, pur essendo stata estesa anche alle emittenti radio televisive private dall'art. 9 *bis* della legge numero 807 del 1994, ad oggi non è considerata applicabile alle piattaforme *social*. Di conseguenza, poiché queste ultime non sono comprese neanche dalla legge numero 515 del 1993 in tema di disposizioni sulla parità di accesso ai mezzi di informazione durante le campagne elettorali e

[184] Cass. Sez. I, 26 giugno 1989, n. 11835, *in* www.dejure.it.
[185] Cass. Sez. I, 20 dicembre 2018, n. 16381, www.dejure.it.
[186] GUERINI, *Fake news e diritto penale, la manipolazione digitale del consenso nelle democrazie liberali,* cit., p. 154.

referendarie e per la comunicazione politica nell'ambito delle campagne elettorali per l'elezione della Camera dei Deputati e del Senato della Repubblica, attualmente sussiste un vuoto legale circa la disciplina sul silenzio elettorale sui *social network*[187].

Proprio in ragione di tale assenza di disciplina, in occasione della campagna elettorale del 2018, l'AGCOM ha emanato delle linee guida, con l'auspicio che le piattaforme *social,* pur non essendone legalmente obbligate, si uniformassero ai principi alla base del dettato normativo, garantendo così anche sui *social network* un accesso imparziale ed equo ai mezzi di informazione e comunicazione politica a tutti i soggetti politici[188].

Tuttavia, essendo le linee guida emanate dall'Agenzia solamente uno strumento di *soft law*, esse non vincolano le piattaforme digitali, che quindi, ad oggi, continuano a beneficiare del vuoto normativo in materia di silenzio elettorale.

2.6. Il reato di sostituzione di persona e *identity theft*

Il reato di sostituzione di persona si configura spesso su Internet sotto forma di *identity theft*[189].

Ai sensi dell'art. 494 c.p. «chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino ad un anno».

Si tratta di un reato comune, specificamente di uno dei delitti contro la fede pubblica. Anche in questo caso, dunque, ci troviamo di fronte a una norma in cui la tutela della verità viene assicurata solo in quanto funzionale alla tutela di beni giuridici ulteriori. Infatti, il reato di sostituzione di persona può essere annoverato tra i reati cosiddetti plurioffensivi, in quanto se da una parte tutela il pubblico interesse alla fede pubblica, con particolare riferimento a quei comportamenti che

---

[187] GUERINI, *Fake news e diritto penale, la manipolazione digitale del consenso nelle democrazie liberali,* cit. p.158.

[188] AGCOM, *Linee guida per la parità di accesso alle piattaforme online durante la campagna elettorale per le elezioni politiche 2018*, 1 febbraio 2018.

[189] ZICCARDI, *Furto di identità*, in *Dig. Disc. Pen*., IV, Torino, 2011, p. 255.

alterano l'identificazione di un individuo, dall'altra assicura una protezione agli interessi del soggetto privato leso dalla condotta di falso.

In tal senso si è pronunciata la Corte Suprema nel 2007 statuendo che ai delitti contro la fede pubblica deve riconoscersi, «oltre ad un'offesa alla fiducia che la collettività ripone in determinati atti, simboli, documenti, etc., anche una ulteriore e potenziale attitudine offensiva, che può rivelarsi poi concreta in presenza di determinati presupposti, avuto riguardo alla reale e diretta incidenza del falso sulla sfera giuridica di un soggetto»[190].

E', inoltre, opportuno sottolineare che la norma in questione trova applicazione solo se la condotta non costituisce altro delitto contro la fede pubblica, avendo questa natura sussidiaria. E ancora, ai fini della configurabilità del reato *ex.* art. 494 c.p., la condotta dell'attore può essere finalizzata all'acquisizione di un'utilità di qualsiasi natura, non essendo necessario uno scopo patrimoniale.

Infatti, pur integrando la fattispecie di sostituzione di persona un reato a dolo specifico, per cui l'autore deve agire con coscienza e volontà di commettere il fatto e con lo scopo di recare danno al soggetto passivo ovvero ottenere un vantaggio, tale vantaggio, può, tuttavia indifferentemente essere patrimoniale o non patrimoniale[191]. Nello specifico, secondo la Corte di Cassazione nel concetto di "vantaggio" indicato dalla norma in esame rientra il bene immateriale della visibilità, così che la configurazione del reato di sostituzione di persona sussista in tutte le ipotesi in cui un utente crea un profilo *fake* su una piattaforma *social* per una propria "velleità narcisistica", causando al soggetto passivo un danno che si sostanzia nella lesione della dignità o dell'immagine di quest'ultimo[192]. Infine, poiché, come detto, si tratta di un reato a dolo specifico, la fattispecie si configura anche qualora l'agente non raggiunga il vantaggio a cui è finalizzata la propria condotta, rilevando esclusivamente l'intenzione di questo al momento della commissione del fatto.

Proseguendo nell'analisi della disposizione in esame, si tratta evidentemente di un reato a condotta vincolata, quindi non configurabile in forma omissiva, che può sostanziarsi in quattro condotte tipiche tra loro equivalenti, per cui il concretizzarsi

[190] Cass., SS. UU, 25 ottobre 2007, n. 46982, in *www.dejure.it*.
[191] Cass. pen., Sez. V, 28 gennaio 2013, n. 13296, in *www.dejure.it.*
[192] Cass. pen., Sez. V,16 giugno 2014, n. 25774, in *www-dejure.it.*

di una o più di queste nel medesimo ambito spazio-temporale realizza un unico reato.

Nello specifico, l'art. 494 c.p. concerne quattro condotte che possono essere riassunte in due fattispecie: la prima si sostanzia nel sostituirsi *in toto* ad un altro individuo, mentre la seconda nell'attribuirsi un falso nome, un falso stato o false qualità[193].

Ciò detto, in passato la giurisprudenza ha considerato il reato configurato in ipotesi di matrimoni per procura in cui uno dei due coniugi dichiarava un falso status sociale o una falsa identità. A titolo esemplificativo, in una pronuncia del 2016 la Corte di Cassazione[194]ha ritenuto configurato il reato di sostituzione di persona in un caso in cui un uomo si era finto *single* per conquistare l'amante, mostrandole un finto atto di annullamento del matrimonio.

Da qui, l'incertezza, anche dovuta alla genericità della formulazione della disposizione, sulla configurabilità della fattispecie in esame nel caso in cui un utente di un *social network* affermi il falso sul proprio stato del profilo Internet definendosi *single*.

La prima pronuncia in materia di sostituzione di persona tramite Internet risale al 2007, con riferimento a un *account* di posta elettronica mediante il quale un individuo si era abusivamente attribuito l'altrui generalità, inducendo così in errore gli utenti del *web*, al fine di arrecare un danno all'individuo cui queste erano realmente riferibili. Nel caso in questione[195], la Corte di Cassazione ritenne configurato il reato di sostituzione di persona *ex.* art. 494 c.p.

E ancora, è stata ricondotta al paradigma normativo dell'art. 494 c.p., la condotta di chi crea un profilo su un *social network* utilizzando l'immagine di un altro individuo senza l'autorizzazione di questo, al fine di comunicare con altri utenti e pubblicare contenuti sul *web*[196].

Infatti, se l'originaria formulazione della norma era volta alla tutela dell'identità personale, con l'avvento di Internet il nostro ordinamento accorda una tutela sempre

---

[193] REDAZIONE ALTALEX, *Cybercrime: sostituzione di persona mediante furto di identità digitale,* in *altalex.,* 2019, https://www.altalex.com/documents/news/2019/04/12/sostituzione-di-persona-mediante-furto-di-identita-digitale.

[194] Cass. pen., Sez. V, 15 giugno 2016, n. 34800, in *www.dejure.it.*

[195] Cass. pen., Sez.V, 8 novembre 2007, n. 46674, in *Cass. Pen.*, 2008, 7-8, 2878.

[196] Cass. pen. Sez. V, 2 aprile 2014, n. 25744, in *Giur. Pen.*, 2014, p. 804; Cass. pen., Sez. V, 30 gennaio 2018, n. 4413, in *www.dejure.it*.

maggiore anche alla cosiddetta *identità digitale*[197], la quale è oggi espressamente riconosciuta dall'art. 9 del D.L. 93 del 2013[198]. Con tale termine si indica la «rappresentazione informatica della corrispondenza biunivoca tra un utente ed i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale»[199].

D'altronde, costituendo il profilo *web* l'insieme degli aspetti che caratterizzano e individuano un utente, oggi il profilo digitale non può che integrare un'importante forma di rappresentazione dell'individuo[200]. Di conseguenza, secondo quanto affermato dalla Corte di Cassazione[201], l'ordinamento giuridico italiano considera integrato l'art. 494 c.p. in tutte le ipotesi di violazione di un *account social* altrui già esistente per finalità generiche di vantaggio dell'agente o di danno del soggetto passivo, ovvero nei casi in cui viene utilizzata un'immagine altrui come fotografia di un profilo *social*[202].

Con riferimento a tale seconda ipotesi, il caso di specie riguardava un uomo adulto, il quale aveva creato un falso profilo *Facebook* utilizzando un'immagine di un minore realmente esistente, trovata sul profilo *social* di questo, con la finalità contattare per scopi illeciti alcune utenti, anch'esse minorenni.

Tralasciando gli altri reati configurati nel caso in esame, per quel che concerne il reato di sostituzione di persona la Suprema Corte ha confermato la condanna dell'uomo per i delitti di cui all'art. 494 c.p, così ribadendo l'orientamento già espresso nella pronuncia 25774 del 23 aprile 2014[203], secondo cui integra il reato di sostituzione di persona la condotta di chi crea su una piattaforma *social* un falso profilo utilizzando l'effige del soggetto offeso e, successivamente, utilizza con tale profilo *fake* i servizi del *socia network*, quali la possibilità di instaurare

---

[197] RODOTÀ, *Quattro paradigmi per l'identità*, in *Il diritto di avere diritti*, Bari, 2012, pp. 298-310; RESTA, *Identità personale e identità digitale*, in *Dir. Informatica*, fasc.3, 2007, pp. 511 ss.

[198] Convertito dalla L. 15.10.2013, n. 119.

[199] Decreto Semplificazione e innovazione digitale, DL. 76/2020.

[200] GAETA, *La protezione dei dati personali nell'internet of things: l'esempio dei veicoli autonomi*, in *Dir. informaz. e informatica*, fasc. 1, 1.2.2018, pp. 147 ss; MALGERI, *Il furto di "identità digitale": una tutela "patrimoniale" della personalità,* in *La giustizia penale nella "rete", le nuove sfide della società dell'informazione nell'epoca di Internet,* FLOR, FALCINELLI, MARCOLINI (a cura di), 2015, p. 37.

[201] Cass. pen, Sez. V, 8 giugno 2018, n. 33862, in *Dir. Pen. Cont*. 21 giugno 2019.

[202] Cass. pen., Sez. V, 10 ottobre 2017, n. 4413, in www.dejure.it; Cass. Pen., Sez. V, 22 giugno 2018, n. 42572, in www.dejure.it.

[203] Cass. pen., Sez. V, 23 aprile 2014, n. 25774, con nota di SANSOBRINO, *Creazione di un falso account, abusivo utilizzo dell'immagine di una terza persona e delitto di sostituzione di persona*, in *Dir. Pen Cont.*, 30 settembre 2014.

conversazioni con altri utenti, al fine di ottenere un vantaggio o di recare un danno alla persona offesa.

Allo stesso modo, la Corte di Cassazione in una recentissima pronuncia ha ritenuto integrata la fattispecie della sostituzione di persona nel caso in cui un soggetto crei un *account* su un sito Internet facendo uso delle altrui generalità[204]. Il caso specifico riguardava un individuo che, essendo impossibilitato ad accedere al sito di *eBay* con il proprio account in quanto *bannato* dalla stessa piattaforma, aveva aperto un nuovo *account* usando l'identità di un ex socio, dietro il pretesto di fornirgli aiuto in alcuni acquisti sul *web*. In un secondo momento, però, l'imputato ha deciso di usare i dati dell'ex socio anche per creare un *account* su un sito Internet dedicato al gioco d'azzardo.

Secondo quanto affermato dalla Corte, a nulla rilevano né l'eventuale consenso all'uso delle generalità da parte dell'effettivo titolare, né i motivi che hanno spinto l'agente, al contrario, assumono rilevanza solo la creazione di un'apparenza nei rapporti tra gli utenti idonea a trarre in inganno e realizzata con la finalità di acquisire un vantaggio, ovvero di arrecare un danno al soggetto passivo.

Un'altra circostanza in cui la Suprema Corte ha ritenuto integrato il reato di sostituzione di persona, fa riferimento all'ipotesi di utilizzo su un sito di incontri dell'altrui *nickname* e numero telefonico,[205] ovvero di attribuzione di una qualifica professionale falsa su un *social network* quale *Skype* o *LinkedIn.*

Infatti, la Corte di Cassazione ha osservato che l'identità e le qualità prospettate nel profilo digitale di un soggetto non sono affatto indifferenti per gli altri utenti, poiché è proprio sulla base di queste ultime che gli stessi decidono se instaurare o meno un primo reciproco contatto[206].

Un problema ad oggi ancora irrisolto, e quindi oggetto di dibattito in dottrina, è costituito da quei casi in cui l'utente sostituisce la propria identità non a quella di un'altra persona realmente esistente, bensì a quella di un personaggio di fantasia o inesistente.

La dottrina e la giurisprudenza maggioritarie[207], poggiandosi sul principio della general-prevenzione e quindi su un giudizio *ex. ante* che tiene conto solo delle

---

[204] Cass, pen., Sez. V, 20 febbraio 2019, n. 7808, in *www.dejure.it.*

[205] Cass. pen., Sez. V, 28 novembre 2012, n. 18826, in *www.dejure.it*.

[206] Cass. pen., Sez. V, 14 dicembre 2007, n. 46674, in *www.dejure.it.*

[207] Cass. pen Sez. II, 21 dicembre 2011, n. 4250, in *www.dejure.it;* Cass. pen., Sez. V, 8 novembre 2007, n. 46674, in *www.dejure.it*; STAMPANONI BASSI, *Sostituzione di persona commessa nella rete*

informazioni conosciute o conoscibili al momento della commissione del reato[208], ritengono che il delitto *ex.* art. 494 c.p. si configuri ugualmente qualora l'identità sottratta concerna una persona che, ancorché inesistente, appaia reale in quanto provvista di un nome e un cognome verosimili.

Al contrario, si tende a ritenere che qualora un soggetto si appropri delle generalità di un personaggio palesemente di fantasia il reato non sussiste, in quanto l'utente è necessariamente consapevole dell'inesistenza del personaggio; si pensi ad esempio a Paperino o Diabolik.

Infine, in tema di sostituzione di persona sui *social network*, appare opportuno ricordare la nuova normativa introdotta con il Regolamento dell'Unione Europea 2016/679, cosiddetto GDPR, il quale ha l'obiettivo di limitare i casi di sostituzione di persona *online*, rendendo più difficilmente attaccabili i *database* informatici. Nonostante ciò, il reato di sostituzione di persona *on-line* si può configurare in tutte le ipotesi in cui un soggetto forzi le credenziali di accesso del soggetto passivo, effettuando poi abusivamente operazioni per conto di quest'ultimo, o, più semplicemente, qualora un soggetto menta sulla propria età al momento dell'iscrizione su un *social network*, in quanto attribuirsi un'età falsa equivale ad attribuirsi una falsa qualità ai sensi dell'art. 494 c.p.[209].

In conclusione, nonostante l'assunzione dell'altrui identità non rappresenti affatto un fenomeno giuridico di nuova o recente formazione, nell'era della Post-Verità l'avvento di Internet ha fatto sì che si sia assistito a una proliferazione del reato di sostituzione di persona, mediante la creazione di profili *fake* o l'indebito accesso ad *account* altrui sui *social network.*[210]

Dunque, avendo analizzato la disciplina penalistica italiana applicabile ai soggetti che diffondono *fake news* su Internet, risoluta, ora, interessante delineare il quadro regolatorio della responsabilità delle piattaforme digitali per i cosiddetti *user-generated contents;* ponendo a confronto le soluzioni adottate nell'ambito dell'Unione Europea e nell'ordinamento statunitense.

---

internet, IN *Cass. pen.*, n. 1, 2014, P. 147; PAGLIARO, voce *Falsità personale*, in *Enc. Dir.*, Milano, 1967, p. 646; MANZINI, *Trattato di diritto penale italiano*, vol. VI, Torino, 1983, 976; FIANDACA MUSCO, *Diritto penale. Parte speciale*, vol. I, Zanichelli, 2012, p. 621; FLICK, *Falsa identità su internet*, in *Dir. informaz. e informatica*, 2008, p. 527.

[208] MANTOVANI, *Manuale di diritto penale*, parte generale, 10ª ed., Padova, 2017, pp. 453 ss.

[209] PERINI, *Cybercrime: sostituzione di persona mediante furto di identità digitale*, cit.

[210] PICOTTI, *I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali*, in *Giur. mer.*, 2012, n. 12, pp. 2522 ss.

CAPITOLO III

III. LA RESPONSABILITÀ DEGLI *INTERNET SERVICE PROVIDERS*

3. Gli *Internet Service Providers*: definizione e ontologia

L'evoluzione delle nuove tecnologie, l'avvento di nuove piattaforme, l'ingresso dei *social network* nel panorama di Internet e le modifiche che tutto ciò ha comportato alla dimensione partecipativa che caratterizza l'era della Post-Verità, hanno condotto a un inevitabile ripensamento circa le tradizionali categorie di inquadramento degli *Internet Service Provider* (ISP). Nello specifico, lo scenario in esame ha suscitato delle riflessioni sull'adeguatezza della disciplina vigente, soprattutto con riferimento alla responsabilità degli ISP per gli *user-generated contents*[211].

Con il termine *Internet Service Provider* si fa riferimento a «quelle organizzazioni che offrono ai propri utenti accesso alla rete Internet e/o servizi in qualche modo connessi all'utilizzo della stessa»[212].

Tra gli ISP possiamo poi distinguere diverse categorie. Riprendendo la suddivisione suggerita da Giovanni Pitruzzella nel libro "Parole e Potere, libertà di espressione, *hate speech* e *fake news*", è possibile individuare le seguenti tipologie: i *content provider*, ossia i fornitori e autori dei contenuti pubblicati sui propri *server*; i *network provider*, si tratta di soggetti che si limitano a fornire accesso alla rete attraverso Internet; i *mere conduit*, vale a dire coloro che offrono agli utenti accesso a Internet; i *caching provider*, cioè di soggetti che memorizzano i dati provenienti dall'esterno in un'area di temporanea allocazione; e infine, gli *hosting provider* che forniscono ai siti *web* "ospitalità" e una memorizzazione durevole dei dati.

Negli anni più recenti, tuttavia, le innovazioni tecnologiche hanno portato a un significativo ampliamento delle attività svolte dagli *Internet Service Providers.* Ciò ha reso progressivamente più difficile far rientrare tali soggetti nelle tradizionali

[211] POLLICINO, *Tutela e pluralismo nell'era digitale: ruolo e responsabilità degli Internet service providers*, in *Consulta Online*, 2014, p. 3.
[212] PITRUZZELLA, POLLICINO, QUINTARELLI, *Parole e Potere, libertà d'espressione, hate speech e fake news*, cit., p. 80.

categorie sopra elencate, rendendo, quindi, necessario un ripensamento sulla disciplina a questi applicabile, soprattutto in tema di responsabilità.

Per comprendere tale evoluzione basti pensare ai servizi offerti dai motori di ricerca, dalle piattaforme *social,* e dalle piattaforme che aggregano contenuti pubblicati d soggetti terzi – quale ad esempio *YouTube*. Questi *provider* svolgono una molteplicità di servizi: a titolo esemplificativo, essi pongono in essere attività di indicizzazione, selezione e organizzazione di contenuti e filtraggio di materiale diffuso *on-line*, con la finalità di realizzare utili di impresa[213].

Lasciando ai paragrafi successivi un'analisi approfondita delle soluzioni prospettate nei vari ordinamenti, in prima approssimazione risulta opportuno sottolineare che la dottrina, nel corso del tempo, ha individuato due diversi paradigmi di responsabilità che potrebbero trovare applicazione nei confronti degli *Internet Service Providers*: la cosiddetta *strict liability* e un sistema basato sulla *fault,* ossia sulla colpa[214].

Per quanto concerne il primo, si tratta di un sistema in cui un *provider* sarebbe responsabile dei contenuti pubblicati da terzi, a prescindere dalla sua conoscenza e dalla sua materiale possibilità di esercitare un controllo sul materiale che è trasmesso attraverso la sua piattaforma[215].

Si tratta indubbiamente di un approccio molto rigido, in quanto questo prevede la possibilità di considerare responsabile un ISP, anche se di fatto questo non aveva alcuna conoscenza o controllo su un determinato contenuto, per il semplice fatto che il materiale in questione è stato pubblicato sullo stesso.

Seguendo il modello basato sulla colpa, invece, gli *Internet Service Providers* sarebbero ritenuti responsabili dei contenuti ivi pubblicati solo in caso di una loro violazione intenzionale dei diritti di soggetti terzi.

Nell'ambito di questo paradigma, è poi necessario distinguere a seconda che si prenda in considerazione la cosiddetta *constructive knowledge* o la *actual knowledge.* Nel primo caso, per integrare la responsabilità dell'ISP sarebbe sufficiente il fatto che, sulla base di determinati indizi o informazioni, questo

---

[213] D'ALFONSO, *Verso una maggiore responsabilizzazione dell'hosting provider tra interpretazione evolutiva della disciplina vigente, innovazioni legislative e prospettive de jure condendo,* in *Federalismi.it,* n. 2/2020, p. 114.

[214] BAISTROCCHI, *Liability of intermediary service providers in te EU directive on electronic commerce*, in *Computer and high technology law journal*, 2003, vol. 19, p. 114.

[215] BARCELO, *Liability for online intermediaries: A European Perspective*, in *Centre de recherches informatique et droit,* 1998, pp. 7-10.

avrebbe dovuto ragionevolmente presumere che alcuni contenuti fossero lesivi di diritti altrui.

Nel secondo caso, invece, ossia prendendo in considerazione la *actual knowledge*, gli *Internet Service Providers* sarebbero responsabili solo a condizione che questi abbiano una conoscenza effettiva della presenza di materiale illecito sulla propria piattaforma.

Dunque, se da un lato il modello di responsabilità basato sulla colpa, può dirsi meno rigido rispetto al paradigma della *strict liability*, dall'altro, come evidenziato dallo *UN Special Rapporteur* Frank La Rue, in ogni caso qualsiasi sistema si scelga permane la possibilità che gli ISPs di fronte al rischio di essere considerati finanziariamente e penalmente responsabili dei contenuti che non rimuovono, una volta avuta notizia dell'illiceità degli stessi, cadano in una censura eccessiva di materiale anche solo potenzialmente lesivo di diritti altrui[216].

Alla luce di ciò, nel corso del tempo si sono succeduti diversi tentativi, essenzialmente di matrice giurisprudenziale, di classificare gli ISPs inquadrandoli in una specifica disciplina.

La responsabilità delle piattaforme per i contenuti pubblicati da soggetti terzi, infatti, è uno dei principali temi che ha caratterizzato l'industria di Internet, già dalla sua fase emergente negli anni '90 del secolo scorso. I primi casi in materia hanno riguardato principalmente gli Stati Uniti, concernendo la responsabilità dei primi *Internet Service Providers,* quali AOL e CompuServe, per l'attività di *hosting*, trasmissione e pubblicazione di contenuti diffamatori o altrimenti illeciti[217].

A partire dall'inizio degli anni 2000, si è, poi, formato un consenso, tanto nel continente Europeo quanto nel continente Americano, sulla necessità di trovare un bilanciamento tra i diversi interessi in gioco, individuando una disciplina organica, moderna e conforme ai vari ordinamenti giuridici[218].

Ad oggi possiamo distinguere due diversi approcci alla regolamentazione della responsabilità degli *Internet Service Providers:* uno "orizzontale" e l'altro

---

[216] *Report of Special Rapporteur on the Promotion and protection of the right to freedom of opinion and expression, Frank la Rue on the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet*, A/HRC/17/27, 16 May 2011, para 42.

[217] *OECD Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy, the role of internet intermediaries in advancing public policy objectives- Forging partnerships for advancing policy objectives for the Internet economy*, Part II, 22 June 2012, p. 10.

[218] AVIGNO, *Intermediary Liability for User-Generated Content in Europe*, Tallinn University of Technology, Tallinn 2016, p. 17.

"verticale"[219]. Come vedremo meglio nei paragrafi successivi, il primo modello è abbracciato dalla Direttiva CE n. 31 del 2000, nota come Direttiva *E-Commerce*. Si tratta di un paradigma regolatorio che suddivide gli *Internet Service Providers* in categorie sulla base delle funzioni da questi svolte, e prevede specifiche limitazioni di responsabilità per ciascuna di queste.

L'approccio "verticale", al contrario, prevede regole specifiche circa la responsabilità degli ISPs sulla base dell'ambito in cui questi operano; distinguendo, ed esempio, il copyright, la tutela dei minori, i discorsi d'odio e la diffamazione.

L'emblema di questo secondo modello è rappresentato dagli Stati Uniti i quali negli anni hanno emanato leggi *ad hoc* per ogni ambito di operatività dei *providers*: a titolo esemplificativo possiamo ricordare il *Communication Decency Act, il Defamation Act e il Digital Communication Act*[220].

3.1. La Responsabilità degli *Internet Service Providers*: l'esperienza Statunitense

Prima dell'adozione del *Communication Decency Act*, nell'ambito della *common law* statunitense agli ISPs che diffondevano materiale lesivo dell'altrui reputazione veniva applicava la disciplina generale in tema di diffamazione[221].

Ai sensi del secondo *Restatement of Torts* statunitense, il reato di diffamazione tutela gli individui privati e le società da affermazioni false diffuse per ledere la loro reputazione privata o professionale[222]. E', inoltre, importante sottolineare che nell'ambito della *common law* la responsabilità per la divulgazione di materiale diffamatorio si estende al di là dell'originario autore, fino a ricomprendere i cosiddetti *secondary disseminators,* ossia tutti i soggetti che successivamente diffondano la notizia lesiva dell'altrui reputazione[223].

---

[219] RODRIGUEZ RENGIFO, *Internet Intermediaries Liability: Participative Networking Platforms and Harmful Content,* in *Researchgate.net*, 2016, p. 14; EDWARDS, *Role and Responsibility of internet intermediaries in the field of copyright and related rights*, 2011, p. 7.

[220] EDWARDS, *Role and Responsibility of internet intermediaries in the field of copyright and related rights,* cit., p. 7.

[221] Stratton Oakmont, Inc. v. Prodigy Servs Co. No. 31063/94, 1995 N.Y. Misc.; 7 Coffey v. Midland Broadcasting Co., D. C. Mo., 1934; Gertz v Robert Welch, Inc., 418 U.S., 1974; New York times v. Sullivan, 376 U.S. 1964.

[222] *Restatement second of torts*, 1977, para 577.

[223] New York Times v. Sullivan, 376, U.S., 1964, paras 254, 267.

Ad oggi, le Corti statunitensi distinguono i *secondary disseminators* tra *publishers*, *distributors e common carriers*, applicando a ciascuno di questi *standard* di responsabilità diversi[224].

Per quanto concerne i primi, si tratta di coloro che diffondono molto rapidamente grandi quantità di informazioni, ma che non sono né legalmente né tecnicamente idonei a monitorare e controllare tali contenuti. Ne consegue che questi non possono essere ritenuti responsabili per le informazioni divulgate, a prescindere dalla loro consapevolezza o ignoranza circa il carattere diffamatorio di suddette informazioni[225]. Un esempio di *common carrier* è rappresentato dalle compagnie telefoniche.

I *distributors*, come ad esempio le televisioni, invece, sono soggetti che a differenza dei primi possiedono un certo margine di discrezionalità nel limitare il materiale che diffondono[226], e che, quindi, teoricamente potrebbero monitorare e controllare tutte le informazioni che diffondono, ma che, tuttavia, difettano delle risorse necessarie per svolgere tale attività assicurando la veridicità delle informazioni trasmesse[227].

In altre parole, non essendo per i *distributors* possibile controllare tutte le informazioni che diffondono[228], la loro responsabilità rimane limitata[229]. Nello specifico, nel corso del tempo le Corti hanno ritenuto i *distributors* responsabili per aver stampato o diffuso un'informazione lesiva dell'altrui reputazione solo nelle circostanze in cui questi, pur avevano una *actual* o *constructive knowledge* che quello specifico contenuto era qualificabile come diffamatorio, non hanno adottato le misure necessarie al fine di rimuoverlo[230].

Per quanto riguarda, infine, i *publishers*, tale termine viene utilizzato nella prassi della giurisprudenza americana per indicare «un soggetto che renda pubblico qualcosa»[231]. A differenza dei *distributors*, in ragione del controllo che questi esercitano sul materiale divulgato, i *publisher* possono essere ritenuti responsabili

[224] ROLAND, *Rethinking Defamation Liability for Internet Service Providers*, in *Suffolk University Law Review*, 2001, pp. 651-653.
[225] *Ivi*, p. 651.
[226] Auvil v. CBS 60 Minutes ,800, F. Supp., E.D. Washington, 1992.
[227] Smith v. california, 361 U.S., 1959; Cianci v. New York Times Publ'g Co., 639 F. 2d, 1980.
[228] New York Times v. Sullivan, 376, U.S., 1964.
[229] Cianci v. New York Times Publ'g Co., 639 F. 2d, 1980.
[230] Auvial v. CBS 60 Minutes, 800, F. Supp., E.D. Washington, 1992.
[231] Klayman v. Zuckerberg, 753, D.C. Circ., 2014, paras 1354, 1359.

per aver stampato o diffuso contenuti diffamatori, o altrimenti lesivi dell'altrui reputazione[232].

Per quanto concerne l'analisi della possibilità di qualificare gli ISPs come *secondary disseminators*, una delle prime pronunce da prendere in considerazione è, senz'altro, quella concernente il caso *Daniel v. Dow Jones and Co*[233]. Il caso in esame riguardava una causa presentata da un investitore nei confronti della compagnia Dow Jones. Quest'ultimo invocava una presunta responsabilità della compagnia dovuta al fatto che a questo erano state comunicate informazioni fuorvianti attraverso il servizio Internet di notizie sugli investimenti fornito dalla Dow Jones[234].

La Corte, tuttavia, ha statuito che, non sussistendo alcuna differenza sostanziale tra un giornale cartaceo e un sito di notizie *on-line*, la società Dow Jones doveva essere considerata alla stregua di un giornale.

La tematica della possibilità di considerare gli *Internet Service Providers* come *secondary disseminators* è stata, poi, ripresa dalle Corti statunitensi quattro anni dopo nel caso *Cubby Inc. v. CompuServe Inc*[235].

Il caso in questione riguardava la responsabilità dell'ISP CompuServe per aver fornito accesso ad articoli di una parte terza che, secondo l'accusa, contenevano affermazioni diffamatorie.

Nel pronunciarsi sulla questione, la Corte ha fatto riferimento al caso *Smith v. California*[236], in cui la Corte Suprema, se pur non con riferimento al *web*, aveva definito lo *standard* da applicare ai *distributors* al fine di determinare la responsabilità di questi per i contenuti diffusi.

Alla luce di ciò, la Corte ha statuito che l'ISP CompuServe non potesse essere ritenuto responsabile delle affermazioni diffamatorie diffuse, in quanto questo non era in grado di esercitare un controllo editoriale sulla totalità del materiale divulgato paragonabile a quello posto in essere dai giornali[237].

In altre parole, la Corte ha rigettato la teoria attorea secondo cui l'ISP in questione sarebbe dovuto essere considerato come un *publisher*, al contrario abbracciando la

[232] Gertz v. Robert Welch, Inc, 418 U.S., 1974, paras 323,325-30.
[233] Daniel v. Dow Jones and Co., 520 N.Y.S., 1987.
[234] *Ibidem* paras 337-38.
[235] Cubby, Inc. v. CompuServe, Inc., 776 F. Supp., S.D.N.Y. 1991, paras 135, 141.
[236] Smith v. California 61 U.S. 147, 1959, paras 152-53.
[237] *Ivi*, paras 139-140.

tesi della difesa in base alla quale a CompuServe doveva essere applicato lo *standard* di responsabilità proprio dei *distributors*[238].

Nello specifico la Corte, dopo aver affermato che «*the New York Courts have long held that […] distributors of defamatory publications are not liable if they neither know nor have reasons to know of the defamation*»[239], ha continuato sottolineando che tale statuizione è profondamente e implicitamente radicata nel primo emendamento in quanto «*constitutional guarantees of the freedom of speech and of the press stand in the way of imposing strict liability on distributors for the contents of the reading materials they carry*»[240].

Infine, la Corte ha concluso evidenziando che applicare uno *standard* più rigido di quello previsto per i *distributors* vorrebbe dire imporre un eccessivo onere sulla libera circolazione delle informazioni[241]. Di conseguenza, questa ha ritenuto che nel caso in esame fosse adeguato applicare il regime di responsabilità previsto per i *distributors*, anche alla luce della velocità con cui le informazioni sono raccolte e processate su Internet[242].

Un esito molto diverso dalla sentenza in esame si ebbe quattro anni dopo nella pronuncia di un'altra Corte di New York sul caso *Stratton Oakmont, Inc. v. Prodigy Services Co*[243].

Nel caso in questione, una società aveva fatto causa al *computer network* Prodigy, per aver permesso la pubblicazione di affermazioni lesive della reputazione di questa.

A differenza del caso Cubby, la Corte ha qualificato l'ISP come *publisher* conseguentemente ritenendolo responsabile per la violazione dello *standard* di negligenza[244]. Nello specifico, la Corte ha motivato la propria decisione affermando che «*Prodigy has uniquely reserved to itself the role of determining what is proper for its members to post and read on its bulletin boards*»[245].

In altre parole, la statuizione della Corte si è basata su due punti fondamentali: il fatto che lo stesso ISP qualificava se stesso come un *family network* in grado di

[238] *Ivi*, paras 135,140.
[239] *Ivi*, para 139.
[240] *Ibidem*, a sua volta citando Smith v California, 361 U.S. 147, 1959, 152-53.
[241] *Ivi*, para 140.
[242] *Ibidem*.
[243] Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995.
[244] *Ivi*, paras 7-12.
[245] *Ivi*, paras 4-5.

controllare ed esercitare attività editoriale su tutto il contenuto pubblicato, e il fatto che questo aveva implementato la propria attività di monitoraggio attraverso *software* di *screening* e l'assunzione di soggetti specificatamente preposti a svolgere funzioni di controllo editoriale sul contenuto delle informazioni diffuse dal *network* in questione[246].

La disciplina statunitense sulla responsabilità degli *Internet service providers*, trovò, poi, una sistemazione compiuta quando nel 1996 il Congresso approvò il *Telecommunications Act*, il cui Titolo V è noto come il *Communication Decency Act.*

Per quel che interessa la presente trattazione, la sezione 230 (c) (1) prevede che «*no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider*».

La disposizione chiarisce che con la locuzione *interactive computer service*[247] si fa riferimento a tutti i servizi di informazione, o ai *provider* di *software*, che forniscano o abilitino l'accesso a un unico *server* a una molteplicità di *users*[248].

La nozione di *content provider*[249], invece, indica ogni persona o ente che sia in tutto o in parte responsabile per la creazione e lo sviluppo dei contenuti che sono trasmessi tramite il *web* od ogni altro *interactive computer service.*

E ancora, alla sezione 230 (c) (2) (A) viene statuito che «*no provider or user of an interactive computer service shall be held liable on account of:*

A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected».

---

[246] FRITTS, *Internet libel and communication decency act: how the courts erroneously interpreted Congressional intent with regard to liability of internet service providers*, in *Kentucky Law Journal*, vol. 93, issue 3, 2005, p. 771; ROLAND, *Rethinking Defamation Liability for Internet Service Providers*, cit., p. 656.

[247] 47 U.S. Code § 230 (C)(f)(2) con nota di MIRANDA, *Defamation in Cyberspace: Stratton Oakmont, Inc. v. Prodigy Services Co*., in *Albany Law Journal of Science & Technology*, 1996, pp. 229-248; JOHNSON, *Defamation in Cyberspace: A Court Takes a Wrong Turn on the Information Superhighway in Stratton Oakmont, Inc. v. Prodigy Services Co*., in *Arkansas Law Rev*iew, 1997, pp. 589-624. SIDERITS, *Defamation in Cyberspace: Reconciling Cubby, Inc. v. Compuserve, Inc. and Stratton Oakmont v. Prodigy Services Co*., in *Marquette Law Review*, 1996, pp. 1065-1082.

[248] La sezione 230 (C)(f)(4) definisce gli *access software provider*, come i providers di software (client o software) o coloro i quali forniscano strumenti che permettano: (a) di filtrare, selezionare, permettere o bloccare contenuti; (b) di scegliere, individuare, analizzare o classificare contenuti o (c) trasmettere, ricevere, mostrare, inoltrare, nascondere, cercare, organizzare, riorganizzare o tradurre contenuti.

[249] 47 U.S. Code, sezione 230 (C)(f)(3).

In altre parole, secondo quanto previsto dalla sezione 230 della summenzionata normativa, il semplice fatto che gli ISPs svolgano un'attività che comporta responsabilità simili a quelle previste per gli editori, non è sufficiente al fine di qualificare questi come *publishers*.

Risulta evidente che la *ratio* sottesa alla disposizione è quella di evitare che un *Internet Service Provider* possa essere ritenuto responsabile o corresponsabile del materiale che viene pubblicato dagli utenti, qualificando gli ISPs come meri fornitori di uno spazio su Internet nel quale soggetti terzi possono pubblicare contenuti; evitando che per ciò stesso il concedente divenga automaticamente responsabile dell'eventuale illiceità degli stessi[250].

Di fatto, mediate queste disposizioni, note come le "regole del buon samaritano", è stata ribaltata la decisione del caso Stratton, e, al contrario, è rimasto inalterato quando emerso nella pronuncia Cubby.

Infatti, il Congresso ha esplicitamente affermato che «*one of the specific purposes of this section is to overrule Stratton Oakmont […] and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material*»[251].

Negli anni successivi sono intervenute due pronunce che, a parere di una parte della dottrina[252], hanno espanso l'applicabilità della sezione 230 del *Communication Decency Act* al di là di quanto esplicitamente previsto dal Congresso in fase di stesura dello stesso: il caso *Zeran v. America Online, Inc*. e il caso *Blumenthal v. Drudge*.

La pronuncia *Zeran v. America Online, Inc.*[253] è stata la prima a fornire un'interpretazione della normativa in esame.

Il caso aveva ad oggetto l'accusa rivolta alla piattaforma American Online (AOL) da parte di un residente di Seattle di aver rimosso dei commenti diffamatori pubblicati sulla stessa con un irragionevole ritardo. La Corte, tuttavia, ha accolto la

---

[250] BACCIN, *Responsabilità penale dell'Internet Service Provider e concorso degli algoritmi negli illeciti online: il caso force v Facebook*, in *Sistema penale*, 5/2020, p. 86.

[251] Senate Report, No. 104-230 para 194.

[252] FRITTS, *Internet libel and Communication Decency Act: how the courts erroneously interpreted Congressional intent with regard to liability of internet service providers*, cit., p. 775; SHERIDAN, *Zeran v. AOL and the effect of section 230 of the Communications Decency Act upon liability for defamation on the Internet*, in *Albany Law Review*, 1997, pp. 147, 150.

[253] Zeran v. America Online, Inc. 129 F. 3d, 4th Cir., 1997.

difesa dell'ISP, nella quelle veniva invocata l'immunità prevista dall'art. 230 del *Communicatin Decency Act*, in base alla quale la piattaforma non poteva essere ritenuta responsabile di un eventuale contenuto diffamatorio di materiale pubblicato da soggetti terzi.

Nonostante tale decisione possa apparire una mera ripetizione di quanto affermato da altre Corti statunitensi nei casi precedentemente analizzati, in realtà il caso in questione ha una portata profondamente innovativa.

Infatti, la vicenda in esame più che avere ad oggetto una presunta responsabilità dell'ISP per aver esercitato un'attività editoriale su un contenuto poi risultato diffamatorio, riguarda la responsabilità dell'America Online in quanto *distributor*. L'attore, in effetti, lamenta la responsabilità del presunto *distributor* per non aver rimosso un contenuto nonostante fosse a conoscenza del carattere diffamatorio di questo.

Ne consegue che, stando alla lettera del testo dell'art. 230, in realtà questa controversia non avrebbe dovuto comportare l'applicazione della suddetta norma.

Proprio a tal riguardo, tuttavia, la Corte si è espressa affermando che quando il Congresso ha utilizzato il termine "*publisher"* nella sezione 230 in realtà intendeva includere anche il *distributor* perché la responsabilità di quest'ultimo non è altro che una *species* della responsabilità del primo[254].

Da ciò è conseguita la scelta della Corte di rigettare la teoria dell'attore secondo cui l'immunità garantita dalla sezione 230 del *Communication Decency Act* esonererebbe da responsabilità solo il *publisher*, lasciando inalterata quella del *distributor*[255].

A tal riguardo la Corte ha affermato che «*it would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress…chose to immunize service providers to avoid any such restrictive effect*»[256].

[254] *Ivi*, para 332.
[255] *Ivi*, para 331.
[256] Zeran v. America Online, Inc., 129 F.3d, 4th Cir., 1997, para 327, citato in Force v. Facebook, No. 18-397, 2nd Cir. 2019, p. 25 con nota di PANTAZIS, *Zeran v. America Online, Inc.: Insulating Internet Service Providers from Defamation Liability*, in *Wake Forest L. Rev.*, 1999, pp. 531-566.

Per quanto concerne la seconda pronuncia, ossia quella che ha visto contrapposti *Blumenthal* e *Drudge*[257], si tratta di un caso che assume particolare rilevanza in tema di *fake news.*

Nella vicenda in esame un giornalista aveva stipulato con AOL un contratto che prevedeva che la colonna di gossip affidata a questo sarebbe stata accessibile per un anno ai membri della piattaforma AOL. Il 10 agosto 1997, il giornalista ha pubblicato una storia secondo cui l'assistete di Clinton avrebbe abusato di sua moglie nel passato. Tale storia si è poi rivelata falsa, in quanto meramente frutto dell'immaginazione della fonte di Drudge. Il soggetto interessato ha, quindi, intentato una causa sia nei confronti del giornalista che nei confronti di AOL, ritenendoli entrambe responsabili sulla base del rapporto contrattuale esistente tra i due.

Anche in questo caso, l'ISP ha invocato la tutela assicuratagli dalla sezione 230 del *Communication Decency Act,* tutela che gli è stata garantita dalla Corte, la quale ha ritenuto la normativa in questione applicabile.

Tale pronuncia, tuttavia, è stata oggetto di grande dibattito, soprattutto in quanto parte della dottrina[258], soffermandosi sull'esistenza di un rapporto contrattuale tra il giornalista e la piattaforma, ha affermato che sussiste una differenza notevole tra il ritenere che non potesse essere imposto ad AOL di effettuare un controllo generalizzato sui contenuti pubblicati sul suo *bulletin board*, e il sostenere che l'ISP non avesse sufficiente personale o capacità per leggere una copia dell'articolo in questione prima di pubblicarlo sul sito; anche considerando il rapporto contrattuale che la piattaforma aveva instaurato con il giornalista.

La decisione sulla vicenda Zeran è poi stata ripresa nel 2001 dalla Corte Suprema della Florida nella pronuncia sul caso *Do v. America Online, Inc*[259]. Anche in questa occasione, la Corte ha escluso che l'ISP, in quanto *distributor*, potesse essere considerato responsabile per la mancata rimozione di materiale diffamatorio pubblicato da soggetti terzi, anche dopo averne ricevuto notizia.

[257] Blumenthal v Drudge, 992, F. Supp., DDC, 1998.
[258] LABUNSKI, *The second constitutional convention: how the American people can take back their government*, 2000, p. 255
[259] Do v. America Online, Inc. 783, So. 2d. 1010, 2001.

Risulta, tuttavia, particolarmente interessante l'opinione dissenziente del giudice Lewis, in cui viene critica l'eccessiva estensione dell'ambito di applicabilità dell'art. 230 del *Communication Decency Act.*

Questo, infatti, ha affermato che né lo statuto né la storia legislativa statunitense «*reflect an intent to totally exonerate and insulate an ISP from responsibility where […] it is alleged that an ISP has acted as knowing distributor*»[260].

A conferma di quanto espresso dal giudice Lewis, pochi anni dopo, due pronunce di grande rilevanza si sono contrapposte a quanto statuito nel caso Zeran, distinguendo nettamente la responsabilità dei *publisher* da quella dei *distributors:* si tratta dei casi *Bratzel v Smith e Barrett v Rosenthal*[261].

A titolo esemplificativo, nella pronuncia sulla vicenda Barrett la Corte ha affermato che quando viene distinta la responsabilità dei *publisher* da quella dei *distributors*, i più eminenti esperti utilizzano il termine *publisher* con riferimento al *primary publisher*, anche quando l'oggetto della divulgazione è la diffusione di un contenuto nel *cyberspace*.

In conclusione, si può affermare che, a seguito delle citate pronunce la tradizionale distinzione tra *publisher* e *distributors* abbia nuovamente trovato applicazione nell'ambito della *common law* statunitense, anche con riferimento agli *Internet Service Providers.* Di conseguenza, la responsabilità degli ISPs per contenuti ivi pubblicati scatta una volta che questi vengono a conoscenza della natura diffamatoria dei suddetti materiali. In altre parole, nell'eventualità in cui un *Internet Service Provider* riceva notifica della lesività di un contenuto, questo è tenuto a rimuoverlo al fine di non incorrere in responsabilità[262].

Tale approccio è stato ulteriormente confermato nel caso *Viacom v. YouTube* del 2007[263], in cui la Corte distrettuale ha ritenuto che non sussistesse alcuna responsabilità in capo al *provider* in relazione alle contestate violazioni del diritto di autore, dal momento che nella *common law* statunitense una conoscenza solamente generica e non specifica non è sufficiente a far scattare l'obbligo di attivazione della piattaforma per la rimozione di materiale. Al contrario, tale onere

[260] Do v. America Online, Inc. 783, So. 2d. 1010, 2001, dissenting opinion Judge Lewis.
[261] Batzel v. Smith, 333 F.3d, 9th Cir., 2003; Barrett v. Rosenthal, 5 Cal. Rptr. 3d, Cal. Ct. App., 2003.
[262] BAYER, *Liability of internet service providers for third party content*, in *Resarchgate.net*, 2007, p. 62.
[263] Viacom Int'l Inc, et al., v. YouTube, Inc. et al., 676, F.3d 19, 2007.

sussiste esclusivamente in presenza di una comunicazione circostanziata sull'esistenza di contenuti illeciti. Di fatto, come sarà analizzato nel paragrafo successivo, con le dovute differenze, il risultato così raggiunto non è dissimile rispetto al sistema di *take down* dell'UE.

Negli ultimi anni, tuttavia, la giurisprudenza statunitense si è trovata a fronteggiare un'ulteriore questione connessa al paradigma di responsabilità degli ISPs, ossia quale responsabilità sia possibile attribuire alle piattaforme, se i contenuti non sono più controllati da umani, bensì da apposti algoritmi di associazione e filtraggio[264].

La questione è stata affrontata per la prima volta in maniera esaustiva nel caso *Force v. Facebook* nel 2019[265]. La pronuncia riguardava l'accusa rivolta da un cittadino americano, superstite di attacchi terroristici posti in essere in Israele dall'organizzazione *Hamas,* e dai parenti delle vittime, nei confronti del *social network* per avere questo concorso nella realizzazione dei suddetti attacchi.

Nello specifico gli attori lamentavano il fatto che *Facebook* avesse consentito ad *Hamas* di mantenere attiva la propria pagina sulla piattaforma, così permettendogli di divulgare messaggi e informazioni che istigassero alla realizzazione degli attacchi e di reclutare nuove cellule terroristiche.

E ancora, secondo l'accusa il convenuto avrebbe dovuto prendere iniziative più drastiche e più efficaci rispetto alla semplice sospensione per un periodo di tempo limitato di alcuni *account* riconducibili all'organizzazione terroristica, e all'oscuramento delle pagine in questione agli utenti di Israele.

La principale fonte di rilevanza dell'argomentazione dell'attore, tuttavia, risiede nell'aver messo in dubbio la tradizionale connotazione dei *social network* come *provider* neutri, sostenendo che questi svolgono un ruolo attivo nella scelta e manipolazione dei contenuti grazie agli algoritmi che sono alla base della piattaforma.

Tuttavia, ancora una volta, i giudici di New York hanno escluso la responsabilità di *Facebook*, ritenendo a questo applicabile l'esonero di responsabilità previsto dalla sezione 230 del *Communication Decency Act.*

---

[264]DOMINGOS, *L'algoritmo definitivo. La macchina che impara da sola e il futuro del nostro mondo*, Milano, 2015; DIAKOPOULOS, *Algorithmic Accountability Reporting: On the Investigation of Black Boxes*, in *Columbia Journalism School*, 2014, p. 3.

[265] Force v. Facebook, Inc. No. 18-397, 2nd Cir., 2019.

A seguito di tale decisione, gli attori hanno presentato appello, sottolineando la sussistenza del nesso causale tra gli algoritmi utilizzati dalla piattaforma e la capillare diffusione dei messaggi di *Hamas.*

In via sussidiaria, l'accusa ha sostenuto che, anche nell'eventualità in cui la Corte escludesse una responsabilità civile di *Facebook,* in ogni caso sussisterebbe una sua responsabilità penale ai sensi dell'*Anti-Terrorism Act* e dello *Justice Against Sponsors of Terrorism Act*, dal momento che la stessa sezione 230 (e) (1) del *Communication Decency Act* prevede che «*nothing in this section shall be construed to impair the enforcement of […] any other Federal criminal statute*».

Nonostante ciò, i giudici dell'appello hanno confermato la decisione della Corte distrettuale, escludendo la responsabilità di *Facebook* in virtù della sezione 230 del *Communication Decency Act*, per altro in piena conformità con precedenti pronunce giurisprudenziali su temi analoghi[266].

Tra i summenzionati precedenti, una controversia affine per oggetto al caso Force è rappresentato dal caso *Cohen v Facebook*[267], in cui 20.000 israeliani hanno fatto causa al *social network* per averli fatti vivere in un clima di paura e minaccia per la propria sicurezza personale, a causa dei ripetuti attacchi rivolti a questi da parte di terroristi palestinesi per il tramite della piattaforma.

Anche in questo caso, secondo l'accusa la responsabilità di *Facebook* deriverebbe dall'aver permesso e agevolato la raccolta di adepti da parte dell'organizzazione terroristica, grazie all'impiego di algoritmi che, amplificando la portata del materiale diffuso dall'organizzazione, avrebbero fatto venir meno il tradizionale carattere di *provider* neutro proprio del *social network.*

Nello specifico, gli attori hanno sostenuto che *Facebook* «*does not act as the publisher of Hamas's content within the meaning of section 230 (c)(1) because it uses algorithms to suggest content to users, resulting in matchmaking*»[268].

Così come nel caso Force, tuttavia, la Corte ha rigettato la domanda degli attori ritenendo che il fondamento delle doglianze altro non fosse che un insieme di

[266] Fields v. Twitter, No. 16-cv-00213-WHO, 2017; Cohen v. Facebook Inc., 252 F. Supp. 3d 140; Cain e Gonzalez v. Twitter, 17 Civ. 122, PAC, S.D.N.Y. 2017; Reynaldo Gonzalez v. Twitter Inc., Google Inc. e Facebook Inc.; Palmucci v. Twitter, 18-cv-03947-WHO, N.D. Cal., 2019.

[267] SPIVAK, *Facebook Immune from Liability Based on Third-Party Content*, in *Lawfare*, 2017; TATE, *Maybe Someone Dies: The Dilemma of Domestic Terrorism and Internet Edge Provider Liability*, in *Boston College Law Review*, 2019, pp. 1731-1770.

[268] Force v. Facebook, Inc. No. 18-397, 2nd Cir. 2019, p. 32.

congetture, dal momento che questi avrebbero voluto dimostrare la compartecipazione della piattaforma in attacchi terroristici non ancora verificatisi.
Tale decisione è stata poi confermata in grado di appello in cui i giudici di New York hanno ritenuto che l'utilizzo di elementi di intelligenza artificiale non possa restringere o addirittura escludere l'applicabilità della sezione 230 del *Communication Decency Act.* Infatti, ad opinione della Corte, permettere una tale limitazione equivarrebbe a svuotare la norma del proprio significato, anche alla luce del fatto che «*the services have always decided, for example, where on their sites (or other digital property) particular third-party content should reside and to whom it should be shown. Placing certain third-party on a homepage, for example, tends to recommend that content to users more than if it were located elsewhere on a website. […] Internet services have also long been able to target the third-party content displayed to users based on, among other things, users' geolocation, language of choice, and registration information*»[269].
Ne consegue che, secondo la Corte, il fatto che, con l'evoluzione della tecnologia, i *providers* abbiano incrementato la propria capacità di creare connessioni e individuare soggetti potenzialmente interessati ai propri contenuti, non possa comportare penalizzazione nei confronti di questi.
In conclusione, i giudici hanno escluso che *Facebook* abbia posto in essere un contributo materiale su quanto pubblicato dell'organizzazione terroristica, affermando che «*the algorithms take the information provided by Facebook users and "match" it to other users – again, materially unaltered – based on objective factors applicable to any content, whether it concerns soccer, Picasso, or plumbers*»[270].
Nell'ambito della vicenda in esame, risulta particolarmente interessante l'opinione dissenziente del giudice Katzmann[271].
La critica mossa da questo alla decisione del collegio risiede essenzialmente in due aspetti fondamentali.
Innanzitutto, il giudice ritiene che l'art. 230 del *Communication Decency Act* abbia una portata più ristretta rispetto a quanto sostenuto dal collegio, così che

[269] *Ivi*, p. 35.
[270] *Ivi*, p. 47.
[271] *Ivi*, dissenting opinion Judge Katzmann.

l'applicabilità della disposizione in esame non dovrebbe essere estesa alla tutela dell'editore per contenuti aventi minacce terroristiche.

Più precisamente, il magistrato ha affermato che la sezione 230 fornisce l'immunità a coloro i quali pubblichino contenuti derivanti da parti terze solo qualora si limitino alle tradizionali funzioni editoriali, ovverosia decidere l'*an* e il *quando* della pubblicazione dei contenuti; al contrario, tale norma non si estende in alcun modo a coprire attività quali il suggerimento di profili, gruppi o pagine con cui stringere amicizia o di contenuti sulla base di preferenze precedentemente espresse dagli utenti.

In secondo luogo, Katzmann ritiene che proprio l'impiego dell'intelligenza artificiale costituisca l'elemento in grado di trasformare il *social network* in un collaboratore dell'organizzazione terroristica, in virtù dell'incremento vertiginoso nella quantità di *audience* raggiungibile dagli utenti grazie agli algoritmi.

Nello specifico, il magistrato ha sottolineato che «*Facebook uses algorithms to create and communicate its own message: that it thinks you, the reader – you, specifically – will like this content. And second, Facebook's suggestions contribute to the creation of real-world social networks. The result of at least some suggestions is not just that the user consumes a third-party's content. Sometimes, Facebook's suggestions allegedly lead the users to become part of a unique global community, the creation and maintenance of which goes far beyond and differs in kind from traditional editorial functions*».

Ne consegue che, secondo il magistrato il ruolo attivo della piattaforma nell'agevolare l'intento di *Hamas* di creare un *network* di utenti faccia sì che *Facebook* debba essere ritenuto un *information content provider*, e che quindi non possa beneficiare dell'immunità fornita dalla sezione 230 del *Communication Decency Act.*

Il giudice conclude la propria opinione dissenziente rivolgendo al Congresso l'invito a riconsiderare la previsione contenuta nella sezione 230 del *Communication Decency Act* alla luce della rapidità con cui si sono espansi i *social network* negli ultimi anni, affermando che «*while the majority and I disagree about whether § 230 immunizes interactive computer services from liability for all these activities or only some, it is pellucid that Congress did not have any of them in mind when it enacted the CDA. […] Congress could not have anticipated the pernicious spread of hate and violence that the rise of social media likely has since fomented.*

Nor could Congress have divined the role that social media providers themselves would play in this tale»[272].

In conclusione, nonostante il *Communication Decency Act* e le interpretazioni giurisprudenziali degli ultimi anni abbiano fornito un quadro entro cui è possibile orientarsi per l'attribuzione di responsabilità in capo ai *provider*, gli *user-generated contents*, la rapida evoluzione delle tecnologie e delle piattaforme *web* sembra richiedere una revisione in chiave evolutiva della disciplina vigente.

3.2. La Responsabilità degli *Internet Service Providers*: l'esperienza Europea dalla Direttiva 31/2000 al *Digital Service Act*

A livello europeo la disciplina della responsabilità degli *Internet Service Providers* trova una sua prima sistemazione compiuta nella Direttiva CE numero 31 del 2000 in tema di *E-Commerce*.

Ai sensi dell'art. 2 lettera b) della stessa si può qualificare come *provider* «la persona fisica o giuridica che presta un servizio della società dell'informazione»; questi ultimi, con un rimando all'art. 1 comma 2 della Direttiva CE numero 48 del 1998, vengono definiti come «qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi».

Seguendo il sopracitato metodo orizzontale[273], la direttiva continua suddividendo i *provider* in tre categorie, a seconda della tipologia di attività che svolgono: *mere conduit, caching, hosting.*

Partendo dalla prima categoria, l'art. 12 della normativa in commento prevede che, nella prestazione di un servizio alla società dell'informazione consistente nella trasmissione, su una rete di comunicazione, di informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione, il prestatore sia esonerato da responsabilità per le informazioni trasmesse, purché siano rispettate determinate condizioni. Nello specifico, l'esenzione di responsabilità opera a condizione che: il prestatore non dia origine alla trasmissione, non selezioni il destinatario di questa, e non selezioni né modifichi le informazioni trasmesse. E ancora, ai sensi dell'articolo in esame, le attività di

[272] *Ivi*, p. 33.
[273] V. *infra* § 3.

trasmissione e di fornitura di accesso sopra menzionate includono la memorizzazione automatica, intermedia e transitoria delle informazioni trasmesse, a condizione che questa sia necessaria solamente alla trasmissione sulla rete di comunicazione e la sua durata non superi il tempo ragionevolmente all'uopo necessario.

E', inoltre, importante ricordare che il terzo comma dell'art. 12 prevede esplicitamente che l'articolo in esame lascia impregiudicata la possibilità che un organo giurisdizionale o un'autorità amministrativa esiga che il prestatore impedisca o ponga fine una violazione.

Per quanto concerne la memorizzazione temporanea automatica dei dati, ossia la cosiddetta attività di *caching*, l'art. 13 della Direttiva 31/2000 prevede che, sempre con riferimento a un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, il prestatore non è responsabile della memorizzazione automatica, intermedia e temporanea, di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta.

Anche in questo caso, perché la previsione in esame trovi applicazione, è necessario che il prestatore rispetti specifiche condizioni: non modifichi le informazioni; si conformi alle condizioni di accesso alle informazioni; si conformi alle norme di aggiornamento delle informazioni indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore; non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni; agisca prontamente per rimuovere le informazioni che ha memorizzato o per disabilitare l'accesso non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione dell'accesso.

Passando alla terza e ultima categoria, ossia l'attività di *hosting*, ai sensi dell'art. 14, l'esonero di responsabilità del prestatore per la memorizzazione di informazioni richieste dal destinatario sussiste a condizione che il *provider:* non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendano manifesta l'illegalità dell'attività o dell'informazione, o, non appena al

corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

E ancora, il secondo comma prevede che la disciplina indicata nel primo non trova applicazione se il destinatario agisce sotto il controllo o l'autorità del prestatore stesso.

Infine, con una dizione analoga agli articoli precedenti, il terzo comma dell'art. 14 lascia impregiudicata la possibilità, per un organo giurisdizionale o un'autorità amministrativa, in conformità agli ordinamenti giuridici degli Stati membri, di esigere che il prestatore ponga fine ad una violazione o la impedisca, nonché la possibilità per gli Stati membri di definire procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime.

Il quadro normativo in esame viene completato dalla disposizione contenuta nell'art. 15, il quale prevede l'assenza di un obbligo generale di sorveglianza da parte dei *provider* sulle informazioni che trasmette o memorizza, nell'esercizio delle attività previste dagli articoli 12,13 e 14. Ugualmente, l'art. 15 esclude in capo ai prestatori un obbligo di ricerca attiva di fatti o circostanze che indichino la presenza di attività illecite.

Infine, il terzo comma dell'articolo in esame stabilisce che gli Stati Membri possano prevedere che i prestatori della società dell'informazione siano tenuti ad informare la pubblica autorità in caso di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati.

Dunque, in ottica riassuntiva, alla luce della Direttiva europea sul commercio elettronico dell'8 giugno del 2000, gli *Internet Service Providers* non possono essere ritenuti responsabili quando questi svolgono attività di *mere conduit, caching* o *hosting*[274].

Tuttavia, a seguito delle evoluzioni tecnologie e della comparsa di nuove piattaforme sul *web*, anche in Europa si è posta la problematica di determinare in maniera più specifica e attuale la responsabilità che è possibile attribuire agli

[274] PITRUZZELLA, POLLICINO, QUINTARELLI, *Parole e Potere, libertà d'espressione, hate speech e fake news,* cit., p. 80.

Internet Service Providers per i contenuti che questi rendono accessibili al pubblico[275].

Si è, dunque, assistito a diversi tentativi, tanto giurisprudenziali quanto dottrinali, di adattare la disciplina prevista dalla Direttiva in esame allo scenario delineatosi nell'era della Post-Verità.

Prima di addentrarsi nell'analisi delle pronunce giurisprudenziali, è necessario premettere che, nonostante la definizione di "servizi della società dell'informazione" fornita dall'art. 1 comma 2 della direttiva parli di «qualsiasi servizio prestato normalmente dietro retribuzione», recente dottrina ritiene che tale dizione possa estendersi anche a *provider* che non richiedono alcuna retribuzione, quali motori di ricerca e *social network,* in quanto l'avverbio "normalmente" alluderebbe al fatto che la retribuzione non sia un elemento essenziale, bensì solamente un aspetto che di frequente caratterizza la prassi[276].

Quanto alla giurisprudenza in materia, già nel 2008 la Corte Europea dei Diritti dell'Uomo aveva mostrato la propria preoccupazione per la tematica in esame, affermando che, nonostante sia indubbio che la tutela della libertà di espressione rientri tra le principali garanzie che devono essere fornite agli utenti, tale diritto non può essere illimitato, essendo necessario che questo sia bilanciato con altri beni da tutelare, quali la prevenzione di crimini e la protezione della libertà altrui[277].

In risposta a tale preoccupazione, la giurisprudenza dell'Unione, nel corso degli anni, si è mossa verso la prefigurazione di due tipologie diverse di *Internet Service Providers*: gli ISP "passivi" o "neutri" e gli ISP "attivi" o "non neutri"[278].

In quest'ottica, sarebbe proprio la "neutralità" o meno del *provider* l'elemento chiave al fine di attribuire a questo una responsabilità per i contenuti pubblicati sulla piattaforma, soprattutto con riferimento alla categoria degli *hosting provider.*

Nello specifico, l'*hosting* passivo, conservando le caratteristiche della neutralità e dell'imparzialità nei confronti dei contenuti pubblicati, beneficia delle esenzioni di responsabilità previste dalla Direttiva numero 31 del 2000.

---

[275] OECD, *The Economic and Social role of internet intermediaries*, aprile 2010, p. 11.

[276] ALLEGRI, *Ubi social, ibi ius. Fondamentanti costituzionali dei social network e profili giuridici della responsabilità dei provider*, Milano, 2018, p. 54; GARZONIO, *Responsabilità degli ISP rispetto al trattamento automatizzato dei dati personali con finalità di comunicazione politica: applicabilità del GDPR alle piattaforme social*, in *Media Laws*, 2019, p. 194.

[277] Corte europea dei diritti dell'uomo, K.U v. Finland, Application No. 2872/02, 2008, para 49.

[278] POLLICINO, *Tutela e pluralismo nell'era digitale: ruolo e responsabilità degli Internet service providers*, cit., p. 3; AVIGNO, *Intermediary Liability for User-Generated Content in Europe*, cit.

A tal riguardo, già nel caso *Google v. Louis Vuitton*, la Corte aveva affermato che al fine di determinare se un intermediario possa beneficiare dell'esonero di responsabilità di cui all'art. 14 della Direttiva CE sull'*E-Commerce*, «*it is necessary to examine whether the role played by that service provider is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores*»[279].

Al contrario, all'*hosting* attivo sarebbe applicabile la disciplina della responsabilità prevista per il gestore di contenuti, dal momento che questo svolgerebbe delle attività più vicine a quelle del gestore che non all'*hosting provider* passivo[280].

E ancora, nel *leading case* in materia *Delfi AS v. Estonia*[281], la Corte ha esplicitamente riconosciuto che i doveri dei *provider*, nello specifico dei portali di notizie, con riferimento ai contenuti pubblicati da soggetti terzi possono differire in qualche misura da quelli dei *publisher* tradizionali, che agiscono come editori di tutti i contenuti che appaiono sulle loro pagine.

Più nello specifico, il caso in esame rappresenta la prima volta in cui la CEDU si è trovata a pronunciarsi sulla possibilità che uno Stato Membro della Convenzione reputi un ISP responsabile per commenti offensivi o incitanti all'odio pubblicati dagli utenti, senza che per questo lo Stato in questione incorra in una violazione dell'art. 10 della Convenzione stessa.

Il caso riguardava uno dei più famosi portali di notizie in Estonia, Delfi AS, in cui era stato pubblicato un articolo riguardante un piano industriale della società di traghetti estone SLK, in cui si condivideva la notizia secondo cui il piano avrebbe previsto una possibile distruzione di strade pubbliche costruite sul mare ghiacciato, che permettevano il collegamento tra la terraferma e alcune isole del Mar Baltico. L'articolo ha ricevuto nell'arco di pochi giorni 185 commenti di utenti, tra cui circa 20 con un contenuto offensivo e minaccioso nei confronti di un membro, e principale azionista, del consiglio di amministrazione della SLK. Di conseguenza, il 9 marzo 2006 l'avvocato di questo ha chiesto a Delfi AS la rimozione dei

[279] Corte di Giustizia dell'Unione Europea, Grande sezione, 23 marzo 2010, cause riunite C-236/08, C-237/08 e C-238/08, Google France SARL, Google Inc. c Luis Vuitton SA, Luteciel SARL, Google Frace SAL c Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL, para 114.

[280] POLLICINO, *Tutela e pluralismo nell'era digitale: ruolo e responsabilità degli Internet service providers*, cit., p. 24.

[281] Corte Europea dei diritti dell'uomo, Delfi AS c. Estonia, Grande Camera, Application n. 64569/09, 2015.

commenti in questione, nonché un risarcimento pari a 32.000 euro per i danni morali sofferti dal suo cliente. Tuttavia, il portale non ha acconsentito al risarcimento, basando il proprio rifiuto sull'argomentazione secondo cui, avendo questo rimosso i contenuti in maniera tempestiva, in conformità a quanto previsto alla piattaforma stessa, egli avrebbe adempiuto a ogni suo onere[282].

I giudici interni hanno considerato il portale Delfi AS come responsabile per non aver evitato la pubblicazione dei commenti offensivi, e comunque per non aver provveduto spontaneamente alla rimozione degli stessi, dopo essere venuto a conoscenza della loro portata palesemente offensiva.

A seguito di tale pronuncia, Delfi ha fatto ricorso alla Corte Europea dei Diritti dell'Uomo lamentando una violazione da parte dei giudici estoni dell'art. 10 della Convenzione.

I giudici di Strasburgo si sono pronunciati a favore della responsabilità dell'ISP, concludendo che l'attribuzione da parte degli giudici estoni della responsabilità per i commenti offensivi effettuati dagli utenti in capo al portale di notizie, non avesse costituito una violazione della libertà di espressione, di cui all'art. 10 della Convenzione.

La pronuncia in esame risulta particolarmente rilevante nell'analisi della giurisprudenza in materia di responsabilità degli ISP attivi, in quanto la Corte non ha ritenuto applicabile l'esenzione di responsabilità prevista dalla Direttive CE sul commercio elettronico, proprio sulla base del fatto che il portale di notizie svolgeva dei servizi che andavano ben oltre l'attività meramente automatica, tecnica e passiva prevista dalla Direttiva[283]. In altre parole, i giudici di Strasburgo hanno ritenuto che l'esonero di responsabilità previsto dalla Direttiva in questione, non fosse applicabile in quanto, il fatto che Delfi AS fosse in grado di esercitare un controllo sul contenuto dei commenti pubblicati dagli utenti, era sufficiente per qualificare il portale come *publisher.*

E', inoltre, interessane notare che una delle valutazioni che ha condotto la Corte a ritenere il *provider* responsabile per la pubblicazione dei cosiddetti *user-generated content,* è stata la gravità dei commenti pubblicati, e, nello specifico, il fatto che questi integrassero condotte di incitamento all'odio e alla violenza.

---

[282] ABBONDANTE, *il ruolo dei social network nella lotta all'hate speech: un'analisi comparata fra l'esperienza statunitense e quella europea*, in *Informatica e Diritto,* XLII, Vol. XXVI, n. 1-2, p. 80.
[283] Corte Europea dei diritti dell'uomo, Delfi AS c. Estonia, Grande Camera, cit., para 145.

In un caso di pochi anni successivo a Delfi, invece, la minore gravità dei commenti pubblicati dagli utenti ha indotto la Corte Europea dei Diritti dell'Uomo ad adottare una decisione profondamente diversa, se pur sulla base di circostanze fattuali analoghe.

Nello specifico, si tratta del caso *MTE and Index c. Ungheria*[284], il quale riguardava la pubblicazione di un articolo su MTE che criticava le strategie di *business* di due siti *web* immobiliari, articolo che poi era stato copiato e pubblicato anche da Index. A seguito della pubblicazione, su entrambe le piattaforme, di commenti di critica degli utenti nei confronti dei siti immobiliari in questione, questi ultimi hanno iniziato una causa contro MTE ed Index ritenendoli responsabili dei suddetti commenti diffamatori e ingiuriosi.

A differenza del caso Delfi AS, tuttavia, in questa occasione la Corte ha ritenuto che le Corti ungare avessero commesso una violazione dell'art. 10 della Convenzione nel ritenere che le piattaforme fossero responsabili per i commenti diffamatori pubblicati dagli utenti. A sostegno della propria decisione, la CEDU ha specificato che la violazione era dovuta al fatto che le Corti nazionali non avevano condotto in maniera appropriata un bilanciamento tra i diversi interessi in gioco, ossia tra la libertà di espressione di MTE e Index, e il diritto al rispetto della reputazione dei due siti immobiliari[285]. La Corte ha anche sottolineato che la propria decisione era dovuta al fatto che, a differenza della vicenda Delfi, nel caso in questione i commenti non integravano discorsi d'odio o minacce a individui singoli[286].

Ciononostante, la Corte ha ribadito il principio secondo cui gli Stati Membri della Convenzione possono attribuire alle piattaforme la responsabilità per i contenuti che costituiscano atteggiamenti di incitamento all'odio e alla violenza ivi pubblicati dagli utenti, nell'ipotesi in cui le piattaforme non abbiano adottato senza indugio misure idonee a rimuovere i commenti illeciti, prescindendo da una segnalazione del soggetto passivo o di soggetti terzi.

Le sentenze in esame, e soprattutto la pronuncia del caso Delfi AS, hanno suscitato un grande dibattito dottrinale in ragione dell'incertezza lasciata dalla Corte circa un

[284] Corte Europea dei diritti dell'uomo, Magyar Tartalomszolgaltatok Egyesulete and Index.hu ZRT v Hungary, Application No. 22947/13, 2016.
[285] *Ivi*, para 88.
[286] *Ivi*, para 91.

eventuale obbligo dei *provider* di prevenire la pubblicazione di commenti illeciti, nello specifico di commenti diffamatori, o comunque lesivi dell'altrui reputazione[287].

Sul punto la Corte nel caso Delfi si è limitata ad affermare che, secondo quanto previsto dalla sentenza della Corte Suprema estone, la rimozione da parte del portale dei commenti, immediatamente dopo la pubblicazione di questi, sarebbe stata sufficiente al fine di non incorrere in responsabilità ai sensi della normativa interna[288].

A tal riguardo, ad oggi si può affermare che, dall'analisi dei principali strumenti internazionali in materia[289], emergono due principi comuni: l'esclusione dell'esistenza di un obbligo dei *provider* di prevenire la pubblicazione di commenti illeciti e la previsione secondo cui, al contrario, è possibile prevedere la responsabilità degli ISPs quando questi non provvedano alla rimozione di contenuti lesivi, a seguito della richiesta di un'autorità giudiziaria.

Proprio con specifico riguardo a tali principi, la Corte di Giustizia si è pronunciata in un caso recente affermando che secondo la direttiva 31/2000 «un prestatore di servizi di *hosting*, quale *Facebook*, non è responsabile delle informazioni memorizzate qualora non sia a conoscenza della loro illiceità o qualora agisca immediatamente per rimuoverle o per disabilitare l'accesso alle medesime non appena ne venga a conoscenza. Tale esonero da responsabilità non pregiudica tuttavia la possibilità di ingiungere al prestatore di servizi di *hosting* di porre fine ad una violazione o di impedire una violazione, in particolare cancellando le informazioni illecite o disabilitando l'accesso alle medesime. Per contro, la direttiva vieta di imporre a un prestatore di servizi di *hosting* di sorvegliare, in via generale,

---

[287] NIGRO, *Diritti civili e politici, la responsabilità degli internet service providers e la convenzione europea dei diritti umani: il caso Delfi AS*, in *Diritti Umani e Diritto Internazionale*, 2015, vol. 9, n. 3, p. 3.

[288] Corte Europea dei diritti dell'uomo, Delfi AS c. Estonia, Grande Camera, cit., para 153.

[289] Direttiva 2000/31/CE, art 15; la Dichiarazione del Comitato dei Ministri del Consiglio d'Europa sulla libertà di comunicazione su Internet, principio n. 3, 28 maggio 2003; la Dichiarazione congiunta dello Special Rapporteur delle Nazioni Unite e dei Rappresentanti dell'OSCE e dell'OAS sulla promozione della libertà di espressione, 28 dicembre 2005, <www.osce.org/fom/27455?download=true>>; il Rapporto del Consiglio dei diritti umani sulla promozione e protezione del diritto alla libertà di opinione e di espressione, UN Doc. A/HRC/17/27, 16 maggio 2011, para 70.

le informazioni da esso memorizzate o di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite»[290].

La Corte ha, poi, proseguito specificando che «affinché un'ingiunzione volta a fare cessare un atto illecito e ad impedire il suo reiterarsi nonché ogni ulteriore danno agli interessi in causa possa effettivamente realizzare siffatti obiettivi, detta ingiunzione deve potersi estendere alle informazioni il cui contenuto, pur veicolando sostanzialmente lo stesso messaggio, sia formulato in modo leggermente diverso, a causa delle parole utilizzate o della loro combinazione, rispetto all'informazione il cui contenuto sia stato dichiarato illecito. Diversamente infatti, e come sottolineato dal giudice del rinvio, gli effetti inerenti a un'ingiunzione del genere potrebbero facilmente essere elusi tramite la memorizzazione di messaggi appena diversi da quelli dichiarati illeciti in precedenza, il che potrebbe condurre l'interessato a dover moltiplicare le procedure al fine di ottenere la cessazione dei comportamenti illeciti di cui è vittima. Tuttavia, in tale contesto va anche ricordato che, come discende dall'art. 15, paragrafo 1, della direttiva 2000/31 e come ricordato al punto 34 della presente sentenza, un giudice di uno Stato membro, da un lato, non può emettere un'ingiunzione nei confronti di un prestatore di servizi di *hosting* per ordinargli di sorvegliare, in via generale, le informazioni da esso memorizzate né, d'altro lato, costringerlo a ricercare attivamente fatti o circostanze sottese al contenuto illecito»[291].

E ancora, la Corte si è espressa in tema di obbligo di filtraggio degli ISP anche nel caso *Scarlet c. Sabam*[292], qualificando come inammissibile l'imposizione in capo agli *Internet Service Providers* di meccanismi di filtraggio preventivo generalizzato dei contenuti, in quel caso, a tutela dei diritti di proprietà intellettuale. Al contrario, la Corte non ha escluso la possibilità di prevedere obblighi di controllo e filtraggio *ex post*, ossia successivi al momento in cui l'ISP viene a conoscenza dell'illiceità di un contenuto per il tramite di una diffida[293].

In ottica riassuntiva si può affermare che l'elemento che la giurisprudenza dell'Unione ha individuato come essenziale ai fini dell'integrazione della

[290] Corte di Giustizia dell'Unione Europea, sez. III, Glawischnig-Piesczek c. Facebook Ireland, 3 ottobre 2019.
[291] *Ivi*, paras 40-47.
[292] Corte di Giustizia dell'Unione Europea, sez. III, Scarlet C. Sabam, 24 novembre 2011.
[293] TOSI, *responsabilità civile degli hosting provider e inibitoria giudiziale dei contenuti digitali illeciti equivalenti tra assenza dell'obbligo di sorveglianza ex ante e ammissibilità' ex post*, in *Il diritto degli affari*, n. 1/20, pp. 18 e ss.

responsabilità dell'*Internet Service Provider* è costituito dalla non neutralità. Ne consegue che, affinché il *provider* possa godere dell'esenzione di responsabilità prevista dalla Direttiva CE numero 31 del 2000 è necessario che questo «agisca come prestatore neutro. Le limitazioni di responsabilità, infatti, si fondano sulla precondizione che il *provider* esegua un'attività di ordine meramente tecnico, automatico e passivo, in modo che esso non conosca né controlli le informazioni trasmesse o memorizzate. Non a caso il confine del regime di "irresponsabilità" del *provider* coincide con la conoscenza, da parte di questi, dell'illeceità di contenuti o delle attività che giungono in rete per suo tramite; conoscenza in corrispondenza logia della quale si attiva l'obbligo per il *provider*, di agire al fine di rimuovere contenuti illeciti»[294]. Al contrario, un *provider* beneficerà del regime previsto dalla normativa in esame quando si limita a svolgere attività di *mere conduit, caching* o *hosting.*

Il quadro regolatorio europeo è poi stato integrato da due comunicazioni della Commissione Europea adottate rispettivamente nel 2015 e nel 2017.

Per quanto concerne la prima, il 6 maggio 2015 la Commissione ha adottato una comunicazione intitolata "Strategia per il mercato unico digitale in Europa"[295], volta a mettere in luce la necessità di una consultazione pubblica sul ruolo delle piattaforme digitali, nonché sull'idoneità delle misure per il contrasto della divulgazione di contenuti illeciti per il tramite del *web.* Nello specifico, la comunicazione in esame ha preso le mosse dall'incremento vertiginoso della quantità di *fake news, hate speech* e altri contenuti illegittimi che, già nel 2015, venivano diffusi su Internet principalmente per il tramite di piattaforme *social.*

A seguito della suddetta consultazione pubblica, la Commissione europea, raccogliendo l'invito mossole dal Parlamento europeo nella risoluzione del 15 giugno 2017 sulle piattaforme *on-line* e il mercato unico digitale[296], ha pubblicato nel 2017 una comunicazione specificatamente volta alla lotta alla divulgazione su

[294] BASSINI, *Commercio elettronico e tutela dei segni distintivi. Responsabilità degli intermediari e trend giurisprudenziali*, MAZZARO - POLLICINO (a cura di), in *Tutela del copyright e della privacy sul web. Quid iuris?*, Roma, 2012, pp. 62-63.

[295] Commissione Europea, *Strategia per il mercato unico digitale in Europa,* COM(2015) 192, 6 maggio 2015.

[296] PARLAMENTO EUROPEO, *Risoluzione del 15 giugno 2017 sulle piattaforme on line e il mercato unico digitale,* 2016/2276(INI).

Internet di contenuti illeciti, attraverso una maggiore responsabilizzazione delle piattaforme[297].

La comunicazione in esame ha messo in luce che il fatto che la direttiva numero 31 del 2000 non contempli una definizione di "contenuto illecito" comporta che la disciplina della responsabilità degli *Internet Service Providers* prevista dalla direttiva venga di fatto applicata ad attività illecite estremamente differenti tra di loro. Alla luce di ciò, la comunicazione della Commissione contiene l'auspicio a che il quadro regolatorio venga armonizzato e razionalizzato a livello nazionale.

E ancora, la Commissione europea individua come concetto chiave la trasparenza e incoraggia la cooperazione tra le piattaforme digitali e le autorità competenti, siano esse giudiziarie o amministrative, nazionali o europee. A tal riguardo la Commissione invita le prime a rispettare il principio della *due diligence*, adottando soluzioni tecniche adeguate a raccogliere le segnalazioni in maniera efficace e provvedendo, poi, alla celere rimozione dei contenuti illeciti; per quanto riguarda le autorità competenti, la comunicazione contiene l'auspicio che queste delineino regole chiare e specifiche, da indirizzare agli operatori di settore, sulle definizioni dei contenuti illegittimi e sulle procedure da seguire per rimuoverli.

La comunicazione affronta, poi, il cosiddetto "dilemma dell'ISP", ossia la problematica relativa al fatto che non esiste nel quadro regolatorio europeo alcuna disposizione che sollevi pregiudizialmente i *provider* da responsabilità in caso di rimozione abusiva di contenuti lesivi di diritti altrui.

Risulta opportuno segnalare che, al contrario, una garanzia di tal genere è prevista dall'art. 230 lettera c) comma 2 del sopra citato *Communication Decency Act*, che prevede che i *publisher* non possano essere considerati civilmente responsabili per aver scelto di eliminare o restringere l'accesso a contenuti osceni volgari, violenti, lascivi, sessualmente molesti o inappropriati sotto altri aspetti.

A tal riguardo, la soluzione prospettata dalla Commissione risiede nell'incrementare il ruolo dei cosiddetti "segnalatori attendibili", come ad esempio l'unità Europol specializzata per la segnalazione di contenuti terroristici *on-line.*

Nello specifico, si tratta di entità specializzate dotate di competenze specifiche che gli consentono di identificare contenuti illeciti, e di strutture specificamente dedicate all'individuazione di tali contenuti su Internet.

---

[297] COMMISSIONE EUROPEA, *Lotta ai contenuti illeciti online. Verso una maggiore responsabilizzazione delle piattaforme online,* COM (2017) 555, 28 settembre 2017.

Infine, risulta essenziale sottolineare che nella Comunicazione non si rintraccia alcuna intenzione esplicita di procedere a una revisione o modifica della direttiva *E-Commerce* del 2000; al contrario, la Commissione ribadisce che la suddetta normativa rappresenta «la base adeguata per elaborare sistemi rapidi e affidabili, idonei a rimuovere le informazioni illecite e disabilitare l'accesso alle medesime». Ciononostante, la comunicazione sottolinea esplicitamente la «necessità che le piattaforme online agiscano in modo più responsabile e intensifichino l'impegno di autoregolamentazione a livello dell'UE per rimuovere i contenuti illegali».

In conclusione, si può affermare che, almeno fino al 2017, la Commissione, più che propendere per una revisione e un aggiornamento della disciplina contenuta nella direttiva CE 31/2000, sembrava preferire un approccio basato sull'autoregolamentazione, ad esempio implementando i meccanismi di *notice and take-down.*

Il quadro è parzialmente cambiato con l'adozione da parte della Commissione europea della proposta per il *Digital Service Act,* ossia una proposta di regolamento che riguardi il Mercato Unico digitale, apportando anche dei cambiamenti rispetto alla disciplina contenuta nella direttiva CE 31/2000.

Il tema della necessità di una revisione della normativa europea applicabile alle piattaforme digitali è stata oggetto di dibattito in seno al Parlamento europeo ormai per anni, e, nello specifico, ha portato nell'ottobre del 2020 all'adozione di tre risoluzioni in materia: *Digital Service Act- Improving the functioning of the Single Market, Digital Service Act: adapting commercial and civil law rules for commercial entities operating online* e *Digital Service Act and fundamental right issues posed.*

Per quanto concerne la prima[298], questa conteneva l'auspicio di una riforma delle regole esistenti a livello dell'Unione in materia di commercio elettronico, ribadendo, tuttavia, la necessità di mantenere inalterata la disciplina contenuta nella Direttiva 31/2000 per quanto concerne il regime di responsabilità delle piattaforme e il divieto di un obbligo generale di controllo.

[298] PARLAMENTO EUROPEO, *Risoluzione sull'improving the functioning of the Single Market*, 2020/2018(INL).

Passando ora alla seconda[299], questa richiedeva un maggiore rispetto del principio di trasparenza da parte delle piattaforme e una maggiore responsabilizzazione di queste.

Infine, per quanto riguarda la terza[300], si tratta di una risoluzione non legislativa che ha messo in luce la necessità di creare un quadro giuridico certo ed armonico, tanto per le piattaforme quanto per gli utenti, e di rispettare i diritti e le libertà fondamentali, data la rapida evoluzione tecnologica.

Risulta interessante notare che ciò che accomuna le tre direttive è il fatto che tutte raccomandano di mantenere inalterati i principi fondamentali espressi nella Direttiva CE sul commercio elettronico.

Tale quadro ha portato il Consiglio, nelle proprie Conclusioni di giungo del 2020[301], ad accogliere la proposta di adozione del regolamento *Digital Service Act*, sottolineando «*the need for clear and harmonised evidence-based rules on responsibilities and accountability for digital services that would guarantee internet intermediaries an appropriate level of legal certainty*».

Tra giugno e settembre 2020, la Commissione Europea ha tenuto una consultazione pubblica al fine di determinare quale fosse il modo più efficace di definire la disciplina delle responsabilità delle piattaforme digitali.

Tale consultazione ha ricevuto più di 200 risposte che sono, poi, confluite nell'*impact assessment* della Commissione[302], da cui emerge che i principi fondamentali della Direttiva CE 31/2000 continuano a mantenere una validità anche nell'era del 2.0, e che sono proprio tali principi che hanno consentito la crescita e l'accessibilità dei servizi digitali tra i diversi Stati Membri. Tuttavia, la Commissione ha anche evidenziato tre principali problematiche: l'incremento vertiginoso di attività illecite *on-line,* la mancanza di cooperazione tra le autorità nazionali che fa sì che l'attività di supervisione dei servizi digitali nell'ambito dell'Unione sia poco efficace e il rischio di una eccessiva frammentazione tra i diversi ordinamenti degli Stati Membri.

---

[299] PARLAMENTO EUROPEO, *Risoluzione sull'Digital Service Act and fundamental right issues posed*, 2020/2022(INL).

[300] PARLAMENTO EUROPEO, *Risoluzione sull'adapting commercial and civil law rules for commercial entities operating online*, 2020/2019(INL).

[301] Conclusioni del Consiglio su *Shaping Europe's Digital Future,* 8711/20, 9 giungo 2020.

[302] COMMISSIONE EUROPEA, *Impact assessment of the Digital Markets Act,* 8 marzo 2021, <<https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-markets-act>>.

Arrivando, ora, all'analisi della proposta del *Digital Service Act,* questa predispone un paradigma orizzontale basato sulla trasparenza e la responsabilizzazione delle piattaforme.

La proposta di *Digital Service Act* divide il regolamento in 4 capitoli, ognuno a sua volta suddiviso in diverse sezioni.

Il primo capitolo riguarda le previsioni generali, includendo nell'art. 1 lo scopo e nell'art. 2 le principali definizioni.

A ciò segue, nel capitolo 2, un insieme di disposizioni sull'esenzione di responsabilità delle diverse tipologie di *Internet Service Providers.*

A tal riguardo, risulta opportuno sottolineare che la nuova disciplina non mira a sostituire la Direttiva CE sull'*E-Commerce*, bensì è volta a costituire un'integrazione di questa, rendendola più specifica, chiara e attuale.

Così come la Direttiva del 2000, la proposta di regolamento differenzia il regime di responsabilità delle piattaforme a seconda dell'attività svolta dai *provider*, riprendendo la distinzione tra *mere conduit, caching* e *hosting*, rispettivamente agli articoli 3,4 e 5.

Partendo da queste tre categorie, le maggiori differenze rispetto alla Direttiva *E-Commerce* si possono individuare nella disciplina dell'*hosting provider.* Infatti, non solo l'art. 5 prevede un paragrafo aggiuntivo rispetto all'art. 14 della Direttiva del 2000, il quale statuisce che «*Paragraph 1 shall not apply with respect to liability under consumer protection law of online platforms allowing consumers to conclude distance contracts with traders, where such an online platform presents the specific item of information or otherwise enables the specific transaction at issue in a way that would lead an average and reasonably well-informed consumer to believe that the information, or the product or service that is the object of the transaction, is provided either by the online platform itself or by a recipient of the service who is acting under its authority or control*», ma modifica parzialmente anche il comma IV e, come vedremo più avanti, la proposta dedica anche la sezione II del capitolo III, a previsioni aggiuntive applicabili agli *hosting providers,* che includono le piattaforme *on-line.*

Inoltre, il capitolo in esame introduce delle innovazioni importanti rispetto al vecchio quadro normativo. Ad esempio, l'art. 6 prevede che l'esonero di responsabilità dei *provider* non dovrebbe venire meno quando questi svolgono controlli e investigazioni di propria iniziativa o agiscono in base alla legge.

E ancora, gli articoli 8 e 9 prevedono rispettivamente l'obbligo per gli ISPs di agire contro i contenuti illeciti sulla base di ordini ricevuti dalle autorità nazionali e di fornire a queste informazioni.

Per quanto concerne il divieto di un obbligo generale di controllo in capo agli ISPs, l'art. 7 riprende esclusivamente il primo comma dell'art. 15 della Direttiva 31/2000, escludendo, al contrario, il comma II.

Passando ora al capitolo III, questo prevede delle obbligazioni generali di *due diligence,* volte ad assicurare il rispetto della trasparenza e della sicurezza *on-line.*

Nello specifico, la prima sezione riguarda disposizioni applicabili a tutte le tipologie di *provider* che rientrano nello scopo del *Digital Service Act*. A titolo esemplificativo, l'art. 10 stipula il dovere dei *provider* di prevedere un punto di contatto singolo per facilitare le comunicazioni con le autorità degli Stati Membri e la Commissione. E ancora, l'art. 13 prevede il dovere dei *provider* di pubblicare almeno una volta l'anno un rapporto chiaro e dettagliato circa qualsiasi attività di moderazione dei contenuti pubblicati sulla loro piattaforma, che abbiano svolto durante il periodo preso in considerazione.

La seconda sezione del capitolo 3, contiene obbligazioni aggiuntive rispetto a quelle della sezione precedente, applicabili agli *hosting providers*: l'art. 14 comprende l'obbligo dei *providers* di predisporre meccanismi grazie ai quali soggetti terzi possano notificare alla piattaforma la presenza di contenuti illeciti, mentre l'art. 15 prevede che, nel caso in cui la piattaforma decida di rimuovere del materiale pubblicato da un utente, quest'ultimo deve essere informato della suddetta attività e delle motivazioni sottostanti.

La terza sezione del capitolo in esame disciplina, poi, delle obbligazioni applicabili a tutte le piattaforme digitali, aggiuntive rispetto a quelle previste nelle sezioni precedenti, specificando, tuttavia, che le previsioni contenute in questa sezione non si applicano alle piattaforme qualificabili come *micro* o *small enterprises,* secondo la definizione che ne è fornita nell'appendice alla Raccomandazione 2003/361/CE. A titolo esemplificativo, l'art. 18 prevede l'obbligo per le piattaforme *on-line* di ricorrere a metodi alternativi di risoluzione delle controversie per conflitti che potrebbero sorgere con gli utenti. E ancora, l'art. 23 prevede l'obbligo per i *providers* di pubblicare rapporti riguardo alla rimozione di informazioni che considerano illecite o contrari ai propri termini e condizioni d'uso.

La quarta sezione concerne obblighi applicabili alle piattaforme considerate *very large*, in aggiunta a quelli previsti dalle sezioni 1 e 3.

Ai sensi dell'art. 25, le piattaforme sono definite *very large* quando queste «*provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, calculated in accordance with the methodology set out in the delegated acts referred to in paragraph* 3». Tra gli obblighi previsti per le piattaforme che rientrano in questa categoria, ricordiamo il dovere di effettuare dei *risk assessment* sui pericoli che derivano dall'utilizzo dei servizi che offrono e di porre in essere sforzi ragionevoli per prevenire i suddetti rischi.

La quinta e ultima sezione del capitolo 3 predispone disposizioni trasversali che riguardano la *due diligence,* ossia, ad esempio, il processo mediante il quale la Commissione supporterà e promuoverà lo sviluppo e l'implementazione degli standard europei armonizzati.

Per quanto riguarda il capitolo 4, questo è dedicato all'implementazione e all'esecuzione del *Digital Service Act.*

A tal riguardo, si prevede che gli Stati Membri debbano designare dei coordinatori dei servizi digitali indipendenti, i quali saranno dotati di specifici poteri di supervisione, saranno autorizzati a ricevere lamentele nei confronti degli ISPs, dovranno cooperare con i coordinatori degli altri Stati Membri e avranno la possibilità di partecipare a indagini congiunte. Inoltre, sarà predisposto uno *European Board for Digital Services* (EDPB), al fine di assicurare un coordinamento efficace e un'applicazione consistente del nuovo regolamento.

E', inoltre, importante sottolineare che le piattaforme definite *very large* saranno soggette alla supervisione della Commissione europea.

In conclusione, con specifico riferimento alla disinformazione, risulta interessante notare che, nonostante la portata innovativa del *Digital Service Act,* tale regolamento si limiti ad affermare all'art. 26 che le piattaforme sono tenute a condividere con la *research community* informazioni che ritengono rischiose in quanto illecite o intenzionalmente manipolate. Tuttavia, non viene specificato come dovrebbe essere posta in essere tale obbligazione nella pratica. A tal riguardo, una parte della dottrina ha espresso l'auspicio che il *Digital Service Act* comprendesse un meccanismo permanente che faciliti la collaborazione con i ricercatori, i quali

hanno sottolineato la necessità della *reasearch community* di avere un accesso permanente ai dati al fine di poter predisporre delle strategie[303].

In ottica riassuntiva, si può, dunque, affermare che le principali innovazioni che saranno introdotte dal *Digital Service Act* consistono in: nuovi sistemi di rimozione dei contenuti illeciti da parte delle piattaforme, con la previsione di una conseguente responsabilità di queste in caso di inerzia; un sistema innovativo di segnalazione da parte degli utenti di contenuti illeciti; l'obbligo di fornire agli utenti una comunicazione trasparente e chiara sulle modalità di erogazione dei servizi da parte della piattaforma; e, infine, il diritto di coloro che pubblicano contenuti sulla piattaforma di essere informati delle ragioni che hanno portato alla rimozione di quel dato contenuto.

3.3. La Responsabilità degli *Internet Service Providers*: l'esperienza italiana

La direttiva CE 31/2000 è stata recepita in Italia con il d.lgs 70/2003, a seguito del quale, per determinare la responsabilità degli ISPs, la giurisprudenza italiana ha adottato un approccio casistico, valutando di volta in volta non solo i criteri oggettivi fissati nella normativa di riferimento ma anche le circostanze concrete del caso[304].

Con specifico riferimento alla responsabilità degli *Internet Service Providers* per il cosiddetto *user-generated content,* anche in Italia viene ripresa la distinzione tra *hosting provider* attivo e passivo, introdotta dalla giurisprudenza europea[305].

---

[303] WANLESS, *How Europe Can Tackle Influence Operations and Disinformation,* in *Carnegie Europe*, 2021; TAMBIAMA MADIEGA, Commissione europea, *Briefing EU Legislation in Progress, European Parliamentary Research Service*, Digital Services Act, marzo 2021, p. 10.

[304] DIOTALLEVI, *Internet e social network, tra "fisiologia" costituzionale e "patologia" applicativa,* in *Giurisprudenza di merito*, n. 12, 2012, p. 2515.

[305] Tribunale Catania, 29 giugno 2004, in *Dir. inf*., 2004, p. 466; Tribunale Milano, 2 marzo 2009, caso RTI c. RCS, in *Dir. inf*., 2009, pp. 521 ss.; Tribunale Roma, 15 dicembre 2009, caso RTI c. You Tube, in *Dir. inf*., 2009, pp. 521 ss.; Tribunale Roma, 11 febbraio 2010, reclamo caso RTI c. You Tube, in *Dir. inf*., 2010, pp. 275 ss.; Tribunale Milano, Sez. Spec. Prop. Ind. e Intellettuale, 7 giugno 2011, n. 7680, caso RTI c. Italia Online (IOL), in *Dir. inf.*, 2011, p. 660 ss.; RTI Mediaset c. IOL (Trib. Milano, Sez. Spec. Prop. Ind. e Intellettuale, 7 giugno 2011, in *Dir. inf*., 2011, p. 660; RONTALDO, PELUSO, *La tutela del diritto d'autore nel settore audiovisivo e la responsabilità degli ISP*, in *Dir. Autore*, 2015, pp. 144 ss.; TOSI, *Contrasti giurisprudenziali in materia di responsabilità civile degli hosting provider - passivi e attivi - tra tipizzazione normativa e interpretazione evolutiva applicata alle nuove figure soggettive dei motori di ricerca, social network e aggregatori di contenuti*, in *Rivista Di Diritto Industriale*, 2017, pp. 75 ss.; Cass. civ., Sez. I, 19 marzo 2019, n. 7708; Cass civ., Sez. I, 19 marzo 2019, n. 7709 con nota di TOSI, *La disciplina applicabile all'hosting provider per la pubblicazione di contenuti digitali protetti dal diritto d'autore, tra speciale irresponsabilità dell'ISP passivo e comune responsabilità dell'ISP attivo, alla luce di Cassazione 7708/2019 e 7709/2019*, in *Rivista di Diritto Industriale*, 2019, pp. 226 ss.

A tal riguardo, un primo approccio alla questione si ebbe nel 2009, se pur con esclusivo riferimento al diritto d'autore.

Si trattava della controversia che ha visto contrapposte la piattaforma *YouTube* e la società RTI[306]. La doglianza di quest'ultima si basava su una presunta violazione dei propri diritti in conseguenza del caricamento sulla piattaforma da parte degli *user* di sequenze di una trasmissione televisiva di cui RTI era licenziataria in via esclusiva. In questa occasione, il Tribunale di Roma ha accolto le argomentazioni di RTI, ritenendo *YouTube* responsabile proprio in ragione della non-neutralità della piattaforma di *hosting*. Nello specifico, il Tribunale ha affermato che il *provider* è responsabile degli illeciti compiuti da soggetti terzi sulla sua piattaforma «quando non si limiti a fornire la connessione alla rete, ma eroghi servizi aggiuntivi […] e/o predisponga un controllo delle informazioni».

La Corte continua affermando che la responsabilità degli ISPs sussiste, tanto più, quando questi nonostante le diffide ripetute e la conseguente consapevolezza dell'illeceità dei contenuti non si attivano per la rimozione di questi.

Dall'analisi di questa pronuncia emerge come, all'epoca, nell'ambito della giurisprudenza di merito vi fosse ancora poca chiarezza sulla differenza tra la responsabilità dell'ISP che deriva dallo svolgimento di un'attività editoriale, facendo quindi venire meno l'esonero di responsabilità in capo al *provider*, e la responsabilità che deriva dall'inerzia di questo quando ricorrono i presupposti di cui all'art. 16 del d.lgs 70/2003[307].

Nel medesimo anno, la tematica della differenza tra *provider* attivo e passivo è stata affrontata anche dalla Corte di Cassazione[308], ancora una volta nell'ambito del diritto d'autore.

Nello specifico, nella pronuncia in esame, secondo la Corte, il fatto che il sito *The Pirate Bay* non si fosse limitato a rendere disponibile per gli utenti un mero protocollo di comunicazione per la condivisione del materiale, ma, al contrario, avesse posto in essere anche attività ulteriori, quali l'indicizzazione dei contenuti, era sufficiente a modificare la qualifica del sito trasformandolo in un ISP attivo.

---

[306] Tribunale Roma, 16 dicembre 2009; Tribunale Roma, 11 febbraio 2010.

[307] POLLICINO, *Tutela e pluralismo nell'era digitale: ruolo e responsabilità degli Internet service providers*, cit., pp. 18-19.

[308] Cass. pen., Sez. III, 29 settembre 2009, n. 49437.

E ancora, nella medesima direzione negli anni successivi si sono mosse diverse pronunce[309], alla luce della quali si può affermare che, proprio seguendo l'approccio casistico che ha caratterizzato la giurisprudenza di merito italiana sin dall'entrata in vigore del d.lgs 70/2003, talvolta non è necessario stabilire se il *provider* sia attivo o passivo, essendo al contrario sufficiente dimostrare che questo fosse a conoscenza, o avrebbe dovuto essere a conoscenza, dell'illiceità dei contenuti pubblicati dagli utenti[310]. A tal riguardo, tuttavia, se da un lato l'acquisizione di conoscenza dell'illecito da parte dell'ISP si presume realizzata in seguito alla diffida del titolare dei diritti lesi, dall'altro quest'ultimo non può limitarsi a diffide generiche, ma deve indicare tutti gli URL di cui chiede l'eliminazione[311].

Per quanto concerne, però, specificatamente la figura dell'*hosting provider* attivo, assume particolare rilevanza il caso *RTI v. Yahoo*[312]. Su questo si è pronunciato dapprima il Tribunale di Milano fornendo una delle prime elaborazioni della nozione del *hosting attivo* e successivamente la Corte di Appello[313], che ha riformato la precedente decisione specificando che l'esenzione di responsabilità deve essere applicata a tutti gli *hosting provider* che non abbiano una conoscenza diretta dell'illiceità dei contenuti.

Tuttavia, la Corte di Cassazione ha cassato la pronuncia della Corte di Appello riconoscendo la distinzione tra *hosting provider* attivo e passivo[314], e precisando che ai primi deve essere applicato il regime generale della responsabilità civile aquiliana[315].

A tal riguardo la Corte ha affermato che «L'*hosting provider* attivo è il prestatore dei servizi della società dell'informazione il quale svolge un'attività che esula da un servizio di ordine meramente tecnico, automatico e passivo, e pone, invece, in essere una condotta attiva, concorrendo con altri nella commissione dell'illecito,

[309] Tribunale Roma, 17 agosto 2011; Cass. pen., sez. III, 3 febbraio 2014, n. 3672, in www.dejure.it.
[310] Tribunale Roma, 5 maggio 2016, n. 24707, RTI Italia c. Kit Digital France.
[311] Tribunale Roma, 11 luglio 2011, PFA Film s.r.l. c. Google Italia s.r.l. e Yahoo! Italia Inc.
[312] Tribunale Milano, sez. spec. prop. ind. e intellettuale, 9 settembre 2011, n. 10893, in *Riv. dir. ind*., 2012, p. 364 ss., con nota di SARACENO, *Note in tema di violazione del diritto d'autore tramite Internet; la responsabilità degli Internet service provider*.
[313]Corte di Appello di Milano, sez. impr., 7 gennaio 2015, n. 29, in *Dir. ind*., 2016, pp. 166 ss., con nota di IASELLI, *Caso Yahoo! Video: la Corte di Appello di Milano non vede responsabilità nell'operato dell'internet provider*.
[314] Cass. civ., I sez., 19 marzo 2019, n. 7708.
[315]FRIGERIO, *Responsabilità dell'hosting provider: la Cassazione conferma la distinzione tra attivo e passivo*, in *www.filodiritto.it*, 2019.

onde resta sottratto al regime generale di esenzione di cui all'art. 16 d.lgs. n. 70 del 2003, dovendo la sua responsabilità civile atteggiarsi secondo le regole comuni».

La Corte ha, poi, continuato precisando che «nell'ambito dei servizi della società dell'informazione, la responsabilità dell'*hosting provider*, prevista dall'art. 16 d.lgs. 9 aprile 2003, n. 70, sussiste in capo al prestatore dei servizi che non abbia provveduto all'immediata rimozione dei contenuti illeciti, nonché se abbia continuato a pubblicarli, pur quando ricorrano congiuntamente le seguenti condizioni: a) sia a conoscenza legale dell'illecito perpetrato dal destinatario del servizio, per averne avuto notizia dal titolare del diritto leso oppure *aliunde*; b) l'illiceità dell'altrui condotta sia ragionevolmente constatabile, onde egli sia in colpa grave per non averla positivamente riscontata, alla stregua del grado di diligenza che è ragionevole attendersi da un operatore professionale della rete in un determinato momento storico; c) abbia la possibilità di attivarsi utilmente, in quanto reso edotto in modo sufficientemente specifico dei contenuti illecitamente immessi da rimuovere».

Dunque, in questa prospettiva, alla figura dell'*hosting provider* attivo si applicherebbe la disciplina di diritto comune prevista dall'art. 2043 c.c.[316]. In altre parole, il filone dottrinale e giurisprudenziale in esame sostiene che possa configurarsi la fattispecie della *culpa in vigilando* in capo agli ISPs in tutti quei casi in cui gli illeciti sul *web* si verificano a causa dell'attività da questi svolta.

Più precisamente, all'*hosting provider* dovrebbe essere ricondotta una responsabilità esclusiva quando l'autore diretto non sia identificabile e una responsabilità concorrente nei casi in cui questo, invece, sia identificato[317].

A tal riguardo, una soluzione peculiare è stata proposta da Bocchini, secondo il quale l'illecito in esame costituirebbe un «illecito plurisoggettivo eventuale a formazione progressiva» o un «illecito plurisoggettivo permanente a cooperazione eventuale successiva», in quanto il *provider* coopererebbe con l'autore diretto sin dall'origine del perfezionamento dell'illecito, dal momento che è «l'autore della intermediazione che ha creato il presupposto necessario del fatto».

---

[316] Tribunale Milano, 25 gennaio 2011, in *Resp. civ. prev.*; Tribunale Milano, 31 marzo 2011, in *Resp. civ. prev*., 2011, p. 1320, con nota di PERON, *Sulla diffamazione commessa tramite motore di ricerca*; Tribunale Milano, 25 maggio 2013, in *Resp. civ. prev*., 2013, p. 119, con nota di BUGIOLACCHI, *Evoluzione dei servizi di hosting provider, conseguenze sul regime di responsabilità e limiti dell'attuale approccio case by case*.

[317] NATOLI, *La tutela dell'onore e della reputazione in internet: il caso della diffamazione anonima*, in *Eur. dir. priv.,* 2001, p. 461.

In aggiunta, secondo l'autore, l'illecito si trasformerebbe da monosoggettivo a plurisoggettivo nel momento in cui la piattaforma non agisce *ex post* per rimuovere il contenuto[318].

Un'altra corrente di pensiero ritiene che anche l'art. 2050 c.c. dovrebbe essere considerato applicabile agli *Internet Service Providers*.

Tale teoria prende le mosse dall'ampia nozione di attività pericolose fornita dalla giurisprudenza, secondo cui queste comprendono anche quelle condotte non tipizzate nel codice o nelle leggi speciali che, tuttavia, per la loro stessa natura e per la tipologia dei mezzi utilizzati comportano una rilevante possibilità che si verifichi un danno[319].

In tale ottica, viene affermato che l'attività dei *provider* rientrerebbe tra le attività pericolose atipiche, in quanto queste possiederebbero una oggettiva potenzialità lesiva più alta del normale, rilevabile non solo tramite dati statistici, ma anche sulla base di elementi di comune esperienza[320].

Ne consegue che l'applicabilità dell'art. 2050 c.c. agli ISPs, che viene giustificata proprio alla luce di tale potenziale pericolosità specifica[321], comporterebbe l'inversione nell'onere probatorio in relazione all'elemento soggettivo della colpa, facendo sì che dovrebbe essere il *provider* a dimostrare di aver posto in essere ogni cautela idonea ad evitare il danno.

In ottica riassuntiva, ad oggi si afferma che, nonostante alcuni pareri contrari,[322] si sia consolidato il filone interpretativo che sostiene che il regime di esonero da responsabilità debba essere considerato quale disciplina speciale applicabile esclusivamente ai *provider* che non intervengano in alcun modo sullo *user-*

---

[318] BOCCHINI, *La responsabilità di Facebook per la mancata rimozione di contenuti illeciti*, in *Giur.it*., 2017, pp. 640-643.

[319] Cass. civ., sez. III, 6 aprile 2006, n. 8095, in *Responsabilità Civile*, 7/2006, pp. 662 ss., con nota di FACCI; Cass. civ., sez. I, 27 gennaio 2006, n. 1755; Cass. civ., sez. III, 21 ottobre 2005, n. 20359; Cass. civ., sez. III, 21 ottobre 2005, n. 20357; Cass. civ., sez. III, 27 maggio 2005, n. 11275; Cass. civ., sez. III, 15 ottobre 2004, n. 20334; Cass. civ., sez. III, 26 aprile 2004, n. 7916; Cass. pen., sez. IV, 27 maggio 2003, n. 34620; Cass. civ., sez. III, 10 febbraio 2003, n. 1954; Cass. civ., sez. III, 19 luglio 2002, n. 10551, in *Danno e Resp*., 12/2002, 1214 ss., con nota di AGNINO; Cass. civ., sez. III, 5 giugno 2002, n. 8148.

[320] MICELI, *Profili evolutivi della responsabilità in Rete: il ruolo degli Internet Service Providers tra prevenzione e repressione*, in *Media Laws*, 2017, p. 113.

[321] SICA, *Il commercio elettronico. Profili giuridici*, Torino, 2001.

[322] POLLICINO, T*utela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider*, in *www.giurcost.org*, p. 13; BOCCHINI, *La responsabilità di Facebook*, cit., pp. 639 e ss; Tribunale Pinerolo, 30 aprile 2012; Tribunale Milano, 25 marzo 2013.

generated content, che, dunque, deve essere pubblicato in maniera autonoma dagli utenti senza alcun intervento ulteriore da parte della piattaforma[323].

Nello specifico, per quanto concerne attività quali l'indicizzazione, organizzazione e selezione del materiale diffuso sulla piattaforma, è stato affermato che questi costituiscano «indici rivelatori di un'attività di interferenza» posta in essere dal *provider,* in quanto mediante lo svolgimento di tali funzioni questi acquisiscono una, seppur minima, consapevolezza di ciò che viene divulgato[324].

Per quanto concerne l'obbligo di rimozione *ex post*, noto come *take-down,* secondo un filone dottrinale, al fine di far sorgere tale dovere in capo al *provider*, sarebbe sufficiente la conoscenza comunque acquisita da questo, pur in assenza di formali comunicazioni dell'autorità competente[325].

Tale orientamento è stato oggetto di forti critiche[326], che sono andate a inserirsi nel solco di pronunce giurisprudenziali secondo cui sussistono dei requisiti molto rigorosi che devono essere soddisfatti al fine di poter affermare che il *provider* abbia una conoscenza effettiva dell'illiceità del contenuto[327]; nello specifico, è necessario

---

[323] Trib. Roma, sez. impr., 27 aprile 2016, n. 8437, in *Riv. dir. ind*., 2017, p. 56 ss.; BUGIOLACCHI, *Ascesa e declino della figura del provider "attivo"? Riflessioni in tema di fondamento e limiti del regime privilegiato di responsabilità dell'hosting provider*, in *Resp. civ. prev*., 2015, p. 1261 ss.; BOCCHINI, *La responsabilità di Facebook per la mancata rimozione di contenuti illeciti*, cit., pp. 638 ss.; TOSI, *Contrasti giurisprudenziali in materia di responsabilità civile degli hosting provider- passivi e attivi- tra tipizzazione normativa e interpretazione evolutiva applicata alle nuove figure soggettive dei motori di ricerca, social network e aggregatori di contenuti*, in *Riv. dir. ind*., 2017, pp. 61 ss.

[324] TOSI, *Contrasti giurisprudenziali in materia di responsabilità civile degli hosting provider - passivi e attivi- tra tipizzazione normativa e interpretazione evolutiva applicata alle nuove figure soggettive dei motori di ricerca, social network e aggregatori di contenuti*, cit., pp. 84 ss.; GELLI *False recensioni su TripAdvisor: accolta l'azione inibitoria promossa dal ristoratore diffamato*, in *Corr. giur*., 2016, p. 89.

[325] BUGIOLACCHI, *I presupposti dell'obbligo di rimozione dei contenuti da parte dell'hosting provider tra interpretazione giurisprudenziale e dettato normativo*, in *Resp. civ. prev*., 2017, pp. 540-541; Tribunale Catania, 29 giugno 2004, in *Resp. civ. prev*., 2005, 188, con nota di BUGIOLACCHI, *La responsabilità dell'host provider alla luce del d.lgs. n.70 del 2003: esegesi di una disciplina "dimezzata"*; Tribunale Bari, 13 giugno 2006, in *Dir. internet*, 2006, p. 563; Tribunale Trani, 14 ottobre 2008, in *Danno resp*., 2009, p, 105; Tribunale Roma, 11 febbraio 2010, in *Dir. inform. e informatica*, 2010, p. 275; Tribunale. Milano, 20 gennaio 2011, n. 7680, in *Dir. ind*., 2012, p. 255, con nota di BELLAN, *Per una reasonable liability: critiche alla responsabilità oggettiva dei provider e tutela dei diritti su internet*; Tribunale Torino, 5 maggio 2014, in *www.marchiebrevettiweb.it*; Tribunale Torino, 23 giugno 2014, in *www.marchiebrevettiweb.it*; Tribunale Napoli Nord, sez. civ., II, 3 novembre 2016, in *Giur. it*., 2017, p. 629 ss., con nota di BOCCHINI, *La responsabilità di Facebook per la mancata rimozione di contenuti illeciti*; Tribunale. Torino, sez. impr., 7 aprile 2017, n. 1928, in *Danno resp*., 2018, pp. 87 ss.

[326] RICCIO, *La responsabilità civile degli internet providers*, in *Media Laws*, 2012, p. 210; SICA, *Responsabilità del provider: per una soluzione "equilibrata" del problema*, in *Corr. giur*., 2013, p. 509.

[327] Tribunale Firenze, 25 maggio 2012, in *Dir. informaz. informatica*, 2012, p. 1210, con nota di SCANNICCHIO, *La responsabilità del motore di ricerca per la funzione "auto-complete" – che sottolinea come le diffide dei terzi non siano sufficienti a far sorgere, in capo al provider, l'obbligo*

che siano rispettate entrambe le condizioni poste dall'art. 16 d.lgs 70/2003, rispettivamente alle lettere a) e b) del comma I.

Ne consegue che, secondo tale orientamento, l'ISP diviene responsabile della rimozione di contenuti illeciti solo a seguito della ricezione di un ordine da parte dell'autorità competente.

Tuttavia, a livello giurisprudenziale sembra prevalere l'opinione secondo cui l'obbligo di *take down* del *provider* sussisterebbe anche a seguito della semplice segnalazione da parte della persona offesa[328]; opinione per altro in linea con l'interpretazione fornita dalla Corte di Giustizia dell'Unione Europea della nozione di "conoscenza effettiva"[329].

Una pronuncia emblematica in materia di responsabilità degli *hosting providers*, obblighi di rimozione e doveri di sorveglianza è rappresentata dal caso Cantone[330]. La vicenda riguardava una donna napoletana, Tiziana Cantone, la quale si è tolta la vita a seguito del fatto che alcuni suoi video intimi, dalla stessa condivisi su *WhatsApp* con un piccolo gruppo di conoscenti, sono divenuti virali sui *social network.* Nel 2015 la donna si è rivolta al giudice civile chiedendo l'emissione di un provvedimento d'urgenza che intimasse alle piattaforme *social* in questione di rimuovere i video e di inibire ogni accesso. Il Tribunale, tuttavia, ha accolto il ricorso in maniera parziale, ordinando solamente nei confronti di *Facebook* e altri quattro siti, tra cui alcune testate giornalistiche, «l'immediata cessazione e rimozione dalla piattaforma del *social network* di ogni *post* o pubblicazione contenente immagini (foto e/o video) o apprezzamenti riferiti specificamente alla persona della ricorrente».

---

di intervento, dal momento che si tratta, pur sempre, di prospettive unilaterali; Corte di Appello Milano, 7 gennaio 2015, n. 29.

[328] PANATTONI, *Il sistema di controllo successivo: obbligo di rimozione dell'ISP e meccanismi di notice and take down*, in *Dir. pen. cont.*, 2018, n. 5, pp. 255-256; IASSELLI, *Responsabilità del provider: la Cassazione detta rilevanti principi di diritto*, in <<https://www.altalex.com/documents/news/2019/03/20/diritto-d-autore-responsabilita-dell-hosting-provider>>; Cass. civ., sez. I, del 19 marzo 2019, n. 7708.

[329] Corte di Giustizia UE (Grande sezione), 23 marzo 2010 (domande di pronuncia pregiudiziale, proposte dalla Cour de Cassation - Francia), cause riunite da C-236/08 a C-238/08, Google France SARL e Google Inc. c. Louis Vouitton Malletier SA (C-236/08), Google France SARL c. Viaticum SA e Luteciel SARL (C-237/08), Google France SARL, Centre National de recherche en relations humaines (CNRRH) SAR, Pierre Alexis Thonet, Bruno Raboin e Tiger SARL (C-238/08); SCANNICCHIO, VECCHIO, I *limiti della neutralità: la Corte di giustizia e l'eterno ritorno dell'hosting attivo*, in *www.filodiritto.it*, 2019; Corte Giustizia UE, 12 luglio 2011, C-324/09, l'Oréal SA e a.c. eBay International AG, in *AIDA*, 2011, pp. 480 ess., con nota di NORDEMANN, *Liability of Social Networks for IP Infringements (Latest News): The Eu Law Regime after l'Oréal/eBay*, paras 120-121.

[330] Tribunale Napoli Nord, 10 agosto 2016.

Nel settembre del 2016, avverso la suddetta ordinanza la piattaforma *social Facebook Ireland Ltd.* ha presentato un reclamo avente ad oggetto tre punti principali.

Innanzitutto, *Facebook* sottolineava che i *link* indicati da Tiziana Cantone non erano più visibili attraverso la piattaforma al momento della decisione di primo grado. In secondo luogo, il *social network* poneva l'accento sul fatto che l'eccessiva genericità dell'ordine di rimozione emesso dal Tribunale rendeva questo inattuabile, implicando oneri di sorveglianza preventiva in capo al *provider* non previsti dalla legge. Infine, il reclamo della piattaforma si concentrava sull'affermare che il d.lgs 70/2003 non impone agli ISPs alcun obbligo di rimozione in assenza di un ordine emesso dalle competenti autorità.

In sede di reclamo[331], il giudice ha accolto la doglianza di *Facebook*, abbracciando l'argomentazione secondo cui non sussistono obblighi di sorveglianza preventiva o di ricerca attiva di fatti e informazioni oggetto di *hosting* in capo ai *provider*.

Al contempo, tuttavia, il giudice del reclamo ha ritenuto «sussistente una responsabilità per le informazioni oggetto di memorizzazione durevole o "hosting" laddove, come avvenuto nel caso di specie, il *provider* sia effettivamente venuto a conoscenza del fatto che l'informazione è illecita [...] e non si sia attivato per impedire l'ulteriore diffusione della stessa».

Nello specifico, il giudice ha ritenuto che, pur in assenza di un ordine di rimozione da parte delle autorità competenti, l'obbligo sussista «per effetto di una conoscenza acquisita *aliunde*, magari in modo specifico e qualificato, come nel caso di denuncia del soggetto cui l'attività o l'informazione si riferisce».

Ne consegue che nel caso in esame il giudice è giunto alla conclusione che «pur non essendovi un obbligo di controllo preventivo dei contenuti presenti né una posizione di garanzia, sussiste tuttavia un obbligo successivo di attivazione di modo che la responsabilità a posteriori dell'*hosting provider* sorge per non aver ottemperato – come per l'appunto verificatosi nella fattispecie in esame – a una richiesta (diffida) di rimozione dei contenuti illeciti proveniente dalla parte che assume essere titolare dei diritti, ovvero per non aver ottemperato a un ordine dell'autorità, sia essa giurisdizionale o amministrativa, cui si sia rivolto il titolare del diritto per ottenere il medesimo effetto». Tuttavia, l'onere della prova continua

[331] Tribunale. Napoli Nord, sez. II civ., 3 novembre 2016.

a incombere sul soggetto passivo, il quale in giudizio dovrà dimostrare che «il *provider* era, comunque, stato messo a conoscenza del contenuto illecito di un'attività o di un'informazione alla quale dava accesso e che, nonostante ciò, non si sia attivato per darne tempestiva comunicazione all'autorità, né abbia provveduto ad impedire prontamente l'accesso a quel determinato contenuto».

Tale pronuncia assume una rilevanza particolare in quanto, a differenza delle precedenti decisioni analizzate, in questo caso il giudice non ha fondato la propria statuizione sulla distinzione di matrice giurisprudenziale tra *hosting* attivo e passivo, bensì si è soffermato sull'aspetto dell'effettiva conoscenza dell'illecito, in qualsiasi modo acquisita, da parte del *provider*. Ne è conseguito che, il giudice ha considerato tale conoscenza effettiva come fonte dell'obbligo di rimozione *ex post* dei contenuti pubblicati dagli utenti, prendendo in considerazione anche il profilo della lesione dei diritti della personalità[332].

Passando ora specificatamente all'ambito del diritto penale italiano, la giurisprudenza di legittimità ha adottato approcci divergenti: se in un primo momento questa ha escluso che sussista una posizione di garanzia in capo ai *provider* nel caso *Google c. Vividown*[333], successivamente il rappresentante legale della società Kines s.r.l. è stato ritenuto responsabile di diffamazione per non essersi attivato per rimuovere un contenuto lesivo dell'altrui reputazione, pur essendo a conoscenza del carattere diffamatorio di questo[334].

In ottica di comparazione con il modello statunitense, assume particolare rilevanza il caso *Force v. Facebook* sopra analizzato[335]. Infatti, la vicenda in questione presentava l'essenziale elemento di novità del ruolo giocato dagli algoritmi nella definizione della responsabilità degli ISPs per i contenuti pubblicati dagli utenti.

Riportando tale dibattito nel panorama penalistico italiano, vi è una parte della dottrina che sostiene che in caso di utilizzo di elementi di intelligenza artificiale dovrebbe essere ritenuto responsabile l'utente finale, per essersi colposamente affidato all'innovazione tecnologica, ed essersi, quindi, consciamente assunto il rischio del verificarsi di illeciti[336].

---

[332] ABBONDANTE, *il ruolo dei social network nella lotta all'hate speech: un'analisi comparata fra l'esperienza statunitense e quella europea*, in *Informatica e Diritto*, XLII, Vol. XXVI, n. 1-2, p. 103.
[333] Cass. pen., Sez. III, 17 dicembre 2013, n. 5107.
[334] Cass. pen., Sez. V, 27 dicembre 2016, n. 54946.
[335] V. *infra* § 3.1.
[336] SARTOR., *L'intenzionalità degli agenti software e la loro disciplina giuridica*, in *Researchgate.net*, 2002.

Tuttavia, tale teoria trova un ostacolo pressoché insormontabile nel divieto di responsabilità penale oggettiva presente nel nostro ordinamento.

Ne consegue che, l'unico fondamento normativo della cosiddetta "teoria dell'utente finale" è ravvisabile nell'art. 116 c.p., effettuando, quindi, un'assimilazione tra l'*hosting provider* attivo, o l'utente finale, e il soggetto che agisce in concorso e che è chiamato a rispondere anche dell'evento non voluto ma prevedibile[337].

In ogni caso, anche tale modello troverebbe difficilmente applicazione nel nostro ordinamento in quanto colui che fa uso dell'algoritmo non sta ponendo in essere alcun illecito voluto e, ad ogni modo, si trova in una posizione di rischio tollerato.

Da ciò discende che risulta necessaria l'introduzione di una disciplina che consenta di ritenere responsabile l'uomo per gli illeciti commessi tramite l'uso di intelligenza artificiale, ma che al contempo comprenda una scriminante per le circostanze in cui siano poste in essere tutte le cautele e le misure necessarie a prevenire la commissione di reati[338].

In conclusione, tanto dall'analisi del quadro normativo statunitense, quanto dall'esposizione della disciplina europea, e nell'ambito di questa della normativa italiana, appare evidente che la giurisprudenza negli ultimi anni abbia fondato la responsabilità degli ISPs sulla distinzione tra *provider* attivi e passivi.

Risulta, tuttavia, altrettanto chiaro che la continua evoluzione tecnologica e digitale richiede l'introduzione di una disciplina specifica per le piattaforme *web*, la quale tenga conto delle peculiarità di queste e del progressivo accrescimento dei processi di automazione da queste impiegati.

[337] BACCIN, *Responsabilità penale dell'Internet Service Provider e concorso degli algoritmi negli illeciti online: il caso Force v. Facebook*, cit., p. 101.
[338] *Ibidem.*

CAPITOLO IV

IV. L'IMPATTO DELLE *FAKE NEWS* SULLA DEMOCRAZIA

4. Processi democratici e *social network*: la "*Bubble Democracy*"

Passando all'analisi delle conseguenze della diffusione di *fake news* a livello nazionale e sovranazionale, tra gli effetti negativi di queste va sicuramente annoverata l'alterazione dei processi democratici, e un conseguente impatto sulla sovranità degli Stati.

Lo stesso Rappresentante OCSE per la Libertà dei Media – ossia l'istituzione che si occupa del monitoraggio dell'esercizio della libertà di espressione attraverso i *media* negli Stati Membri dell'Organizzazione per la sicurezza e la cooperazione in Europa (OCSE) – ha riconosciuto la crescente problematica connessa alla disinformazione nell'ambito dei processi elettorali e democratici, affermando che la «*disinformation, sometime referred to as "false" or "fake news", and propaganda pose numerous threats to democratic societies*»[339].

L'avvento delle nuove tecnologie, e in particolare delle piattaforme *social*, ha creato una nuova sfera pubblica, che, pur potendo apparire come emblema del pluralismo e della condivisione, in realtà costituisce terreno fertile per le campagne di disinformazione e propaganda[340]. In altre parole, i *social network* hanno dato vita a degli spazi pubblici virtuali, che se da un lato potenzialmente consentono il coinvolgimento dell'interezza degli elettori nel dibattito politico, dall'altro di fatto celano e comportano una grande frammentazione[341].

Infatti, mentre i *media* tradizionali avevano una struttura verticale che consentiva un meccanismo di filtraggio in base al quale le notizie venivano pubblicate solo dopo aver passato lo scrutinio degli editori e degli altri soggetti coinvolti, i nuovi *media*, trovando il proprio fondamento in uno scambio orizzontale di idee e opinioni, lasciano libero spazio a manipolazioni e alterazioni del dibattito pubblico.

---

[339] OCSE, *Free media against propaganda*, <<https://www.osce.org/fom/319286>>.

[340] PARLAMENTO EUROPEO, POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS, *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*, 2019, p. 52.

[341] *Ibidem.*

Questo scenario ha comportato il passaggio dalla Democrazia del pubblico a quella che oggi viene definita da molti come l'era della "*Bubble Democracy"*[342].

Nell'ultimo secolo, infatti, si sono succedute tre tipologie di Democrazia[343]: la Democrazia dei Partiti, la Democrazia del Pubblico e la *Bubble Democracy*.

La prima metà del '900 è stata permeata dalla cosiddetta Democrazia dei Partiti di massa, caratterizzata da ideologie forti che hanno permesso l'immissione delle masse nel sistema democratico. A partire dalla metà del '900, soprattutto grazie all'avvento della televisione, si è, poi, assistito alla trasformazione dei partiti nei cosiddetti *catch all parties,* ossia partiti privi di riferimento a una specifica classe sociale, con una scarsa identità ideologica ma alla ricerca di consensi in tutti gli ambiti della società. Infine, nella prima decade degli anni 2000, con il progressivo affermarsi di Internet quale primaria forma di comunicazione e informazione tra cittadini, si è giunti all'era della *Bubble Democracy.*

La locuzione *Bubble Democracy* prende il nome dalle cosiddette bolle di filtraggio presenti su Internet, ossia algoritmi che fanno sì che gli utenti entrino a contatto solo con informazioni coerenti con i propri orientamenti, creando così dei sistemi chiusi e autoreferenziali in cui trovano spazio esclusivamente le notizie conformi alle idee proprie di quella specifica camera d'eco[344].

Ciò non solo comporta una frammentazione, una polarizzazione e una radicalizzazione della politica, ma incentiva anche spinte centripete lesive della democrazia e della sovranità statale.

D'altronde, come affermato da Giovanni Pitruzzella nel suo articolo sulla libertà di informazione nell'era di Internet, «nel DNA delle democrazie occidentali c'è […] il *government by discussion*, cioè il principio secondo cui deve essere garantito un confronto pubblico e aperto tra idee diverse e confliggenti, che permette a ogni cittadino di scegliere la sua verità»[345].

Tutto ciò, al contrario, è impedito dalla polarizzazione e dalle *filter bubbles* che fanno sì che gli elettori siano sempre più chiusi nella propria bolla, nella quale gli

---

[342] PITRUZZELLA, POLLICINO, QUINTARELLI, *Potere e parole, libertà di espressione, hate speech e fake news,* cit., pp. 86.

[343] PITRUZZELLA, POLLICINO, QUINTARELLI, *Potere e parole, libertà di espressione, hate speech e fake news,* cit., pp. 86-89.

[344] MEZZANOTTE, *Fake news nelle campagne elettorali digitali. Vecchi rimedi o nuove regole?,* in *Federalismi.it,* 2018, pp. 19-20; PARLAMENTO EUROPEO, POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS, *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States,* cit., p. 58.

[345] PITRUZZELLA, *La libertà di informazione nell'era di Internet*, in *media laws*, 1/2018, p. 29

vengono offerti "universi paralleli, ma separati"[346], venendo così privati della possibilità di formare un proprio pensiero critico, libero e informato.

Questo scenario ha inevitabilmente una ricaduta diretta su ciò che rappresenta il fulcro della democrazia, ossia sul dibattito politico, e sull'esercizio del diritto di voto che ne costituisce l'estrinsecazione ultima.

Infatti, tale frammentazione rende le democrazie occidentali un facile bersaglio per la disinformazione che, come analizzato in precedenza[347], trova nella polarizzazione presente su Internet terreno fertile per diffondersi in maniera rapida e capillare; non a caso la problematica delle campagne di disinformazione diviene più evidente nel delicato momento delle tornate elettorali, sotto forma di influenza sull'esito delle stesse[348]. Secondo i dati dello *Special Eurobarometer* sulla democrazia e le elezioni, il 73% degli utenti di Internet intervistati ha espresso la propria preoccupazione sulla disinformazione e la *misinformation on-line* con riferimento alla fase immediatamente precedente alle elezioni, siano esse regionali, nazionali o europee[349].

Nello specifico, le campagne di disinformazione nel corso delle elezioni vengono poste in essere mediante delle minacce "ibride" che spesso si avvalgono di elementi di per sé leciti, ma utilizzati in maniera malevola. Si tratta di strategie che non di rado sfruttano zone legali grigie, in cui i confini sono labili e poco precisi[350].

Per quanto concerne le singole metodologie utilizzate, in prima approssimazione possiamo distinguere due categorie: manipolazioni dirette dei risultati delle elezioni, che possono concretizzarsi ad esempio nell'*hackeraggio* di sistemi di votazione, e le cosiddette *Information Operations* o *Cyber Operations*, ossia operazioni che influenzano le abitudini e i comportamenti degli elettori, andando a impattare in via mediata le risultanze delle votazioni elettorali[351].

---

[346] PARISER, *The filter bubble. What the Internet is Hiding from you*, New York, 2011, p. 8

[347] V. *supra* Cap. I, § 1.

[348] ZICCARDI, *Tecnologie per il potere*, Milano, 2019; SUNSTEIN, *A cosa servono le costituzioni. Dissenso politico e democrazia discorsiva*, Bologna, 2009, pp. 17 e ss; SPADARO, *Contrasto alle fake news e tutela della democrazia*, in *dirittifondamentali.it*, 1/2019, p. 10.

[349] Special Eurobarometer 477: *democracy and elections*, <<https://data.europa.eu/euodp/en/data/dataset/S2198_90_1_477_ENG>>.

[350] RODRIGUEZ, *Disinformation Operations Aimed at (Democratic) Elections in the context of Public International Law: The conduct of the Internet Research Agency during the 2016 US Presidential Eelections*, in *International Journal of Legal Information*, 2019, p. 152 e ss.

[351] HANSEN, JIM, *Doxing Democracy: Influencing Elections via cyber Voter influence*, in *Contemporary politics*, 2018, pp. 151-154.

In altre parole si tratta dell'utilizzo di sistemi informatici con lo scopo primario di colpire determinati obiettivi all'interno del cyberspazio o attraverso questo[352].

In questa seconda categoria di operazioni l'informazione, sia essa vera o falsa, viene utilizzata per esercitare un'influenza sul funzionamento stesso dello Stato. Infatti, l'obiettivo perseguito è sì quello di influenzare la coscienza di massa, ma esclusivamente al fine di manipolare l'opinione pubblica e quindi, in ultima analisi, la politica dello Stato. E', dunque, l'apparato pubblico stesso a essere oggetto delle *Information Operations,* più che i singoli soggetti privati[353].

All'interno di questa seconda tipologia di operazioni possiamo ulteriormente individuare tre specifiche strategie di disseminazione di disinformazione: le *Doxing Operations*, le *Propaganda Operations* e le *Disinformation Operations.*

Le *Doxing Operations* consistono nella diffusione selettiva di informazioni vere ma confidenziali. La *ratio* che guida gli Stati nella scelta di adottare tale strategia risiede nella volontà di diffondere informazioni non pubbliche ma verificabili allo scopo di influenzare l'opinione pubblica; attraverso questa tecnica gli autori delle *Doxing Operations* esercitano indirettamente pressione politica e quindi influenzando gli affari interni ed esterni dello Stato passivo, e, in ultima analisi, il processo politico di un altro Stato[354].

La seconda metodologia più diffusa di alterazione del processo democratico fa capo alle cosiddette *Propaganda Operations.* Si tratta ancora una volta di una tecnica di diffusione selettiva di informazioni, ma questa volta riguardanti argomenti normativi. Questa strategia ha lo scopo di diffondere determinate idee o valori, che però molto frequentemente sono manipolati o addirittura consciamente falsi[355].

La terza e ultima tecnica fa riferimento alle *Disinformation Operations*: si tratta di operazioni volte a influenzare il risultato elettorale mediante la diffusione di vere e proprie *fake news* su Internet.

Una volta analizzata la differenza formale tra queste tre categorie, è, tuttavia, importante ricordare che i confini tra queste sono molto labili e, nella pratica, finiscono spesso per sovrapporsi. Ne è dimostrazione il fatto che non di rado la

---

[352] DEPARTMENT OF DEFENCE (US DOD), *Memorandum of chiefs of military services: joint terminology for cyberspace operations*, p. 8.

[353] VAN DE VELDE, *The law of cyber interference in elections*, in *Yale Law School*, 2017, p. 8.

[354] HANSEN, JIM, *Doxing Democracy: Influencing Elections via cyber Voter influence*, cit., pp. 150-154.

[355] VAN DE VELDE, *The law of cyber interference in elections*, cit., pp. 20-21.

NATO e il Parlamento Europeo usano i termini come sinonimi al fine di descrivere campagne di disinformazione strategicamente orchestrate al fine di influenzare i processi democratici[356].

Dunque, quale che sia la tecnica o la combinazione di strategie utilizzate possiamo individuare dei tratti comuni e degli obiettivi condivisi delle cosiddette *fake news* "politiche".

Per quel che concerne il primo profilo, vale a dire gli aspetti che accomunano le *fake news* politiche, queste si caratterizzano per il fatto di fondarsi su una condivisione virale, di confidare da un lato sulla non verificabilità immediata della notizia e dall'altro sull'autorevolezza che una *fake news* acquisisce tramite le tante condivisioni da parte degli utenti, e, infine, di essere sempre più mirate sul soggetto destinatario grazie al fenomeno della polarizzazione[357].

Passando ora agli obiettivi comuni delle *fake news* politiche, tra questi possiamo sicuramente annoverare: la creazione di un clima di abitudine agli scandali e sfiducia nelle istituzioni, finalizzato a rendere più agevole la manipolazione dei comportamenti degli elettori; la creazione di momenti di attrito tra Stati indebolendo, così, le difese di questi; il condurre uno Stato a prendere decisioni di politica interna o estera contrarie al proprio interesse nazionale; il danneggiare la reputazione dello Stato passivo, andando, così, a impattare direttamente la sovranità dello stesso; il diffondere paura od odio, incoraggiando comportamenti irrazionali o violenti; ed infine, l'occupare lo spazio mediato al fine di polarizzare la discussione[358].

L'insieme di questi fenomeni, grazie all'aiuto fornito dalla crescente polarizzazione dell'elettorato, comporta dei seri rischi per il sistema democratico, costituendo una minaccia non solo per il pluralismo, per la diversificazione dell'offerta politica e per il diritto alla parità nella competizione elettorale, ma anche per la corretta informazione dei cittadini, e per la libertà di formazione del consenso elettorale[359]. Questo, negli ultimi decenni, ha comportato un impoverimento del dialogo e del

---

[356] PARLAMENTO EUROPEO, POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS, *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*, cit., p. 27.

[357] SUFFIA, ZICCARDI, *Fake news guerra dell'informazione ed equilibri democratici,* in *Federalismi.it*, 2020, pp. 223-224.

[358] GERMANI, *la minaccia della disinformazione: panoramica introduttiva*, in ID. (a cura di), *Disinformazione e manipolazione delle percezioni, Una nuova minaccia al Sistema-Paese*, Roma, 2017.

[359] GERMANI, *La minaccia della disinformazione: panoramica introduttiva*, cit., pp. 225-226.

dibattito politico che ha avuto e ha tutt'oggi effetti diretti sulla qualità della democrazia: se da un lato vi è stato un generale declino o una radicale trasformazione dei partiti tradizionali in Europa, dall'altro si è assistito all'emersione di nuove forze politiche radicali[360].

D'altronde, non poteva essere altrimenti tenuto conto del fatto che il diritto costituzionale di essere informato comprende necessariamente al proprio interno un profilo di natura qualitativa, inerente il contenuto della notizia diffusa[361].

Se è dunque vero quanto affermato dalla Corte di Cassazione nella sentenza n. 23576 del 2013[362], secondo cui «la critica politica può assumere toni più pungenti rispetto a quelli interpersonali tra privati», tuttavia è anche vero che in questo caso il riferimento della Corte era esclusivamente rivolto al reato di diffamazione; al contrario, la possibilità che la diffusione di notizie false modifichi il consenso elettorale non può che assumere una connotazione diversa.

Già nel 1927 durante il quarto convegno dei costituzionalisti tedeschi, tenutosi a Monaco, Rudolf Smend aveva evidenziato che la libertà di espressione più che un diritto individuale, deve essere considerato un diritto funzionale alla democrazia, e in quanto tale, gli deve essere riconosciuto un valore istituzionale e sociale[363].

E ancora, l'art. 3 del Protocollo numero I della Convenzione Europea dei Diritti dell'Uomo garantisce il diritto alle elezioni libere, implicitamente richiamando l'obbligo degli Stati di assicurare che il processo democratico si svolga in maniera libera, nel rispetto del pluralismo[364].

Ne consegue che, in materia di informazione, e soprattutto nel delicato momento delle elezioni, vada indubbiamente salvaguardata la possibilità del cittadino di formare liberamente il proprio pensiero. A tal fine, risulta imprescindibile che tutti i mezzi di informazione svolgano un'attività ispirata alla completezza e all'imparzialità.

---

[360] SUFFIA, ZICCARDI, *Fake news guerra dell'informazione ed equilibri democratici,* cit., p. 212

[361] POLLICINO, *La prospettiva costituzionale sulla libertà di espressione nell'era di Internet*, in *Media Laws*, 1/2018 p. 79.

[362] Cass. civ., sez. III. 17 ottobre 2013, n. 23576.

[363] PALICI DI SUNI, *Fake news e referendum*, in *Federalismi.it*, n. 11/2020, p. 141.

[364] HARRIS, O'BOYLE,WARBRICK, *Law on the European Convention on Human Rights*, 4ª ed., Oxford, 2018, p. 910.

Nel caso contrario, lasciando che la falsità occupi l'intero ambiente del dibattito pubblico, si assisterebbe alla frustrazione dello scopo primario della stessa libertà di espressione[365].

4.1. Alcuni esempi di campagne di disinformazione nel corso di processi elettorali

Una volta inquadrata la problematica generale, appare opportuno concentrarsi sugli esempi maggiormente emblematici di campagne di disinformazione che hanno inciso significativamente sui processi elettorali, di conseguenza impattando la sovranità stessa degli Stati.

4.1.1. Le elezioni presidenziali americane del 2016: la *Internet Research Agency* (IRA)

La campagna di disinformazione portata avanti nel contesto delle elezioni presidenziali statunitensi del 2016 rappresenta il primo esempio di una *Disinformation Operation* di una portata tale da avere un'incidenza senza precedenti non solo sul risultato elettorale, ma anche sull'intero ambiente socio-politico degli Stati Uniti d'America.

Tali operazioni sono state poste in essere dall'Internet Research Agency, nota come IRA, ossia una *Troll Factory* che ha cominciato a operare nella metà del 2013 a San Pietroburgo, in Russia.

Con il termine *Troll Factory* si intende un'organizzazione creata con lo scopo precipuo di pubblicare un grande quantitativo di messaggi e altri contenuti su Internet, spesso tramite degli *account fake*, al fine di influenzare l'ambiente politico[366].

Il funzionamento di IRA è molto simile a quello di un'agenzia di *marketing*: l'Agenzia ha assunto e formato migliaia di persone al fine di impiegarle in

[365] PARLAMENTO EUROPEO, POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS, *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*, cit., p. 79.

[366] Cambridge Dictionary: Troll Factory, <<https://dictionary.cambridge.org/it/dizionario/inglese/troll-factory >>.

campagne di disinformazione, prima nei confronti dei cittadini russi e ucraini, e successivamente nei confronti degli elettori statunitensi[367].

L'ampiezza delle loro operazioni, così come il budget impiegato, sono stati senza precedenti: avvalendosi di un budget che supera i 25 milioni di dollari statunitensi, è stato stimato che abbiano raggiunto 126 milioni di persone su *Facebook*, più di 20 milioni di utenti su *Instagram*, circa 1,4 milioni su *Twitter* e che abbiano pubblicato migliaia di video su *YouTube*[368].

Dal Rapporto Muller, ufficialmente noto come *Report on the Investigation into Russian Interference in the 2016 Presidential Election*[369], e dall'investigazione portata avanti dallo *United States Senate Selected Committee on Intelligence (SSCI)*[370] emerge che per oltre cinque anni la Russia ha condotto una guerra di disinformazione contro i cittadini americani manipolando i *social media* al fine di influenzare la cultura e la politica americane[371], ponendo in essere quella che è stata definita una vera e propria "*information warfare against the United States of America"*[372].

Tale interferenza è stata caratterizzata da tre passaggi fondamentali: *l'hackeraggio on-line* del sistema di voto, un attacco cibernetico nei confronti del Comitato Democratico Nazionale e operazioni volte a influenzare direttamente la società e i cittadini.

Prima di passare ad analizzare l'ultima fase, oggetto del presente elaborato, appare opportuno approfondire l'operazione svolta nei confronti del Partito Democratico.

Si è trattato di una vera e propria operazione di intrusione nei *server* del Comitato Elettorale di Hilary Clinton, al fine di sottrarre dei documenti riservati per poi

---

[367] DI RESTA, SHAFFER, RUPPEL, SULLIVAN, MATNEY, FOX, ALBRIGHT, JOHNSON, *The Tactics and Tropes of the Internet Research Agency*, in *New Knowledge*, 2019, p. 6.

[368] *Ibidem.*

[369] SPECIAL COUNSEL ROBERT S. MUELLER, III, U.S. DEPARTMENT OF JUSTICE, *Report on The Investigation into Russian Interference in the 2016 Presidential Election*, Washington DC, 2019.

[370] SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE, SENATE, *Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, vol. 5, 116th congress, 1st session.

[371] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, 2017; PROKOP, ANDREW, *All of Robert Muller's Indictments and Plea Deals in The Russia Investigation So Far*, in *Vox*, 2018.

[372] THE UNITED STATES DEPARTMENT OF DEFENCE, OFFICE OF PUBLIC AFFAIRS, *Russian National Charged with Interfering in U.S. Political System*, 19 October 2018, << https://www.justice.gov/opa/pr/russian-national-charged-interfering-us-political-system >>.

diffonderli sulla rete[373]. La conseguenza di tale operazione intrusiva, e della successiva pubblicazione di messaggi di posta elettronica acquisiti in maniera illegittima per il tramite del sito *web Wikileaks*, è stata la diffusione capillare di una teoria complottista secondo cui dall'esame di alcune parole in codice usate nelle *e-mail* in questione, sarebbe emersa la dimostrazione dell'esistenza di un traffico di bambini riconducibile al partito Democratico. Al fine di dare maggiore credibilità a tale costruzione, è stato anche individuato un luogo fisico come base di questa attività, ossia la pizzeria di Washington *Comet Ping Pong*, posseduta da un uomo omosessuale, il quale aveva esplicitamente dichiarato la propria vicinanza al Partito Democratico.

Tale operazione ha avuto una risonanza tale, che nei mesi successivi sulle piattaforme *social* il termine "pizza" è divenuto sinonimo di "pedofilia"[374]. Ciò ha comportato non solo delle conseguenze disastrose per il Partito di Hilary Clinton nelle successive elezioni, ma la credibilità di questa storia è divenuta tale che il 4 dicembre 2016 un uomo armato ha fatto irruzione nella pizzeria sparando colpi di fucile, nell'erronea convinzione di portare avanti una spedizione di liberazione dei bambini ivi illegittimamente detenuti[375].

Passando ora alle operazioni di influenza diretta sulla società, queste furono condotte tramite diverse strategie coordinate di disinformazione rivolte ai cittadini statunitensi per il tramite di molti *social network*, tra cui si possono ricordare *Facebook, Instagram e Twitter*.

Come anticipato, nel 2018 la SSCI ha dato inizio a un'investigazione sull'attività svolta dall'IRA in questo riguardo, facendo anche uso dei dati relativi a tali operazioni fornitegli dalle piattaforme stesse.

Le campagne di disinformazione condotte dall'Internet Research Agency hanno utilizzato diverse metodologie, tra cui *trolls* russi, *account fake* sulle piattaforme *social*, *meme* e soprattutto *social bot*.

---

[373] SPECIAL COUNSEL ROBERT S. MUELLER, III, *Report on The Investigation Into Russian Interference In The 2016 Presidential Election*, 2019, p. 53.

[374] GUERINI, *Fake News e Diritto Penale, la manipolazione digitale del consenso nelle democrazie liberali*, cit., pp. 34-35.

[375] PUENTE, *il grande inganno di internet*, Milano, 2019, pp. 38-40

Partendo dai primi, i *trolls* russi e gli *account* finti sono stati utilizzati dall'IRA al fine di pubblicare commenti sulle nuove informazioni diffuse, con lo scopo strategico di mostrare disaccordo nel sistema politico statunitense[376].

Nello specifico, i *troll* possono essere definiti come membri di una comunità *on-line* il cui obiettivo è quello di creare disturbo, lanciare attacchi e offese, o più in generale di scardinare l'ordine interno di una data comunità, pubblicando commenti, foto e altri contenuti digitali. In aggiunta, i *troll* manipolano gli algoritmi di ricerca e portano avanti campagne di *spam* attraverso l'utilizzo di parole chiave e *link fake*[377].

Per quanto concerne i cosiddetti *meme* si tratta di immagini, icone, video o frasi facili da condividere *on-line* e da ricontestualizzare[378].

Per quel che riguarda i *social bot,* questi si sostanziano in programmi informatici in grado di agire come degli utenti umani, con lo scopo di attrarre l'attenzione degli utenti e della stampa, così andando a occupare lo spazio mediatico e a incrementare la polarizzazione[379].

L'utilizzo coordinato e integrato di queste metodologie ha portato a una crescente polarizzazione della popolazione statunitense durante e dopo le elezioni presidenziali del 2016, soprattutto grazie alle diverse strategie di *targeting* utilizzate dall'IRA.

Si tratta di strategie volte a suddividere la popolazione statunitense sulla base di diversi parametri, tra cui la collocazione geografica, il genere, l'età, la tipologia di impiego lavorativo, così da poter meglio indirizzare le campagne di disinformazione, chiudendo sempre di più gli elettori nelle loro camere d'eco[380].

---

[376] UNITED STATES DEPARTMENT OF JUSTICE, *Internet research agency indictment in the United States District Court for the District of Columbia*, 2018, p. 4.

[377] TUCKER, GUESS, BARBERÁ, VACCARI, SIEGEL, SANOVICH, STUKAL,NYHAN*Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature*, 2018, p. 30; BADER, *Disinformation in Elections,* in *Security and Human Rights*, 2018, p. 27.

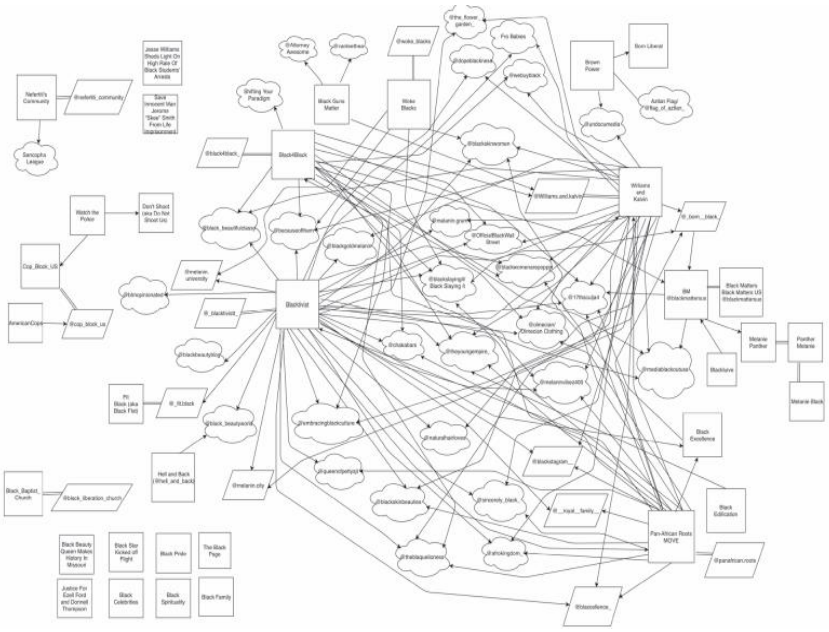
[378] DIRESTA, SHAFFER, RUPPEL, SULLIVAN, MATNEY, FOX, ALBRIGHT, JOHNSON, *The Tactics and Tropes of the Internet Research Agency*, cit., p. 50; HOWARD, WOOLLEY , CALO, *Algorithms, bots, and political communication in the US 2016 Election: the challenge of automated political communication for law and administration*, in *journal of information technology and politics*, n. 2, 2018, p. 85; WOOLLEY AND HOWARD, *computational propaganda worldwide: Executive Summary, computational propaganda research project,* working paper n. 2017.11, 2017, p. 3.

[379] MEZZANOTTE, *Fake news nelle campagne elettorali digitali. Vecchi rimedi o nuove regole?,* in *Federalismi.it,* 2018, p. 11.

[380] DIRESTA, SHAFFER, RUPPEL, SULLIVAN, MATNEY, FOX, ALBRIGHT, JOHNSON, *The Tactics and Tropes of the Internet Research Agency*, cit., pp. 34-36; SUSTEIN, *#republic. La Democrazia all'epoca dei social media*, Bologna, 2017, pp. 39 e ss; RAMAJOLI, *I pericoli del marketplace of idea. Considerazioni sparse a latere di due sentenze della Corte di Giustizia in tema di assegnazione delle frequenze radiotelevisive*, in *Media Laws,* n. 1/2018, p. 8.

Il risultato ultimo raggiunto dall'Internet Research Agency mediante l'insieme di queste strategie, metodologie e operazioni è stata la creazione di ciò che è stato definito come il *Media Mirage.*

Tale locuzione indica la rete mediatica che l'IRA è riuscita a creare mediante il coordinamento tra i diversi *account fake*, *social bot* e *troll* utilizzati sui vari *social network*, riproponendo la stessa storia o la stessa versione di un fatto sulle varie piattaforme, così da rinforzare i temi chiave e creare la percezione che determinati messaggi od opinioni fossero così diffusi da meritare attenzione e, soprattutto, credibilità[381].



Fonte: DIRESTA, SHAFFER, RUPPEL, SULLIVAN, MATNEY, FOX, ALBRIGHT, JOHNSON, *The Tactics and Tropes of the Internet Research Agency*, cit., p. 45

In conclusione, si può senza dubbio affermare che l'influenza che l'IRA ebbe sulle elezioni presidenziali americane del 2016 e sullo stesso sistema democratico è stata ed è tutt'oggi senza precedenti.

Tuttavia, volendo analizzare il potenziale risvolto positivo di tale fenomeno, bisogna dare atto che, in seguito, nel 2019 la Russia ha emanato due leggi *anti-fake news*, che hanno emendato la precedente normativa in materia di accuratezza

[381] DIRESTA, SHAFFER, RUPPEL, SULLIVAN, MATNEY, FOX, ALBRIGHT, JOHNSON, *The Tactics and Tropes of the Internet Research Agency*, cit., p. 62.

dell'informazione, prevedendo sanzioni amministrative pecuniarie per chi diffonde le notizie false[382].

4.1.2. Le elezioni presidenziali americane del 2020

Per quanto concerne le recenti elezioni presidenziali americane, la sussistenza di campagne di disinformazione è stata analizzata da un rapporto del *National Intelligence Council* statunitense pubblicato il 21 marzo 2021.

In un paragone con le elezioni presidenziali del 2016, è possibile notare uno sviluppo nella consapevolezza degli Stati Uniti d'America nei confronti del fenomeno qui in esame.

Ciò è dimostrato, anzitutto, dal fatto che il rapporto si apre evidenziando una differenza tra la nozione di *Elections Influence* e di *Election Interference*[383].

Per quanto concerne la prima, si fa riferimento a tentativi impliciti o espliciti di governi esteri o di attori non statali, che agiscono per conto di questi, volti ad impattare negativamente le elezioni americane in via diretta o mediata; inclusi l'influenza diretta verso i candidati, i partiti politici, gli elettori e le loro preferenze, o il processo politico stesso.

La *Election Interference,* invece, è una sottocategoria del primo concetto che comprende solo quelle azioni volte a influenzare gli aspetti tecnici del processo elettorale: la registrazione dei voti, il conto di questi, o il risultato finale.

Si tratta in sostanza di una distinzione simile a quella fatta in apertura del presente capitolo tra manipolazioni dirette dei risultati delle elezioni, e le cosiddette *Information Operations* o *Cyber Operations*.

Per quanto concerne la *Election Interference,* nella tornata elettorale del 2020 il rapporto della *Intelligence Community* statunitense afferma che non vi sono prove che vi sia stata alcuna interferenza tecnica, ad esempio sul conteggio dei voti[384].

Al contrario, vi sono elementi che dimostrano la presenza di operazioni di *Election Influence* da parte di governi quali la Russia o l'Iran. Questi hanno portato avanti campagne di disinformazione diffondendo *fake news*, ad esempio insinuando che il

[382] Legge Federale russa No. 31-FZ del 2019 e Legge Federale russa No. 27-FZ del 2019.
[383] NATIONAL INTELLIGENCE COUNCIL, *Foreign threats to the 2020 US Federal Elections*, 10 marzo 2021, pp. 1-3.
[384] *Ibidem*, pp. 2.

sistema di voto statunitense fosse compromesso, così minando la fiducia pubblica nella trasparenza delle elezioni e nella veridicità dei risultati di queste[385].

E ancora, nell'ottobre del 2019 su alcune tra le più importanti piattaforme *social*, tra cui *Twitter, Facebook e YouTube*, è stato pubblicato un video, noto come *30-second campaign*, in cui il partito Democratico di Joe Biden veniva ingiustamente accusato di aver ricattato alcuni ufficiali ucraini al fine di far cessare un'investigazione nei confronti di suo figlio[386]. Il video in questione è stato visto più di 1.5 milioni di volte, dopo essere stato ri-condiviso dall'ex Presidente degli Stati Uniti Donald Trump sul proprio profilo *Twitter*[387].

Per quanto concerne nello specifico l'interferenza Russa, il rapporto riporta che il Presidente russo Putin avrebbe autorizzato delle *Influence Operations* volte a minare la fiducia dell'elettorato americano nei confronti di Joe Biden e del partito Democratico, operazioni che poi nella pratica sarebbero state poste in essere da una serie di organizzazioni governative russe.

In aggiunta ai metodi utilizzati nel 2016 di cui si è detto, la *Intelligence Community* statunitense sottolinea che una delle strategie maggiormente utilizzate dalla Russia nell'ultima tornata elettorale americana consisterebbe nell'usare dei *proxies* connessi con l'Ucraina[388].

Il termine *proxy* letteralmente significa agire per conto di un'altra persona[389]; nel linguaggio tecnico-informatico il *proxy* è una tipologia di *server* che funge da intermediario per le richieste dei *client* che vengono effettuate su un altro *server*, disaccoppiando l'accesso al *web* dal *browser*[390].

Mediane questa tecnologia, la Russia è riuscita a diffondere rapidamente e in maniera efficace *fake news* non solo tra gli elettori, ma anche tra i *media* statunitensi.

---

[385] *Ibidem*, pp. 7 e ss.

386 STEWART, *Facebook is refusing to take down a Trump and making false claims about Joe Biden*, in *Vox*, 2019, << https://www.vox.com/policy-and-politics/ 2019/10/9/20906612/trump-campaign-ad-joe-biden-ukraine-facebook >>.

[387] KIELY, FARLEY, *Fact: Trump TV Ad Misleads on Biden and Ukraine*, in *FACTCHECK.ORG*, 2019, << https://www.factcheck.org/2019/10/fact-trump-tv-ad-misleadson-biden-and-ukraine/>>.

[388] NATIONAL INTELLIGENCE COUNCIL, *Foreign threats to the 2020 US Federal Elections*, cit., pp. 7-8.

[389] Cambridge Dictionary: proxy, <https://dictionary.cambridge.org/it/dizionario/inglese/proxy >>.

[390] PCMag, encyclopedia: proxy server << https://www.pcmag.com/encyclopedia/term/proxy-server >>.

Tuttavia, a differenza delle elezioni presidenziali americane del 2016, non sono stati registrati tentativi di attacchi informatici russi al fine di ottenere accesso alle infrastrutture elettorali.

Per quanto concerne l'interferenza dell'Iran, invece, il *report* rileva che la Guida Suprema del Paese Ali Khamenei ha dato autorizzazione all'*intelligence* iraniana di porre in essere una campagna di disinformazione al fine di scongiurare la rielezione di Trump; tuttavia, a differenza della Russia, non vi sono indicazioni che lascino pensare che l'Iran abbia parallelamente portato avanti attività volte ad esaltare la figura di Joe Biden. Tale campagna sarebbe stata volta a generare negli elettori americani sfiducia nel sistema elettorale nazionale, mettendo in luce, tramite notizie *fake*, fratture interne allo stesso[391].

E ancora, a differenza delle elezioni presidenziali americane del 2016, il rapporto evidenzia l'esistenza di tentativi di altri attori internazionali di influenzare l'ultima tornata elettorale americana, tra cui possiamo ricordare Cuba e il Venezuela. Ciò che accomuna questi ultimi soggetti, secondo il *National Intelligence Council* statunitense, è da un lato la dimensione più ridotta delle loro campagne di disinformazione, e dall'altro il fatto che più che da motivazioni politiche questi attori sarebbero stati spinti da ragioni finanziarie[392].

Volendo trarre delle conclusioni in paragone con le campagne di disinformazione delle elezioni presidenziali americane del 2016, in generale le *Disinformation Operations* poste in essere nell'ultima tornata elettorale degli Stati Uniti d'America hanno avuto dimensioni più ridotte e di conseguenza vi è stato un impatto minore sul processo democratico e sulla sovranità del Paese.

4.1.3. *Fake news* e *referendum*

4.1.3.1. Il *referendum* sulla *Brexit*

L'idea del *referendum* sull'uscita del Regno Unito dall'Unione Europea è sorta nel 2013 in occasione del discorso del premier Cameron all'agenzia di stampa Bloomberg. In quella circostanza, il Premier, in risposta all'insistenza deli

[391] NATIONAL INTELLIGENCE COUNCIL, *Foreign threats to the 2020 US Federal Elections*, cit., pp. 10.
[392] *Ibidem* p. 11.

euroscettici interni al proprio partito, si è impegnato, in caso di vittoria delle elezioni del 2015, a ridefinire il rapporto tra il Regno Unito ed Europa, ed a tenere un *referendum* sulla permanenza nell'Unione Europea entro il 2017[393].

Nonostante sia stato definito come il *referendum* con il maggior tasso di *fact-checking* della storia, secondo molti tra i motivi che hanno fatto prevalere la posizione del *leave* sono da annoverare le *fake news* e la disinformazione diffuse nel corso della campagna per la *Brexit.*

Con il termine *fact-checking* si fa riferimento a una forma di giornalismo, in cui vengono passate in rassegna le notizie e le affermazioni politiche, così da selezionare quelle verificabili, al fine di consentire agli elettori di prendere delle scelte libere e informate[394].

Come affermato da Bill Adair, fondatore di *PoliFact*, una delle prime società di *fack-checking*, lo scopo di tale attività non è quello di impedire ai politici di diffondere *fake news* o disinformazione, bensì piuttosto quello di fornire alle persone le informazioni necessarie per effettuare le proprie valutazioni in maniera consapevole[395].

Con specifico riferimento alla *Brexit*, le società incaricate del *fact-checking* hanno pubblicato dei resoconti delle proprie attività durante la campagna, dimostrando che il traffico *web* si è più che duplicato nel corso della notte seguente all'annuncio del *referendum*[396].

Nello specifico, secondo tali rapporti, il *referendum* sarebbe stato caratterizzato dall'utilizzo ingente di *Big Data* per il tramite di algoritmi di ultima generazione[397], in grado di trasmettere, tramite le piattaforme *social*, messaggi talmente personalizzati su ciascun elettore che la *targetizzazione* dei destinatari dei messaggi non avveniva più solo sulla base di categorie di utenti, ma ciascuna notizia era studiata in modo da essere il più efficace possibile per ogni singolo utente. Questo modello è noto come *dog-whistle politics*, in quanto la polarizzazione sfruttata e incentivata è tale che il "richiamo", ossia il messaggio diffuso, viene fatto giungere

---

393 CARAVALE, *La "faglia" della Brexit*, in *Nomos le attualità del diritto*, n. 2/2016, p. 2.
394 GROSS, RENWICK, *Fact-Checking and the EU referendum,* in *Constitution Unit*, 2016.
395 *Ibidem*.
396 BABAKAR, *The EU referendum, factchecked*, in *FullFact,* 2016, << https://fullfact.org/blog/2016/jun/eu-referendum-2016/ >>.
397 SHIPMAN, *All out war: the full story of Brexit*, London, 2017; GUERINI, *Fake News e diritto penale, la manipolazione digitale del consenso nelle democrazie liberali*, cit., p. 34.

esclusivamente ad alcuni soggetti, mentre per gli utenti fuori da quella *filter bubble* la notizia in questione rimane totalmente inesistente[398].

Secondo questa visione, la campagna di disinformazione della *Brexit*, che ha portato alla fuoriuscita del Regno Unito dall'Unione Europea, è stata impostata avvalendosi del supporto di un gruppo di studiosi e ricercatori, nonché della società canadese di *Big Data* AggregteIQ, fortemente connessa con Cambridge Analytica[399]. Il compito affidato a tale *team* sarebbe consistito nel raccogliere il maggior numero di dati e informazioni sugli elettori britannici sulla base dei comportamenti di questi sulle piattaforme *social*, in modo non dissimile da quanto effettuato dalla stessa Cambridge Analytica durante le elezioni di Donald Trump, così da poter effettuare la *targetizzazione* sopra descritta dei messaggi a questi rivolti, chiudendoli sempre più in delle camere d'eco.

E ancora, secondo alcuni, le campagne di disinformazione della Russia sarebbero state destinate anche agli elettori britannici, con lo scopo di far prevalere la posizione del *leave.* A tal riguardo, il *Parlamentary Selected Committee for Culture, Media and Sport* del Regno Unito nel proprio rapporto sulle campagne di disinformazione durante la *Brexit* ha affermato di essere in possesso di prove riguardanti i tentativi della Russia di manipolare le risultanze referendarie[400].

A differenza delle elezioni Presidenziali americane del 2016, tuttavia, nel caso del *referendum* britannico i principali *social network* hanno negato la presenza di qualsiasi attività significativa proveniente dalla Russia sulla propria piattaforma. A dimostrazione del contrario, però, ad esempio, alcuni ricercatori hanno evidenziato la presenza di 150.000 account su *Twitter* aventi il russo tra le lingue predefinite e che, negli ultimi giorni della campagna referendaria, hanno postato tutti assieme più di 45.000 *tweets* sulla *Brexit*, principalmente supportando il lato del *leave*[401].

A corroborare ulteriormente la sussistenza di un'influenza russa nella campagna di disinformazione della *Brexit*, colui che è stato identificato come il *whistleblower* dello scandalo di Cambridge Analytica ha affermato che quest'ultima avrebbe

---

[398] GUERINI, *Fake News e diritto penale, la manipolazione digitale del consenso nelle democrazie liberali*, cit., p. 35.

[399] DA EMPOLI, *Gli ingegneri del caos. Teoria e Tecnica dell'internazionale populista*, Venezia, 2019, p. 38.

[400] HOUSE OF COMMONS CULTURE, MEDIA AND SPORT SELECTED COMMITTEE, *Disinformation and fake news: interim report*, 2018, paragrafo 2.

[401] GORODNICHENKO, YURIY, THO PHAM, AND OLAKSANDER TALAVERA, *Social media, sentiment and public opinions: evidence from #Brexit and #USElection*, Working Paper 24631, Cambridge, MA: National Bureau of Economic Research, maggio 2018.

fornito i dati raccolti a compagnie russe, fortemente legate con l'*intelligence* russa[402].

In conclusione, a prescindere dagli autori formali della campagna di disinformazione durante il *referendum* della *Brexit,* i sospetti di interferenze straniere hanno sollevato grande preoccupazione nella comunità internazionale circa il funzionamento del processo democratico stesso, e finanche sulla legittimità del *referendum*.

4.1.3.2. Il *referendum* costituzionale del 2016 sulla riforma Renzi-Boschi

Le campagne di disinformazione hanno attraversato anche il panorama italiano nel corso della campagna referendaria del 2016.

Informazioni circa la diffusione di *fake news* rivolte a influenzare il risultato del *referendum* costituzionale sono state divulgate inizialmente da un'inchiesta svolta dal sito *web Buzzfeed,* che he evidenziato i legami tra alcuni siti ritenuti poco affidabili e il partito del Movimento 5 Stelle[403].

Nello specifico, il rapporto di *Buzzfeed* rileva che il partito del Movimento 5 Stelle avrebbe creato una rete capillare di siti, *account* finti sui *social network* e siti *web* che si auto-proclamano indipendenti ma che in realtà farebbero capo al partito in questione, al fine di diffondere *fake news*, teorie cospiratorie e, più in generale, di portare avanti una pregnante campagna di disinformazione[404].

A seguito del *referendum*, il rapporto collettivo di *fact-checking* di Pagella Politica[405], ossia l'unico sito *web* italiano dedicato interamente all'attività di *fact-checking,* ha confermato un panorama simile, per quanto di dimensioni più ridotte, rispetto a quello profilatosi nel 2016 durante le elezioni presidenziali statunitensi[406].

---

[402] *Whistleblower: Cambridge Analytica shared data with Russia*, Euractive.com, 2018; PARLAMENTO EUROPEO, POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS, *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*, cit., p. 42.

[403] NARDELLI, SILVERMAN, *Movimento Cinque Stelle Primo In Europa A Diffondere Notizie False E Propaganda Russa*, in *buzzfeddnews.com,* 2016, <<https://www.buzzfeednews.com/article/albertonardelli/movimento-cinque-stelle-primo-in-europa-a-diffondere-notizie >>.

[404] *Ibidem.*

[405] *La notizia più condivisa sul referendum? È una bufala*, in *Pagella Politica,* 2016, <<https://pagellapolitica.it/blog/show/148/la-notizia-pi%C3%B9-condivisa-sul-referendum-%C3%A8-una-bufala >>.

[406] *2016, l'anno della post-verità e del boom delle false notizie*, in *Sky TG24,* 2016, <<https://tg24.sky.it/mondo/2016/12/28/2016-anno-fake-news-post-truth >>.

A titolo esemplificativo, la notizia più diffusa nel corso del *referendum*, il cui *link* nei mesi precedenti alla votazione ha ottenuto 23 mila reazioni, altro non era che una *fake news*. Si tratta del presunto ritrovamento di 500.000 schede elettorali con la casella del "si" già sbarrata, nel paese, per altro inesistente, di Rignano sul Membro[407].

Tale scenario ha suscitato la reazione di diversi esponenti politici, tra cui l'allora Presidente della Camera dei Deputati Laura Boldrini la quale ha manifestato la necessità di prendere provvedimenti contro la disinformazione e le *fake news*; nonché l'ex Premier Matteo Renzi il quale ha affermato che il *web* è stato lasciato a «chi diffonde falsità»[408].

E ancora, in un'intervista con Il Foglio, l'ex Ministro di Giustizia Andrea Orlando ha parlato di responsabilità della piattaforma *social Facebook*, facendo riferimento alla necessità di adottare provvedimenti a livello europeo[409].

In conclusione è necessario sottolineare che, nonostante la diffusione di campagne di informazione abbia raggiunto anche la sfera politica italiana, come emerge da uno studio condotto nel 2018 sulla base dei dati raccolti nei due anni precedenti, i siti *web* che effettuano campagne di disinformazione in Italia hanno un'incidenza pressoché insignificante in confronto ai *media* tradizionali, tanto in termini di ampiezza della diffusione, quanto in termini di utenza[410].

---

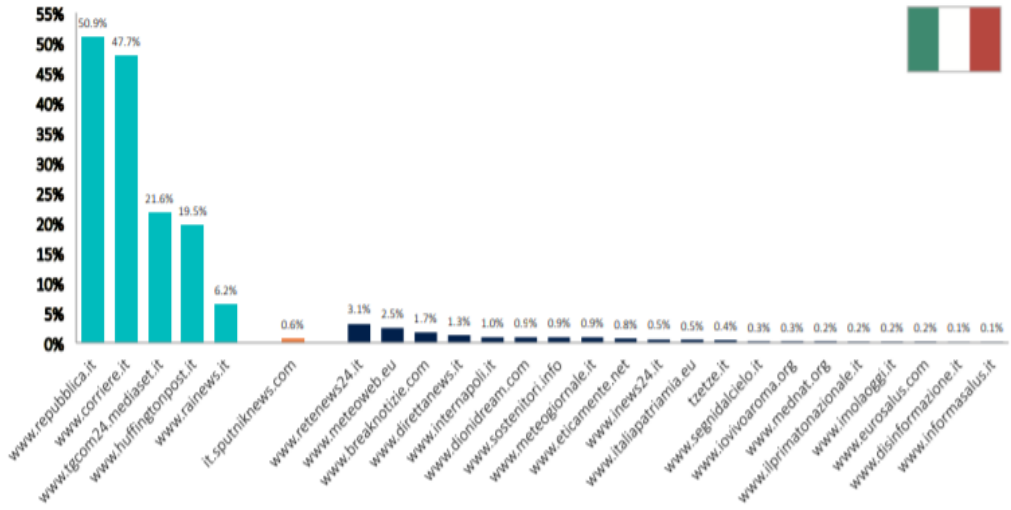
[407] Pagella Politica per AGI, *Referendum e fact checking: la notizia più condivisa è una bufala*, in *AGI*, 2016, <<https://www.agi.it/politica/referendum/referendum_e_fact_checking_la_notizia_pi_condivisa_una_bufala-1289280/news/2016-12-02/ >>.

[408] BRUNO, 2016, *L'anno della post-verità e del boom delle false notizie*, in *Sky TG24*, 2016, <<https://tg24.sky.it/mondo/2016/12/28/2016-anno-fake-news-post-truth >>.

[409] *Facebook e democrazia, il dibattito dopo le parole di Orlando al Foglio*, in *Il Foglio*, 2016, <<https://www.ilfoglio.it/politica/2016/12/28/news/facebook-democrazia-orlando-foglio-dibattito-censura-bufale-112766/ >>.

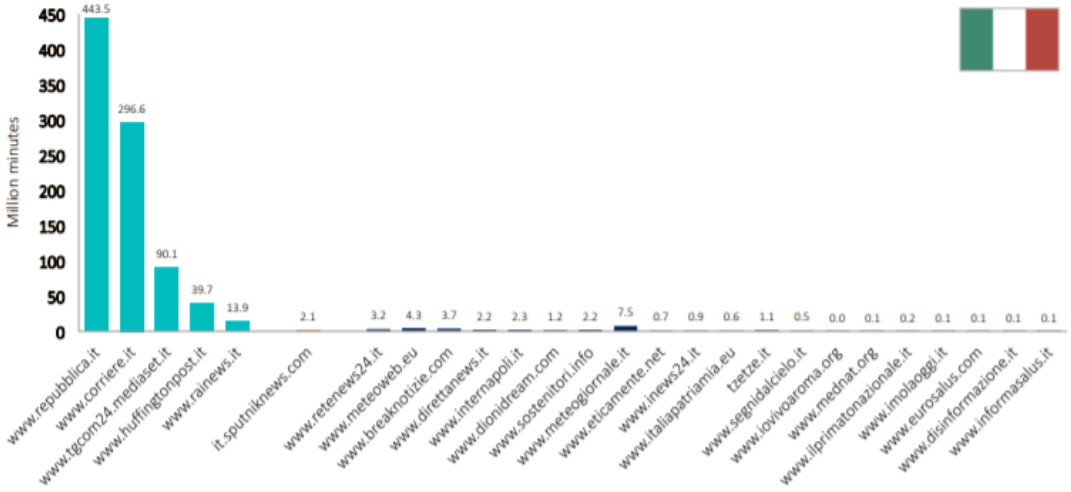
[410] FLETCHER, CORNIA, GRAVES, NIELSEN, *Measuring the Reach of "Fake News" and Online Disinformation in Europe*, in *Reuters Institute for the Study of Journalism, University of Oxford*, 2018, pp. 5-7.

Media mensile di visite ai siti dei principali media italiani, e alcuni dei più famosi siti di *fake news*



Fonte: FLETCHER, CORNIA, GRAVES, NIELSEN, *Measuring the Reach of "Fake News" and Online Disinformation in Europe*, cit., p. 5.

Media mensile del tempo speso dagli Italiani sui siti dei principali media e su alcuni dei più famosi siti di *fake news*



Fonte: FLETCHER, CORNIA, GRAVES, NIELSEN, *Measuring the Reach of "Fake News" and Online Disinformation in Europe*, cit., p. 6.

4.2. Cornice regolatoria e potenziali violazioni

Una volta analizzato l'impatto che tali campagne di disinformazione hanno sulle elezioni, sul sistema delle democrazie liberali e, in ultima istanza, sulla sovranità degli Stati, appare opportuno analizzare l'attuale panorama normativo nazionale e internazionale.

Per quanto concerne il sistema giuridico italiano, oltre ad integrare i reati esaminati in precedenza[411], la tutela della lotta alla diffusione di *fake news* specificamente nell'ambito di campagne di disinformazione nel corso delle elezioni appare come diretta filtrazione del combinato disposto tra l'articolo 1 e l'art. 49 della Costituzione, da cui rispettivamente si ricavano l'obbligo di esposizione corretta dell'informazione elettorale e il concorso dei cittadini nella determinazione della politica nazionale[412]. A ciò potrebbe aggiungersi la tutela fornita legge numero 28 del 2000, recante le disposizioni per la parità di accesso ai mezzi di informazione durante le campagne elettorali e referendarie e per la comunicazione politica, tuttavia tale normativa trova applicazione solo in riferimento alla radiotelevisione e alla carta stampata, non essendo consentita l'applicazione analogica alle campagne effettuate su Internet.

Ne consegue che nessuna delle disposizioni in esame proibisce esplicitamente operazioni di disinformazioni rivolte a manipolare le elezioni e il processo democratico.

Per quanto concerne la cornice del diritto internazionale, nel dicembre del 2016 il Presidente Barak Obama ha dichiarato che l'influenza russa ha violato norme internazionali di comportamento ormai consolidate[413]; tuttavia, anche in questo caso, allo stato attuale non possono essere rinvenute norme di diritto internazionale pubblico o penale che incrimino o considerino esplicitamente illegittime le cosiddette *Disinformation Operations.*

Tuttavia, se è vero che costituisce ormai principio consolidato del diritto internazionale l'assunto secondo cui tutto ciò che non è proibito da questo è

---

411 V. *supra* Cap. II.

412 MEZZANOTTE, *Fake news nelle campagne elettorali digitali. Vecchi rimedi o nuove regole?*, cit., pp. 7-8; VIGEVANI, Sub *art 49*, in BARTOLE, BIN (a cura di), *Commentario Breve della Costituzione*, Padova, 2008, p. 500.

413 Press Release, White House, *Statement by the president on Actions in Response to Russian Malicious Cyber Activity and Harassment*, 29 dicembre 2016, <<https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity >>.

permesso[414], d'altra parte, ciò non implica che le campagne di disinformazione condotte nel corso delle elezioni con lo scopo di frustrare l'apparato democratico di un altro Stato non possano violare principi generali di diritto internazionale.

Costituisce ormai, infatti, opinione cristallizzata l'dea secondo cui la manipolazione del discorso pubblico attraverso le *Cyber Operations* sulle piattaforme *social* rappresenta uno dei più grandi pericoli per la comunità internazionale nel *cyberspazio*; un luogo virtuale non regolato da trattati e convenzioni e in cui la formazione di norme consuetudinarie è ancora in *itinere*[415].

Ciò è stato messo in luce dal mancato successo eai lavori dello United Nations *Group of Governamental Experts of Developments in the Field of Information and Telecommunications in the Context of International Security* (UNGGE) al quale era stato dato incarico dall'Assemblea Generale delle Nazioni Unite di determinare come possa essere applicato il diritto internazionale all'uso da parte degli Stati delle cosiddette *Information and Communication Technologies,* al fine di elaborare norme e principi di comportamento responsabile applicabili alla materia in esame[416].

Infatti, nonostante il gruppo di esperti avesse in un primo momento concordato sul fatto che le *Information and Communication Technologies* siano e debbano essere regolate dal diritto internazionale, e che, nello specifico, gli Stati debbano rispettare principi generali della Carta delle Nazioni Unite, quali la Sovranità statale e la non ingerenza negli affari interni degli altri Stati[417], nel 2017 il mancato accordo dei membri dell'UNGGE su aspetti quali la possibilità per gli Stati oggetto di attacco informatico di porre in essere contromisure, ha portato al fallimento dell'obiettivo del gruppo.

Ad oggi, esistono per lo meno due principi generali di diritto internazionale che in astratto potrebbero trovare applicazione in occasione di campagne di disinformazione nel contesto elettorale.

---

[414] PCIJ, SS Lotus case (France v Turkey), series A n. 10, 1927, para 18; ICJ, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America), 1986, para 269; ICJ, Advisory Opinion on the Threat or Use of Nuclear Weapons, 1966, para 21.

[415] PRIER, *Commanding the Trend: Social Media as Information Warfare*, in *Strategic Studies Quarterly*, 2017, p. 57; VAN DE VELDE, *The law of cyber interference in elections, cit.*, p. 38.

[416] Risoluzione dell'Assemblea Generale 70/237, adottata il 23 dicembre 2015, paragrafo 5, UN Doc. A/RES/70/237.

[417] General Assembly, *Group of Governamental Experts of Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/70/174, 22luglio 2015, paragrafo 28.

Il primo dei principi che appare opportuno prende in considerazione è quello della sovranità statale[418]. Quest'ultimo è stato definito come indipendenza degli Stati, che si sostanzia nel diritto di esercitare nel proprio territorio le funzioni proprie dello Stato, con l'esclusione di altri Stati[419]. Dunque, tale principio comprende due elementi fondamentali: la territorialità e le funzioni dello Stato.

Per quanto riguarda il primo, è ormai opinione consolidata in dottrina che la sovranità territoriale degli Stati si estenda anche al cyberspazio, con la conseguenza, che, anche l'intrusione non consensuale di uno Stato nel cyberspazio di un altro, ovvero la presenza non autorizzata in questo, integra una violazione del principio della sovranità territoriale[420].

Tuttavia, al fine di integrare la violazione in esame non è sufficiente una qualsiasi intrusione; bensì è necessario che anche il secondo elemento fondamentale, vale a dire quello che fa riferimento delle funzioni dello Stato, sia presente. In altre parole, si richiede che l'operazione posta in essere interferisca con le funzioni intrinsecamente governative dello Stato passivo, con la conseguenza di rendere le infrastrutture fisiche o informatiche di questo incapaci di svolgere le proprie funzioni ordinarie[421]; al contrario non si richiede che si verifichi un danno materiale. D'altronde, secondo quanto affermato dalla Corte Internazionale di Giustizia, il principio di sovranità comprende l'autorità dello Stato di prendere in maniera indipendente decisioni sull'ordine politico, sociale, culturale ed economico dello Stato stesso[422].

Tuttavia, con specifico riferimento alle campagne di disinformazione *on-line* è opportuno sottolineare che il mero trasferimento di propaganda nel territorio di un altro Stato generalmente non è sufficiente a integrare una violazione del principio di sovranità[423].

---

[418] BONFANTI, *Attacchi cibernetici in tempo di pace: le intrusioni nelle elezioni presidenziali statunitensi del 2016 alla luce del diritto internazionale*, in *Rivista di diritto internazionale*, 3/2019, pp. 700 e ss; SCHMITT, VIHUL, *Sovereignty in Cyberspace: Lex Lata vel Non?*, in *American Journal of International Law*, 2017, p. 213 e ss.

[419] PCA, Islands of Palmas arbitration case (Netherlands v United States of America), 1928, paras 829, 838.

[420] SCHMITT, *Virtual disenfranchisement: cyber election meddling in the grey zone of international law*, in *Chicago journal of international law*, n. 1, 2018, p. 43; WATTS, RICHARD, *Baseline territorial sovereignty and cyberspace*, in *Lewis and Clark Law Review*, n. 3, 2018, p. 818.

[421] *Tallinn Manual on International Law applicable to cyber warfare*, II edizione, Cambridge University Press, 2017, p. 21.

[422] ICJ, *Military and Paramilitary Activities in and against Nicaragua*, cit., para 263.

[423] *Tallinn Manual on International Law applicable to cyber warfare*, cit., p. 26.

Da ciò deriva la principale problematica relativa alla possibilità di considerare campagne di disinformazione, come quella condotta dall'IRA nel corso delle elezioni presidenziali statunitensi del 2016, in violazione del principio in esame. Infatti, prendendo proprio ad esempio le operazioni dell'IRA, questa pur avendo utilizzato infrastrutture informatiche nel territorio degli Stati Uniti d'America al fine di condurre alcune delle proprie strategie, tuttavia non ha causato i danni o la perdita di funzionalità richiesti per integrare la violazione del principio di Sovranità[424]. In altre parole, l'Internet Research Agency si è mossa in una zona grigia del principio in esame.

A ciò si aggiunge l'esistenza di una corrente di pensiero, se pur minoritaria, secondo cui la legge e la prassi degli Stati dimostrerebbe che il principio della Sovranità degli Stati abbia la funzione di guidare i comportamenti degli Stati nelle relazioni internazionali, ma che non abbia di per sé un'efficacia vincolante[425].

Ne consegue che, adottando tale filone dottrinale, il compimento di attacchi cibernetici, pur integrando gli estremi di una condotta non responsabile degli Stati, non potrebbe essere considerata vietata dal diritto internazionale alla luce del principio della Sovranità statale[426].

Il secondo principio generale di diritto internazionale che in astratto potrebbe essere violato dalle campagne di disinformazione è il principio di natura consuetudinaria di non intervento[427].

Anche questo principio consta di due requisiti fondamentali: l'interferenza nel *Domaine Réservé* dello Stato passivo e la coercizione.

Per quanto riguarda il primo, un'operazione per essere considerata in violazione del principio di non intervento deve interferire con gli affari interni o esteri dello Stato

---

[424] RODRIGUEZ, *Disinformation Operations aimed at (Democratic) Elections in the context of public international law: the conduct of the internet research agency during the 2016 US Presidential Election*, cit., p. 164.

[425] CORN, TAYLOR, *Sovereignty in the Age of Cyberspace*, in *American Journal of International Law*, 2017, p. 208.

[426] SCHMITT, *In defense of Sovereignty in Cyberspace*, 2018, <<https://www.justsecure.org/55876/defense/>>.

[427] ICJ, *Armed Activities in the Territory of Congo*, 2005, paras 161-165; ICJ, Military and Paramilitary Activities in and against Nicaragua, cit., para 202; *Tallinn manual on International Law applicable to cyber warfare*, cit., p. 312.

passivo[428]. E ancora, è necessario che lo scopo precipuo dell'operazione sia minare l'autorità dello Stato nel proprio *Domaine Réservé* [429].

Con la locuzione *Domaine Réservé* nell'ambito del diritto internazionale si fa riferimento all'area degli affari interni dello Stato, che dunque rientrano nella giurisdizione e nella competenza di questo[430].

E ancora, al fine di integrare una violazione del principio di non intervento, a ciò si aggiunge la necessità che le operazioni di disinformazione da parte di uno Stato estero abbiano natura coercitiva. La natura stessa della coercizione richiede che le azioni di disinformazione debbano possedere la potenziale capacità di indurre lo Stato passivo a porre in essere o a non porre in essere azioni che avrebbe voluto intraprendere o da cui si sarebbe astenuto[431].

È inoltre opportuno sottolineare che, con riferimento al cyberspazio, si ritiene che anche un effetto coercitivo indiretto sia sufficiente a integrare la violazione in esame[432].

Nello specifico caso delle elezioni, ciò può sostanziarsi ad esempio nell'elezione di un candidato diverso da colui che altrimenti avrebbe ottenuto la vittoria.

A prima vista si potrebbe ritenere che l'attività dell'IRA nel corso delle elezioni presidenziali americane del 2016 abbia integrato gli estremi di una violazione del principio di non intervento, dal momento che per molti aspetti le operazioni dell'Agenzia si sono sostanziate in una forma di intervento politico con lo scopo di manipolare il processo democratico interno degli Stati Uniti, che è parte integrante del *Domaine Réservé* dello Stato. Tuttavia, si configura come più complessa la possibilità di qualificare come coercitive le singole azioni di tale Agenzia. Per altro, appare opportuno sottolineare che alcuni autori ritengono che la natura non dittatoriale e riservata delle *Disinformation Operations* renda difficile la traslazione della nozione di coercizione al cyberspazio[433].

---

[428] SCHMITT, *virtual disenfranchisement: cyber election meddling in the grey zone of international law*, cit., p. 49.

[429] RODRIGUEZ, *Disinformation Operations aimed at (Democratic) Elections in the context of pubic international law: the conduct of the internet research agency during the 2016 US Presidential Election*, cit., p. 167.

[430] ZIEGLER, *Domaine Réservé*, in *Oxford Public International Law*, 2013, p. 1.

[431] SCHMITT, *virtual disenfranchisement: cyber election meddling in the grey zone of international law*, cit., p. 52.

[432] *Tallinn manual on International Law applicable to cyber warfare*, cit., p. 320.

[433] KILOVATY, *Doxfare: politically motivated leakes and the future of the norm on non-intervention in the era of weaponized information*, in *Harvard National Security journal*, 2018, p. 172.

Oltre ai principi generali summenzionati, le campagne di disinformazione nel corso delle elezioni possono comportare la violazione di diritti umani quali il diritto dei popoli all'autodeterminazione e il diritto di ogni individuo a prendere parte alla vita pubblica, rispettivamente previsti dagli articoli 1 e 25 dell'ICCPR.

Infatti, tra le previsioni contenute nella prima disposizione rientra il diritto di ciascun individuo a determinare liberamente il proprio *status* politico; per quanto concerne la seconda norma, invece, gli individui devono poter esprimere il proprio diritto di voto senza influenze illegittime o coercizioni tali da comportare una distorsione della libera espressione delle loro preferenze elettorali[434].

Tuttavia, prendendo ad esempio ancora una volta l'attività dell'IRA, la responsabilità della Russia per la violazione dei diritti umani in esame potrebbe essere accertata solamente se si accettasse che gli attacchi cibernetici possiedono i requisiti necessari al fine di consentire l'applicazione extraterritoriale dell'ICCPR[435], ossia il controllo effettivo sul territorio e il controllo personale.

A tal riguardo, nel recente *General Comment* n. 36, lo *Human Rights Committe* ha aggiunto un ulteriore requisito per l'applicabilità extraterritoriale dello *International Covenant on Civil and Political Rights,* ossia il criterio dell'impatto[436].

Infine, parte della dottrina ritiene che nel contesto dell'interferenza Russa nelle elezioni presidenziali americane del 2016, l'Agenzia potrebbe essere ritenuta responsabile anche per il non aver adottato misure positive di prevenzione e repressione. Infatti, come affermato dall'ICJ nel *Corfù Channel case*, infatti, «*it is every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States*»[437].

In altre parole, si tratta dello stesso dovere di *due diligence* previsto dalla *rule* 6 del Tallinn Manual, ai sensi della quale «*[a] State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governamental*

---

[434] HUMAN RIGHTS COMMITTEE, *General Comment n. 25. The right to participate in public affairs, voting rights, and the right to equal access to public service (Art. 25),* UN Doc. CCPR/C/21/Rev.1/Add.7, 12 luglio 1996, para 19.

[435] CARREA, *the ECHR in Cyberspace: does the power to infringe always entail the duty to protect*?, in *Diritti Umani e Diritto Internazionale,* 2019, p. 133.

[436] HUMAN RIGHTS COMMITTEE, *General Comment n. 36 (2018) on Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life,* UN Doc. CCPR/C/GC/36, 30 ottobre 2018, para 63.

[437] Corte Internazionale di Giustizia, *Corfu Channel Case,* (United Kingdom of Great Britain and Northern Ireland v Albania, 1949, p. 22.

control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States».

A tal riguardo, appare opportuno preliminarmente sottolineare che lo Stato titolare degli obblighi di controllo e prevenzione oggetto del dovere di *due diligence* deve essere identificato sulla base del criterio della provenienza. Ne consegue, che lo Stato in capo al quale sorge tale onere, al fine di non incorrere in responsabilità internazionale, deve porre in essere tutte le misure necessarie e idonee affinché il proprio territorio non venga utilizzato per condotte lesive di diritti di altri Stati, prevenendo, quindi, un eventuale attacco informatico di cui ha conoscenza, o di cui avrebbe ragionevolmente dovuto avere conoscenza[438].

Tuttavia, poiché il principio della *due diligence* prevede un obbligo di condotta e non di risultato, lo Stato non può incorrere in responsabilità internazionale se nonostante l'adozione di misure discrezionali ma ragionevoli, non raggiunga lo scopo di prevenire l'attacco o l'intrusione[439].

Oltre alle problematiche evidenziate per quanto concerne l'applicazione delle norme e dei principi generali di diritto internazionale summenzionati, è, inoltre, importante ricordare che tutte le violazioni sopra esaminate possono essere commesse solo da parte di uno Stato in via diretta, conducendo delle *Cyber o Information Operations*, oppure indirettamente, attraverso autori non-statali le cui operazioni siano riconducibili allo Stato in questione[440].

Per quanto concerne la seconda ipotesi, ai sensi dell'art. 8 degli *Articles on the Responsibility of States for International Wrongful Acts*[441], la condotta di una persona o di un gruppo di individui può essere considerata un atto di uno Stato ai sensi del diritto internazionale, solo se quella persona o quel gruppo agisce sulla base di istruzioni impartite dallo Stato o sotto la direzione o il controllo di questo. Dunque, in questi casi il soggetto non statale deve agire per conto dello Stato "mandante", incarnandosi in una sorta di strumento utilizzato dallo Stato per raggiungere il proprio fine di interferire con il processo democratico di un altro

---

[438] HERDEGEN, *Possibile legal framework and regulatory models for enhanced inter-State cooperation*, in *German Yeerbook of International Law*, 2015, p. 169.

[439] BONFANTI, *Attacchi cibernetici in tempo di pace: le intrusioni nelle elezioni presidenziali statunitensi del 2016 alla luce del diritto internazionale*, cit., p. 720.

[440] SCHMITT, *Virtual disenfranchisement: cyber election meddling in the grey zone of international law*, cit., p. 43.

[441] INTERNATIONAL LAW COMMISSION, *Articles on Responsibility of States for Internationally Wrongful Acts*, 2001, art. 8.

Stato; al contrario, la motivazione che spinge l'autore non statale risulta irrilevante ai fini dell'integrazione della violazione[442].

Con specifico riferimento alle campagne di disinformazione *on-line* si parla di necessità di un "*effective control"* da parte dello Stato mandante. In altre parole, quest'ultimo deve avere la capacità tanto di dare inizio alle *Cyber* o *Information Operations* quanto di farle cessare[443].

Prendendo ancora una volta ad esempio l'attività svolta dall'IRA, l'*intelligence* statunitense ha concluso che le operazioni che hanno influenzato la campagna presidenziale nel 2016 erano state ordinate dal Presidente della Federazione Russa Vladimir Putin stesso[444]. Inoltre, è stato anche affermato che la Russia possedeva l'*effective control* necessario sulle operazioni dell'Agenzia, avendo il potere di ordinarne la cessazione. Tuttavia, tale affermazione risulta difficile da sostanziare da un punto di vista giuridico, dal momento che condurre il *test* dell'*effective control* implicherebbe risposte a domande specifiche quali se il governo russo forniva istruzioni e indicazioni per ogni singola operazione o meno[445].

Infine, appare opportuno analizzare le contromisure che possono essere poste in essere dagli Stati oggetto dell'attacco cibernetico.

Con il termine contromisure si fa riferimento a condotte, di per sé illecite, che, tuttavia, trovano una giustificazione nel fatto che vengono poste in essere dallo Stato passivo nei confronti del soggetto statale che si trova in violazione di un obbligo internazionale, al fine di indurre quest'ultimo ad adempiervi[446].

Ne consegue che, secondo quanto previsto dagli articoli 49 e seguenti degli *Articles on the Responsibility of States for Internationally Wrongful Acts*[447], le contromisure devono essere proporzionate alla finalità di far cessare il comportamento illecito, possono essere mantenute in essere per tutta la durata della violazione[448], devono a

---

[442] PAYNE, *Teaching old law news tricks: applying and adapting State responsibility to cyber operations*, in *Lewis and Clark law review*, n. 2, 2016, p. 705.
[443] *Tallinn manual on International Law applicable to cyber warfare*, cit., p. 96.
[444] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI), *assessing russian activities and intentions in recent US elections*, ICA 2017.01D, 6 gennaio 2017.
[445] SHACKELFORD, ANDERS, *State responsibility for cyberattacks: competing standards for a growing problem*, in *Georgetown journal of international law*, 2011, pp. 987-988.
[446] BONFANTI, *Attacchi cibernetici in tempo di pace: le intrusioni nelle elezioni presidenziali statunitensi del 2016 alla luce del diritto internazionale*, cit., p. 772
[447] INTERNATIONAL LAW COMMISSION, *Articles on Responsibility of States for Internationally Wrongful Acts*, cit., art. 49.
[448] INTERNATIONAL LAW COMMISSION, *Articles on Responsibility of States for Internationally Wrongful Acts*, cit., art. 49 para 2.

loro volta essere sospese alla cessazione di questa[449] e devono essere reversibili, ossia una volta raggiunto l'obiettivo di porre fine all'illecito, devono permettere l'adempimento degli obblighi[450].

Inoltre, poiché le contromisure possono essere poste in essere solamente nei confronti di uno Stato, risulta necessario distinguere a seconda che sia possibile provare l'attribuzione della responsabilità in capo a un soggetto statale o meno.

Nella prima ipotesi, le contromisure saranno poste in essere nei confronti dello Stato in questione.

Nella seconda ipotesi, generalmente più diffusa nella prassi delle *Disinformation Operations* nel corso delle elezioni, invece, le *countermeasures* potranno comunque essere adottate nei confronti dello Stato nel cui territorio si trovano le infrastrutture utilizzate per sferrare gli attacchi informatici; in quest'ultimo caso, tuttavia, l'illecito contro cui reagisce lo Stato passivo non sarà l'attacco informatico stesso, bensì l'inadempimento degli obblighi di prevenzione e controllo derivanti dal dovere di *due diligence*. Di conseguenza, la valutazione della proporzionalità delle contromisure dovrà tenere conto anche delle eventuali misure di prevenzione adottate dallo Stato responsabile[451].

Prendendo ancora una volta ad esempio la propaganda di disinformazione che ha caratterizzato le elezioni presidenziali americane del 2016, tra le contromisure poste in essere dagli Stati Uniti nei confronti dell'IRA possiamo ricordare l'introduzione di misure di congelamento dei beni, sulla base del *Countering America's Adversaries Through Sanctions Act*[452] .

Tuttavia, per quanto riguarda le misure in esame, queste, pur essendo generalmente ammesse quali legittime *countermeasures*, pongono diverse problematiche circa il rispetto del principio di proporzionalità. Infatti, queste di norma vanno a colpire «tutti i beni assoggettabili all'esercizio della […] giurisdizione, senza […] preoccuparsi se il valore di tali beni, di solito sconosciuto al momento dell'adozione della contromisura, [sia] o meno eccessivo»[453].

---

[449] *Ibidem,* Art. 53.
[450] *Ibidem,* Art. 49 para 3.
[451] *Tallinn manual on International Law applicable to cyber warfare*, cit., p. 130; CHIRCOP, *A due diligence Standard of Attribution in Cyberspace*, in *cambridge.org*, 2018, p. 653.
[452] U.S. DEPARTMENT OF THE TREASURY, *Treasury Sanctions Russian Cybr Actors for Interference with the2016 U.S. Elections and Malicious Cyber- attacks*, 15 marzo 2018.
[453] FOCARELLI, *Le contromisure nel diritto internazionale,* Milano, 1994, pp. 15 e ss.

Nonostante nel caso di specie degli Stati Uniti parte della dottrina ritenga le misure di congelamento proporzionate in ragione del fatto che erano mirate a soggetti la cui partecipazione alla campagna di disinformazione era ormai comprovata[454], dall'analisi del quadro complessivo dei principi e delle norme di diritto internazionale applicabili ad attacchi informatici, continua ad emergere la necessità di adottare soluzioni regolatorie chiare ed armoniche.

4.3.Possibili soluzioni regolatorie

Lasciando al quinto capitolo un'analisi approfondita delle prospettive di riforma circa la regolamentazione della diffusione di *fake news* su Internet[455], appare interessante soffermarsi sulle possibili soluzioni per quanto concerne strettamente le campagne di disinformazione nel corso delle tornate elettorali.

Alcuni autori hanno fatto riferimento alla necessità di adattare norme preesistenti al nuovo contesto che si è venuto a creare nell'era della Post-Verità[456]; ciò potrebbe essere realizzato a livello nazionale mediante delle vere e proprie riforme o, a livello internazionale, mediante un'interpretazione evolutiva di disposti normativi da parte di organi quali la Corte Internazionale di Giustizia. E ancora, il medesimo obiettivo potrebbe essere raggiunto attraverso risoluzioni dell'Assemblea Generale delle Nazioni Unite che definiscano le norme primarie di diritto internazionale applicabili alle *Information* o *Cyber Operations*, o, infine, aggiornando e integrando manuali quali il *Tallinn Manual on International Law Applicable to Cyber Warfare*[457].

Altri autori hanno proposto la creazione di un nuovo trattato internazionale, al fine di regolamentare specificamente il *cyberspazio*; in ultima analisi, in modo non dissimile da come la *United Nations Convention on the Law of the Sea* è stata creata al fine di disciplinare l'ambito marittimo[458].

---

[454] BONFANTI, *Attacchi cibernetici in tempo di pace: le intrusioni nelle elezioni presidenziali statunitensi del 2016 alla luce del diritto internazionale,* cit., p. 726.

[455] V. *infra* Cap. IV.

[456] WALTON, *Duties owed: low intensity cyberattacks and liability for transboundary Torts in international law*, in *Yale law journal*, 2017; KILOVATY, *Doxfare: Politically Motivated leaks and the future of the norm of non-intervention in the era of weaponized information*, in *Harvard National Security journal*, 2018; VAN DE VELDE, *the law of cyber interference in elections*, cit.., 2017.

[457] RODRIGUEZ, *Disinformation Operations aimed at (Democratic) Elections in the context of public international law: the conduct of the internet research agency during the 2016 US Presidential Election*, cit., pp. 182-183.

[458] ASHLEY, *Taming Trolls: The need for an International Legal Framework to Regulate State use of Disinformation on Social Media*, in *The Georgetown Law Journal online*, vol. 107, *2018;* LEWIS,

Secondo tale filone dottrinale, il trattato in questione dovrebbe prendere le mosse dalla consapevolezza che i *social media* sono uno strumento forte, non vincolato da confini fisici, e che la diffusione di *fake news* per il tramite di queste piattaforme ha un impatto negativo sulla stabilità dell'intera comunità internazionale. L'accordo multilaterale sarebbe, dunque, rivolto alla regolamentazione dell'uso da parte degli Stati dei *social media* al fine di diffondere campagne di disinformazione. Proprio a tale scopo, sarebbe, quindi, necessario inserirvi delle disposizioni chiare e puntuali, circa i tentativi di attori statali di manipolare la popolazione di un altro Stato sovrano attraverso l'uso doloso di campagne di disinformazione sulle piattaforme *social*, così interferendo in maniera illegittima nel *Domaine Réservé* dello Stato passivo[459].

Il trattato avrebbe l'ulteriore scopo di rappresentare la cristallizzazione delle definizioni di diversi termini, quali appunto *fake news*, *Information* o *Cyber Operations*, nozioni sulle quali ad oggi vi è ancora grande dibattito nella comunità internazionale[460].

Secondo una parte degli autori, il perfetto foro per l'elaborazione di tale nuovo trattato internazionale sarebbe rappresentato proprio dalle Nazioni Unite; altri, sono dell'avviso che sarebbe sufficiente aggiungere un Protocollo Addizionale alle Convenzioni di Ginevra del 1949, ritendendo le C*yber Operations* come una nuova forma di conflitto internazionale.

Nonostante la apparente solidità di tale proposta, su un piano pratico la creazione di un trattato internazionale di tale genere risulta ardua. Molti autori, infatti, hanno mostrato scetticismo nei confronti della soluzione prospettata, ritenendo che la notevole disparità esistente tra le grandi potenze tecnologiche, quali Russia, Cina e Stati Uniti, e il resto del mondo, renderebbe i primi quantomeno reticenti ad

---

multilateral agreements to constraint cyberconflict, in *arms control today*, 2010; COUZIGOU, *securing cyber space: the obligation of States to prevent harmful international cyber operations*, in *International review of law, computer and technology*, n. 1, 2018, p. 54; ARIMATSU, *a treaty for governing cyber-weapons: potential benefits and practical limitations*, paper presented at the 4th international conference on cyber conflict, NATO, CCD, COE publications, Tallinn, 2012; HAMILTON, *beyond ballot-stuffing: current gaps in international law regarding foreign state hacking to influence a foreign election*, in *Wisconsin international law journal*, 2017; LAM, *a slap on the wrist: combatting Russia's Cyber attack on the 2016 U.S. Presidential election*, in *Boston College law review*, 2018.

[459] ASHLEY, *Taming Trolls: The need for an International Legal Framework to Regulate State use of Disinformation on Social Media*, cit., pp. 53 e ss.

[460] *Ibidem* p. 54; VAN DE VELDE, *The law of cyber interference in elections*, cit., pp. 53-54.

accettare la stipula di tale accordo; se non nel rispetto di condizioni poste da loro stessi [461].

In mancanza di un accordo internazionale, diversi attori nel corso del tempo hanno cercato soluzioni alternative, che ad oggi però non sembrano aver dato i frutti sperati.

A tal riguardo, possiamo ricordare il tentativo del 2015 del gruppo di esperti costituito dalle Nazioni Unite di sviluppare uno paradigma di comportamento nel *cyberspazio*, specificamente affermando che «*States must observe, among other principles of international law, State sovereignty, sovereign equality […]. and non-intervention in the internal affairs of other States*»[462].

E ancora, con un obiettivo analogo nel 2017 gli Stati del G7 hanno emanato una dichiarazione esponendo la loro crescente preoccupazione per le interferenze nei processi elettorali democratici, e dichiarando il proprio sostegno all'apertura di un dialogo internazionale al fine di dare forma al diritto internazionale del *cyberspazio*[463].

A tali iniziative, si aggiungono degli strumenti che potrebbero essere considerati di *soft law*.

Si tratta di norme di condotta non vincolanti, che hanno lo scopo di guidare e influenzare il comportamento degli Stati.

Tra questi va sicuramente annoverato il sovra menzionato *Tallinn Manual on International Law Applicable to Cyber Warfare.* Si tratta di un testo elaborato da un gruppo di esperti internazionali, sotto la spinta del NATO Cooperative *Cyber Defence Center of Excellence*, con specifico riguardo alla nuova forma di conflitti nota come c*yber warfare*. Tuttavia, nonostante questo potrebbe rivelarsi uno strumento molto importante, per ciò che concerne le campagne di disinformazione ad oggi la sua efficacia è limitata dalla mancanza di norme specifiche in materia di *Cyber o Information Operations* nel corso delle elezioni.

---

[461] GOLDSMITH, *Cybersecurity treaties: a skeptical view*, in *Hoover Institution at Stanford University*, 2011; PAGALLO, *Cyber force and the role of sovereign States in Informational warfare*, in *philosophy and technology*, n 3, 2015, p. 416.

[462] U.N. Secretary-General, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174, 22 luglio 2015, para 28.

[463] G7 Declaration on Responsible States behavior in Cyberspace, 11 aprile 2017, <<http://www.esteri.it/mae/resource/doc/2017/04/declaration_on_cyberspace.pdf >>.

E ancora, nel 2015 è stato elaborato *l'International Code of Conduct for Information Security*, il quale contiene norme che ben potrebbero essere adattate alla regolamentazione delle *disinformation operations* rivolte alle elezioni; a titolo esemplificativo, il paragrafo 3 prescrive «*not to use information and communications technologies and information and communication networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability*»[464]. Tuttavia, ad oggi si ritiene che tale strumento non abbia ancora la forza persuasiva e l'autorità necessarie per poter assurgere a efficiente strumento di *soft law* nella lotta contro le campagne di disinformazione[465].

Infine, per concludere gli strumenti di *soft law* potenzialmente idonei a porre rimedio al dilagare delle *Cyber* o *Information Operations* è necessario ricordare lo *EU Code of Practice on Disinformation*. Lasciando al prossimo capitolo un'analisi dettagliata[466], con specifico riferimento alle elezioni questo rappresenta uno strumento di grande importanza al fine di assicurare ciò che è stato definito dallo stesso Presidente della Commissione Europea delle «*free and fair elections*»[467]. Si tratta, infatti, di un codice di condotta non vincolante in cui vengono raccolte una serie di regole specificamente volte a combattere le *fake news*[468].

In conclusione, si è parlato di rimettere ai singoli ordinamenti nazionali la disciplina delle campagne di disinformazione, ad esempio estendendo le disposizioni che incriminano la violazione del silenzio elettorale anche alle notizie pubblicate o diffuse su Internet. Tuttavia, questo scenario appare poco efficace per una molteplicità di motivazioni.

Innanzitutto, come è stato evidenziato nei paragrafi precedenti, molto spesso queste campagne vengono condotte al di fuori del territorio Statale, come nel caso

---

[464] Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General, U.N. Doc. A/69/723, 13 gennaio 2015.

[465] MCKUNE, *An analysis of the International code of conduct for Information Security*, in *the citizen lab*, 2015.

[466] V. *infra* Cap. IV.

[467] Stato dell'Unione 2018, Discorso annuale sullo stato dell'UE pronunciato dal presidente Juncker al Parlamento europeo, 12 settembre 2018, p.7.<<https://ec.europa.eu/info/sites/info/files/soteu2018-speech_en_0.pdf>>,<<https://ec.europa.eu/info/priorities/state-union-speeches/state-union-2018_it>>.

[468] MEZZANOTTE, *Fake news nelle campagne elettorali digitali. Vecchi rimedi o nuove regole?*, cit., p. 22.

dell'IRA nel corso delle elezioni presidenziali americane del 2016 o delle *Disinformation Operations* che hanno caratterizzato la *Brexit*. Inoltre, la scarsa efficacia della proposta, che lascerebbe alle giurisdizioni nazionali la disciplina delle campagne di disinformazione nel contesto delle elezioni, deriva anche dal fatto che alcuni Stati potrebbero non avere a disposizione le risorse necessarie al fine di poter prevenire e reprimere le condotte in questione; ciò accentuerebbe la disparità tra le diverse aree del globo, implicitamente incentivando campagne di disinformazione da e verso quei Paesi in cui la disciplina e i mezzi per porla in essere sono più scarni. E ancora, normative nazionali di lotta contro le *fake news* potrebbero facilmente essere fatto oggetto di abuso al fine di introdurre delle norme di censura mistificate[469], soprattutto in Stati con forme di governo autoritarie.

Di conseguenza, rimettere ai singoli ordinamenti nazionali la regolamentazione di un fenomeno globale quale quello delle campagne di disinformazione appare un primo passo promettente, ma non una soluzione definita. Al contrario, ciò che potrebbe portare dei risultati vantaggiosi è prevedere un paradigma internazionale di regolamentazione, lasciando agli ordinamenti nazionali l'introduzione di norme mirate; ad esempio, come accennato sopra, disposizioni sul silenzio elettorale sulle piattaforme *social*, direzione in cui si sono già mossi alcuni Paesi, tra cui il Portogallo.

In definitiva, a differenza di singole *fake news* diffuse su Internet, le campagne di disinformazione nel corso delle tornate elettorali non hanno come unico obiettivo quello di andare a impattare o danneggiare la reputazione di un singolo partecipante della vita pubblica. Al contrario, queste mirano a minare la sovranità stessa dello Stato, manipolando il processo democratico che ne costituisce le fondamenta[470].

Ne consegue che il *fil rouge* che lega i vari strumenti ad oggi disponibili per contrastare le campagne di disinformazione è la raccomandazione, rivolta a tutti i soggetti coinvolti, di incentivare la trasparenza, i meccanismi di verifica della veridicità delle informazioni, la consapevolezza dei cittadini e la tutela dei dati personali.

---

[469] RODRIGUEZ, *Disinformation Operations Aimed at (Democratic) Elections in the context of Public International Law: The conduct of the Internet Research Agency during the 2016 US Presidential Elections*, in *International Journal of Legal Information*, cit., pp. 188-189.

[470] Organization of American States, Inter-American Commission on Human Rights, Special Rapporteur for Freedom of Expression, *Guide to guarantee freedom of expression regarding deliberate disinformation in electoral contexts*, 2019, p. 23.

CONCLUSIONI

Sulla base di quanto emerso dall'analisi delle conseguenze giuridico-penali della diffusione di *fake news*, si può concludere che la scelta ultima degli Stati e degli organismi sovranazionali risiede nel binomio eteroregolazione-autoregolazione.

Per quanto concerne la prima, in Italia sono stati proposti tre disegni legge in materia: il d.d.l. Gambaro, il d.d.l. Zanda – Filippin e il d.d.l. De Girolamo.

Partendo dal primo, questo è stato depositano il 7 febbraio 2017 dall'allora Senatrice Adele Gambaro del Movimento 5 Stelle.

Tale proposta parte dalla constatazione dell'asimmetria esistente tra il regime stringente previsto per gli operatori tradizionali e la disciplina lacunosa applicabile ai nuovi *providers.*

Nello specifico il d.d.l. Gambaro prevedeva l'introduzione di tre nuove disposizioni nel codice penale: l'art. 656 *bis* c.p. concernente il reato di pubblicazione o diffusione di notizie false, esagerate o tendenziose, atte a turbare l'ordine pubblico, attraverso piattaforme informatiche, e gli articoli 265 *bis* e 265 *ter* c.p. riguardanti due delitti contro la personalità dello Stato.

Per quanto attiene alla prima norma, risulta evidente che questa è stata plasmata sul modello della contravvenzione della pubblicazione di notizie false, esagerate o tendenziose, atte a turbare l'ordine pubblico. Rispetto a tale disposizione, tuttavia, il nuovo art. 656 *bis* c.p. sarebbe stato caratterizzato da due differenze significative: la specifica individuazione del luogo di divulgazione del materiale falso, ossia le piattaforme informatiche, e la rimozione dell'elemento dell'idoneità a turbare l'ordine pubblico, eliminazione che avrebbe trasformato la fattispecie di reato da pericolo concreto a pericolo astratto[471].

Tra le principali critiche mosse al d.d.l. in questione appare opportuno ricordare che secondo alcuni un'interpretazione restrittiva del testo in questione avrebbe portato al risultato, quasi paradossale rispetto allo scopo della disposizione, di escludere l'applicabilità di questa ai *social network,* dal momento che tali piattaforme non sono specificatamente create per la divulgazione di materiale informativo.

Passando ora all'articolo 265 *ter* c.p., rubricato "Diffusione di campagne d'odio volte a minare il processo democratico", questo presenta la caratteristica peculiare

[471] GUERINI, Fake News *e Diritto Penale, La Manipolazione Digitale del Consenso nelle Democrazie Liberali,* cit., pp. 170-171.

di aprirsi con la dichiarazione di intenti "al fine della tutela del singolo e della collettività". In altre parole, si sarebbe trattato di un delitto comune plurioffensivo, la cui formulazione, tuttavia, è apparsa, a gran parte della dottrina, come non compatibile con il principio di materialità dell'incriminazione, data la genericità e l'atecnicità della locuzione "campagne d'odio"[472].

E ancora, alla luce della Raccomandazione numero 2143 del 2017 del Consiglio d'Europa e del d.d.l. Gambaro, il 14 dicembre 2017 è stato, poi, presentato il disegno di legge Zanda-Filippin, in cui viene sottolineato l'effetto distorsivo dell'opinione pubblica provocato dalla diffusione di *fake news* nel corso delle consultazioni elettorali.

A differenza della proposta precedente, il disegno di legge in esame si pone quasi a metà strada tra il costituire una forma di eteroregolazione e il suggerire l'adozione di strumenti di autoregolazione.

Infatti, i due proponenti, sul modello del Netz DG tedesco, adottano un approccio preventivo, basato su una responsabilizzazione dei *provider* delle piattaforme *social*, inducendo questi a dotarsi di meccanismi interni di rimozione dei contenuti illeciti e raccolta delle segnalazioni degli utenti.

Nello specifico, il d.d.l. Zanda-Filippin avrebbe previsto l'introduzione di un procedimento di rimozione dei materiali illeciti, che sarebbe stato caratterizzato dall'attivazione su reclamo, e dal fatto che i *social network* avrebbero dovuto dotarsi di un meccanismo efficace, trasparente e permanente per la ricezione e la gestione delle denunce.

Per quanto attiene ai contenuti manifestatamente illeciti, tale procedura avrebbe dovuto consentire alla piattaforma di prendere immediatamente in carico la denuncia, di verificare l'illiceità del contenuto oggetto del reclamo e di rimuovere o bloccare l'accesso al contenuto in esame entro 24 ore dalla ricezione; ovviamente, fatta eccezione per l'ipotesi in cui il gestore avesse preventivamente concordato con le autorità competenti un termine più lungo. Per i reclami sui contenuti non manifestatamente illeciti, invece, il blocco o la rimozione sarebbero dovuti avvenire solo dopo che fosse stata accertata l'illegalità effettiva, e in ogni caso non oltre 7 giorni dalla denuncia.

---

[472] GUERINI, *Fake News e Diritto Penale, la manipolazione digitale del consenso nelle democrazie liberali,* cit., p. 172; NISCO, *La tutela penale dell'integrità psichica*, Torino, 2012.

In caso di violazione dei rispettivi termini di 24 ore o di 7 giorni, inoltre, la piattaforma *social* sarebbe incorsa in una sanzione pecuniaria compresa tra un minimo di cinquecentomila e un massimo di cinque milioni di euro.

A tal riguardo, la proposta in esame suggeriva l'istituzione e l'accreditamento di organismi ad *hoc* di autoregolazione, ai quali i *provider* di *social network* avrebbero potuto affidare le procedure di gestione dei reclami. In altre parole, si sarebbe trattato di strutture associative composte da più fornitori di servizi di *social network*, che avrebbero dovuto possedere specifici requisiti quali: l'indipendenza e l'esperienza dei loro componenti, l'utilizzo di strutture adeguate e la possibilità di adesione di altri fornitori di servizi.

Infine, appare opportuno ricordare il d.d.l De Girolamo che, nonostante riguardasse un argomento parzialmente differente, mirava a sanzionare condotte prodromiche alla commissione di illeciti *on-line.*

Il disegno di legge in esame, rubricato "L'introduzione del divieto dell'uso anonimo della rete internet e disposizioni in materia di tutela del diritto all'oblio", è stato proposto il 10 ottobre 2017 dall'onorevole De Girolamo e da altri parlamentari del gruppo politico di Forza Italia.

Tale proposta si caratterizza per la sua estrema concisione, comprendendo l'introduzione di due soli nuovi articoli che avrebbero mirato da un lato a combattere l'anonimato su Internet, rendendo le interazioni tra gli utenti tracciabili e riconducibili a una persona fisica, e dall'altro a consentire un effettivo esercizio del diritto all'oblio.

Nella medesima ottica di eteroregolazione, negli Stati Uniti nell'anno fiscale 2017, con l'approvazione del *National Defense Authorization Act (*NDAA), è stato istituto il *Global Engagement Center*. Questo ha la funzione di coordinare, integrare e sincronizzare gli sforzi nazionali e internazionali di riconosce, comprendere e combattere la disinformazione e la propaganda, tanto estera, quanto non statale.

L'adozione di forme di regolamentazione pubbliche è stata, tuttavia, oggetto anche di forti critiche, molte delle quali, a livello del nostro ordinamento interno, hanno trovato il proprio fondamento nella pronuncia della Corte Costituzionale del 2000 n. 502[473]; secondo questa, la determinazione di cosa sia vero o giusto può solamente essere rimessa al contraddittorio delle idee dei soggetti coinvolti. Di conseguenza,

[473] Corte Cost., 17 novembre 2000, n. 502.

secondo la Corte, sarebbe irragionevole pretendere da soggetti pubblici una comunicazione imparziale in materia.

Passando ora alle proposte di autoregolazione del fenomeno della divulgazione di *fake news on-line*, appare opportuno ricordare il *Code of Practice on Disinformation* dell'Unione Europea.

La problematica relativa ai fenomeni manipolativi dell'informazione, infatti, è stata oggetto di numerosi interventi da parte dell'Unione, la quale dopo la sponsorizzazione del rapporto "*A multi-dimensional approach to disinformation*"[474], ha emanato la comunicazione "*Tackling online disinformation: a European approach*"[475], di cui il *Code of Practice on Disinformation* costituisce diretta propaggine.

Si tratta di uno strumento di *soft law* che, riunendo su base volontaria alcuni tra i più importanti e influenti soggetti del *web*, ha lo scopo di orientare l'azione degli individui privati nella lotta contro la diffusione di *fake news*, mediante l'individuazione di principi guida che ogni firmatario è, poi, libero di attuare e implementare nel modo che ritiene più consono ed efficace[476]. Inoltre, così come ogni sottoscrittore può ritirare in ogni momento la propria adesione al Codice, o a parte di questo, mediante notifica alla Commissione e agli altri membri, allo stesso modo è consentito a nuovi attori di aderirvi.

E ancora, è lo stesso Codice a chiarire che «*the Code shall apply within the framework of existing laws of the EU and its Member States and must not be construed in any way as replacing or interpreting the existing legal framework, and, in particular*»[477].

Tra i meriti del Codice è, inoltre, importate ricordare che questo, inserendosi nella scia dei precedenti interventi europei, delinea una definizione di *fake news* chiara e lineare, descrivendole come «*verifiably false or misleading information*», create o divulgate per scopi economici o al fine di generare disinformazione.

[474] COMMISSIONE EUROPEA, *A multi-dimensional approach to disinformation,* cit.
[475] COMMISSIONE EUROPEA, *Tackling online disinformation,* cit.
[476] MONTI, *Il Code of Practice on Disinformation dell'UE: tentativi in fieri di contrasto alle fake news,* in *Media Laws,* 2019, p. 320.
[477] COMMISSIONE EUROPEA, *Code of Practice on Disinformation,* ottobre 2018, p. 2.

Il vantaggio fornito da tale definizione è quello di rendere palese l'esclusione dalla nozione di *fake news* concetti quali quello di satira, errori giornalistici o comunicazioni politiche[478].

Inoltre, i confini di ciò che può essere considerato una *fake news* sono chiariti ulteriormente dalla specificazione prevista dal *Code of practice on Disinformation* secondo cui, al fine di integrare gli estremi della nozione in questione, è necessario un requisito di pericolosità che si sostanzia in elementi quali «*threats to democratic political and policy making processes as well as public goods such as the protection of EU citizens' health, the environment or security*».

E ancora, lo strumento di *soft law* in esame prosegue elencando le finalità a cui è preposto: la lotta alla *disinformation*; il miglioramento dei meccanismi di controllo nell'assegnazione delle pubblicità; la trasparenza sulla targetizzazione degli *user* a cui sono rivolti i materiali informativi; la promozione di *policies* anti *misrepresentation*; la chiusura degli *accounts fake* e la regolamentazione dell'attività dei *bots*; l'attenzione agli sforzi contro coloro che divulgano *fake news*; investimenti in tecnologie per incrementare la ricerca e l'indicizzazione delle notizie affidabili, senza tuttavia cedere a pressioni governative o censure basate sulla mera "falsità" dei contenuti; la garanzia della trasparenza delle informazioni ricevute dagli utenti in relazione alla loro affidabilità e all'identità delle fonti di provenienza; il disincentivo della disinformazione rispetto all'informazione affidabile; l'aumento delle possibilità e della capacità degli utenti di trovare informazioni con diversi orientamenti e punti di vista; l'incentivo rivolto alle attività di *fact-checking*.

In ottica riassuntiva, si può, dunque, affermare che lo scopo ultimo del Codice sia quello di disincentivare la disinformazione, al contempo promuovendo e incentivando l'informazione corretta e veritiera, mediante l'introduzione di "marchi di affidabilità", ad esempio collaborando direttamente con società di *fact-checking.*

In altre parole, il Codice adotta una prospettiva basata sull'autoregolazione, delegando alle piattaforme digitali la scelta del regime di lotta contro la divulgazione di *fake news on-line* da adottare, non riservando ad alcun organo

[478] MONTI, *Le "bufale" online e l'inquinamento del public discourse*, in P. PASSAGLIA - D. POLETTI (a cura di), *Nodi virtuali, legami informali: Internet alla ricerca di regole*, Pisa, 2017, 182 ss.; MONTI, *The New Populism and Fake News on the Internet: How Populism Along with Internet New Media is Transforming the Fourth Estate*, in *StalsResearchPaper*, 2018.

pubblico alcun potere di controllo sul raggiungimento degli obiettivi di trasparenza e correttezza.

Nella medesima ottica di autoregolazione, a livello nazionale, nel 2018 l'AGCOM ha istituito il Tavolo Tecnico per la Garanzia del Pluralismo e della Correttezza dell'Informazione sulle Piattaforme Digitali[479] che, avendo l'obiettivo specifico di promuovere l'autoregolazione delle piattaforme e la condivisione di buone pratiche per la lotta contro i fenomeni manipolativi dell'informazione su Internet, ha portato all'adozione delle "Linee guida per la parità di accesso alle piattaforme online durante la campagna elettorale per le elezioni politiche 2018"[480].

Si tratta di un intervento di autoregolazione volto a delineare dei principi generali, applicabili a tutti i mezzi di informazione, comprese le piattaforme su Internet. Nello specifico, tra tali principi fondanti della materia è opportuno ricordare: la parità di accesso, la quale deve essere garantita a tutti i soggetti politici, con imparzialità ed equità e alle medesime condizioni; l'accesso agli strumenti di informazione e comunicazione politica forniti dalle piattaforme digitali; il rispetto della trasparenza dei messaggi pubblicitari elettorali; la rapidità e la tempestività d'intervento in caso di pubblicazione di contenuti illeciti o di materiali la cui divulgazione è vietata dalla legge; l'invito all'estensione del divieto di pubblicazione istituzionale, previsto dall'art. 9 della legge n. 28 del 2000,

anche all'utilizzo di account istituzionali di *social media* per la diffusione di messaggi e comunicazione istituzionale; l'auspicio a che venga estesa la disciplina sul silenzio elettorale nel giorno del voto e nel giorno precedente a questo, anche sulle piattaforme digitali, al fine di evitare di esercitare influenza e pressioni indebite sull'elettorato; la raccomandazione sul rafforzamento delle attività di *fact-checking*.

Nonostante i numerosi tentativi di delineare codici o principi che possano guidare e orientare la condotta delle piattaforme verso comportamenti responsabili e trasparenti, tuttavia, l'uso esclusivo di forme e strumenti di autoregolazione ha incontrato notevoli dissensi in dottrina, basati principalmente sull'eccessivo potere che sarebbe conferito alle piattaforme o ad altri soggetti privati.

---

[479] AGCOM, *News vs Fake, nel sistema dell'informazione, interim report, indagine conoscitiva*, DEL. 309/16/CONS, novembre 2018.

[480] AGCOM, *Direzione Contenuti Audiovisivi, Servizio Economico-Statistico, Linee guida per la parità di accesso alle piattaforme online durante la campagna elettorale per le elezioni politiche*, 2018.

A titolo esemplificativo, tale timore è stato sintetizzato dalla professoressa D. Keller nella sua affermazione secondo cui scegliere un approccio basato esclusivamente sull'autoregolazione avrebbe la conseguenza di rendere "*Google the Censor*"[481].

Alla luce di tali orientamenti, l'approccio maggiormente condivisibile appare quello presentato da Giovanni Pitruzzella, secondo cui sarebbe più efficace adottare una soluzione ibrida tra autoregolazione ed eteroregolazione, predisponendo, quindi, una *partnership* pubblico-privata.

Ciò assicurerebbe un'informazione corretta e completa, al contempo, però, tutelando il pluralismo ed evitando il rischio che si cada in forme di censura, siano esse pubbliche o private[482].

Nello specifico, l'Autore ha proposto l'istituzione di una cosiddetta "Autorità Pubblica della Verità"[483], ossia un'autorità amministrativa indipendente preposta ad intervenire, in via sussidiaria ma tempestiva, al fine di rimuovere dal *web* materiale palesemente *fake*, diffamatorio, lesivo di diritti fondamentali o altrimenti illegittimo.

Si tratterebbe, in altre parole, di un intervento *ex post*, sussidiario rispetto all'applicazione degli strumenti di autoregolazione, che consentirebbe di tutelare la libertà di espressione a tutto tondo, sia dal lato attivo di chi diffonde notizie, che da quello passivo dei soggetti che le percepiscono.

---

[481] KELLER, *Make Google The Censor*, in *New York Times*, 12 giugno 2017.

[482] MONTI, *Il Code of Practice on Disinformation dell'UE: tentativi in fieri di contrasto alle fake news*, cit., p. 324; CUNIBERTI, *Il contrasto alla disinformazione in rete tra logiche del mercato e (vecchie e nuove) velleità di controllo*, in *media laws*, 2017, pp. 35, 37.

[483] PITRUZZELLA, POLLICINO, QUINTARELLI, *Parole e potere. Libertà d'espressione, hate speech e fake news*, cit., p. 88.

INDICE BIBLIOGRAFICO

47 U.S. Code § 230 (C)(f)(2) con nota di MIRANDA, *Defamation in Cyberspace: Stratton Oakmont, Inc. v. Prodigy Services Co*., in *Albany Law Journal of Science & Technology*, 1996.

ABBONDANTE, *il ruolo dei social network nella lotta all'hate speech: un'analisi comparata fra l'esperienza statunitense e quella europea*, in *Informatica e Diritto*, XLII, Vol. XXVI, n. 1-2.

ALLEGRI, *Ubi social, ibi ius. Fondamentanti costituzionali dei social network e profili giuridici della responsabilità dei provider*, Milano, 2018.

AMERIO, La responsabilità ex. art. 57 c.p. del direttore di testate telematiche: tra estensione interpretativa ed analogia in malam partem, in media laws, 2019.

ARIMATSU, *a treaty for governing cyber-weapons: potential benefits and practical limitations,* paper presented at the 4th international conference on cyber conflict, NATO, CCD, COE publications, Tallinn, 2012.

ASHLEY, *Taming Trolls: The need for an International Legal Framework to Regulate State use of Disinformation on Social Media*, in *The Georgetown Law Journal online*, vol 107, 2018.

AUTORITÀ GARANTE PER LE COMUNICAZIONI, *Direzione Contenuti Audiovisivi, Servizio Economico-Statistico, Linee guida per la parità di accesso alle piattaforme online durante la campagna elettorale per le elezioni politiche*, 2018.

AUTORITÀ GARANTE PER LE COMUNICAZIONI, *New vs. Fake nel Sistema dell'informazione,* Interim Report, Indagine Conoscitiva, Del. 309/16/Cons, novembre 2018.

AUTORITÀ PER LE GARANZIE E NELLE COMUNICAZIONI, *Linee guida per la parità di accesso alle piattaforme online durante la campagna elettorale per le elezioni politiche 2018*.

Auvial v. CBS 60 Minutes, 800, F. Supp., E.D. Washington, 1992.

AVIGNO, *Intermediary Liability for User-Generated Content in Europe*, Tallinn University of Technology, Tallinn 2016.

BABAKAR, *The EU referendum, factchecked*, in *FullFact*, 2016, <<https://fullfact.org/blog/2016/jun/eu-referendum-2016/ >>.

BACCIN, *Responsabilità penale dell'Internet Service Provider e concorso degli algoritmi negli illeciti online: il caso force v Facebook*, in *Sistema penale*, 5/2020.

BADER, *Disinformation in Elections,* in *Security and Human Rights*, 2018.

BAISTROCCHI, *Liability of intermediary service providers in the EU directive on electronic commerce*, in *Computer and high technology law journal*, 2003, vol. 19.

BARCELO, *Liability for online intermediaries: A European Perspective*, in *Centre de recherches informatique et droit*, 1998.

BASSINI, *Commercio elettronico e tutela dei segni distintivi. Responsabilità degli intermediari e trend giurisprudenziali*, MAZZARO - POLLICINO (a cura di), in *Tutela del copyright e della privacy sul web. Quid iuris?*, Roma, 2012.

BASSINI, *La disciplina penale della stampa alla prova di internet: avanzamenti e arresti nella dialettica giurisprudenziale da una prospettiva costituzionale*, in FLOR, FALCINELLI, MARCOLINI (a cura di), *La giustizia penale nella "rete" Le nuove sfide della società dell'informazione nell'epoca di Internet,* 2015.

BASSINI, *Primi appunti su* fake news *e dintorni*, in *Media Laws*, 11 ottobre 2017.

Batzel v. Smith, 333 F.3d, 9th Cir., 2003; Barrett v. Rosenthal, 5 Cal. Rptr. 3d, Cal. Ct. App., 2003.

BAYER, *Liability of internet service providers for third party content*, in *Resarchgate.net,* 2007.

BENNATO, *L'emergere della disinformazione come processo socio-computazionale, Il caso Blue Whale,* in *Problemi dell'Informazione*, dicembre 2018.

Blumenthal v Drudge, 992, F. Supp., DDC, 1998.

BOCCHINI, *La responsabilità di Facebook per la mancata rimozione di contenuti illeciti,* in *Giur.it*., 2017.

BONFANTI, *Attacchi cibernetici in tempo di pace: le intrusioni nelle elezioni presidenziali statunitensi del 2016 alla luce del diritto internazionale*, in *Rivista di diritto internazionale*, 3/2019, pp. 700 e ss; SCHMITT, VIHUL, *Sovereignity in Cyberspace: Lex Lata vel Non?,* in *American Journal of International Law*, 2017.

BRUNO, 2016, *L'anno della post-verità e del boom delle false notizie,* in *Sky TG24*, 2016, <<https://tg24.sky.it/mondo/2016/12/28/2016-anno-fake-news-post-truth>>.

BUGIOLACCHI, *Ascesa e declino della figura del provider "attivo"? Riflessioni in tema di fondamento e limiti del regime privilegiato di responsabilità dell'hosting provider*, in *Resp. civ. prev*., 2015.

BUGIOLACCHI, *I presupposti dell'obbligo di rimozione dei contenuti da parte dell'hosting provider tra interpretazione giurisprudenziale e dettato normativo*, in *Resp. civ. prev*., 2017.

CAGE, HERVE, VIAUD, *The Production of Information in an Online World*, in *NetInstitute.org*, working paper n. 2015/05.

CALVERT, VINING, *Filtering fake news through a lens of the supreme Court observations and adages*, in *UF Law Faculty Publications*, 2018.

Cambridge Dictionary: proxy, <<https://dictionary.cambridge.org/it/dizionario/inglese/proxy >>.

Cambridge Dictionary: Troll Factory, <<https://dictionary.cambridge.org/it/dizionario/inglese/troll-factory >>.

CANTRIL, *The Invasion from Mars*, in *Princeton Legacy Library*, 1982.

CARAVALE, *La "faglia" della Brexit,* in *Nomos le attualità nel diritto*, n. 2/2016.

CARREA, *the ECHR in Cyberspace: does the power to infringe always entail the duty to protect*?, in *Diritti Umani e Diritto Internazionale,* 2019.

CASCELLA, *Le condizioni per il legittimo esercizio del diritto di cronaca*, in *diritto.it,* 2012.

Cass civ., Sez. I, 19 marzo 2019, n. 7709 con nota di TOSI, *La disciplina applicabile all'hosting provider per la pubblicazione di contenuti digitali protetti dal diritto d'autore, tra speciale irresponsabilità dell'ISP passivo e comune responsabilità dell'ISP attivo, alla luce di Cassazione 7708/2019 e 7709/2019*, in *Rivista di Diritto Industriale*, 2019.

Cass, pen., 4. Febbraio 1976, in *Cass. Pen. Mass.ann.*, con nota di MULLIRI.

Cass, pen., Sez. V, 20 febbraio 2019, n. 7808, in *www.dejure.it.*

Cass. civ., I sez., 19 marzo 2019, n. 7708, in *www.dejure.it.*

Cass. civ., sez. I, 27 gennaio 2006, n. 1755, in *www.dejure.it.*

Cass. civ., sez. I, 6 aprile 1993, n. 4109, in *Corr. giur*., 1993, nota ZENCOVICH.

Cass. civ., sez. III, 10 febbraio 2003, n. 1954, in *www.dejure.it.*

Cass. civ., sez. III, 13 gennaio 2009, n. 482, in *Foro it*.

Cass. civ., Sez. III, 15 gennaio 2002, n. 370, in *Foro it*, Rep., 2002, voce Responsabilità civile, n. 197.

Cass. civ., sez. III, 15 ottobre 2004, n. 20334, in *www.dejure.it.*

Cass. civ., sez. III, 19 luglio 2002, n. 10551, in *Danno e Resp*., 12/2002, con nota di AGNINO.

Cass. civ., sez. III, 21 ottobre 2005, n. 20357 in *www.dejure.it.*.

Cass. civ., sez. III, 21 ottobre 2005, n. 20359, in *www.dejure.it.*.

Cass. civ., sez. III, 26 aprile 2004, n. 7916, in *www.dejure.it.*.

Cass. civ., sez. III, 27 maggio 2005, n. 11275 in *www.dejure.it.*.

Cass. civ., sez. III, 3 marzo 2010, n. 5081, in *La responsabilità civile*, 2011, con nota di BALLERINI.

Cass. civ., Sez. III, 5 giugno 2002, n. 8148, in *www.dejure.it*.

Cass. civ., Sez. III, 6 aprile 2006, n. 8095, in *Responsabilità Civile*, 7/2006, con nota di FACCI.

Cass. civ., Sez. III, 7 febbraio 1996, n. 982, in *Danno e resp.,* 1996, con nota di CHIAROLLA.

Cass. civ., Sez. III, 7 ottobre 2011, n. 20608, in *Foro it*.

Cass. civ., Sez. III. 17 ottobre 2013, n. 23576, in *www.dejure.it*.

Cass. pen Sez. II, 21 dicembre 2011, n. 4250, in *www.dejure.it.*

Cass. pen, Sez IV, 11 gennaio 1977, n. 3967, in *riv. En*.

Cass. pen, Sez. I, 7 novembre 1996, n. 9475, in *Pluris*.

Cass. pen, Sez. V, 1 febbraio 2017, n. 4873, in *www.dejure.it*.

Cass. pen, Sez. V, 8 giugno 2018, n. 33862, in *Dir. Pen. Cont*.

Cass. pen, Sez. V, 8 novembre 2018, n.12546, in *www.dejure.it*.

Cass. pen. Sez. I, 28 aprile 2015, n. 24431, in *www.pluris.it.*

Cass. pen. Sez. III, 11 dicembre 2008, n. 10535, in *Foro it.*, 2010, con nota di CHIAROLLA, *Riflessioni introno al concetto di produzione editoriale digitale.*

Cass. pen. Sez. U.U., 17 luglio 2015, n. 31022, in *www.dejure.it*.

Cass. pen. Sez. V, 16 luglio 2010, n. 35511, in *www.dejure.it.*

Cass. pen. Sez. V, 2 aprile 2014, n. 25744, in *Giur. Pen*.

Cass. pen. Sez. V, 22 novembre 2017, n. 5352, in *www.dejure.it*.

Cass. pen. Sez. V, 29 novembre 2011, n. 44126, in *www.dejure.it.*

Cass. pen. Sez. V. 11 giugno 2010, n. 30065, in *www.dejure.it*.

Cass. pen. Sez., V, 1 luglio 2008, n. 31392, in *Dir. Inf.*

Cass. pen. Sez., V, 11 novembre 2009 n. 7407, in *www.dejure.it*.

Cass. pen., Sez. I, 9 febbraio 2018, n. 26897, in *www.dejure.it.*

Cass. pen., Sez. III, 17 dicembre 2013, n. 5107, *www.dejure.it.*

Cass. pen., Sez. III, 29 settembre 2009, n. 49437, *www.dejure.it.*

Cass. pen., sez. IV, 27 maggio 2003, n. 34620, in *www.dejure.it.*

Cass. pen., Sez. V, 10 ottobre 2017, n. 4413, in *www.dejure.it*.

Cass. pen., sez. V, 11 dicembre 2017, n. 13398, in *Foro it*., 5, 2018, II.

Cass. pen., Sez. V, 14 agosto 2008n. 33472, in *www.dejure.it*.

Cass. pen., Sez. V, 14 dicembre 2007, n. 46674, in *www.dejure.it.*

Cass. pen., Sez. V, 15 giugno 2016, n. 34800, in *www.dejure.it.*

Cass. pen., Sez. V, 16 luglio 2010, n. 35511, in *penale.it.*

Cass. pen., Sez. V, 19 febbraio 2018, n. 16751, in *Cass. pen*., 11, 2018, con nota di PEDULLÀ.

Cass. pen., Sez. V, 19 giugno 2008, n. 30664, in *www.dejure.it.*

Cass. pen., Sez. V, 2 dicembre 2004, n. 46786, in *www.dejure.it*.

Cass. pen., Sez. V, 22 aprile 2010, n. 34916, in *www.dejure.it.*

Cass. Pen., Sez. V, 22 giugno 2018, n. 42572, in *www.dejure.it.*

Cass. pen., Sez. V, 23 aprile 2014, n. 25774, con nota di SANSOBRINO, *Creazione di un falso account, abusivo utilizzo dell'immagine di una terza persona e delitto di sostituzione di persona*, in *Dir. Pen Cont.*, 2014.

Cass. pen., Sez. V, 27 dicembre 2016, n. 54946, in *www.dejure.it*.

Cass. pen., Sez. V, 28 gennaio 2013, n. 13296, in *www.dejure.it.*

Cass. pen., Sez. V, 28 novembre 2012, n. 18826, in *www.dejure.it*.

Cass. pen., Sez. V, 29 ottobre 2008, n. 40359, in *www.pluris.it*.

Cass. pen., Sez. V, 30 gennaio 2018, n. 4413, in *www.dejure.it*.

Cass. pen., Sez. V, 8 novembre 2007, n. 46674, in *www.dejure.it*.

Cass. pen., Sez. V, 8 novembre 2018, n. 12546 in *www.dejure.it*.

Cass. pen., Sez. V, n. 24727, del 21 gennaio 2016, *www.dejure.it.*

Cass. pen., Sez. V,16 giugno 2014, n. 25774, in *www-dejure.it.*

Cass. pen., Sez.V, 8 novembre 2007, n. 46674, in *Cass.Pen*.

Cass. Sez. I, 20 dicembre 2018, n. 16381, *www.dejure.it.*

Cass. Sez. I, 26 giugno 1989, n. 11835, *in* *www.dejure.it.*

Cass., civ., Sez. III, 29 ottobre 2019, n. 27592, in *www.dejure.it*.

Cass., Pen., 23 ottobre 2018, n. 1275, in *Dir. pen. cont. (online)*.

Cass., Sez. I, 22 gennaio 2014 n. 16712, con nota di TURCHETTI, *Diffamazione su Facebook: comunicazione con più persone e individuabilità della vittima, in Dir. pen. cont.*, 8 maggio 2014.

Cass., SS. UU, 25 ottobre 2007, n. 46982, in *www.dejure.it*.

Cass.pen, Sez. V, 14 novembre 2016, n. 4873, in *Dir. pen. cont*.

CASTELLS, *Comunicazione, potere e contro-potere nella network society* in <<http://www.caffeuropa.it/socinrete/castells.pdf>>.

CHESNEY, CITRON, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 14 luglio 2018, in *University of California Berkeley School of Law*.

CHIRCOP, *A due diligence Standard of Attribution in Cyberspace*, in *cambridge.org*, 2018.

Cianci v. New York Times Publ'g Co., 639 F. 2d, 1980.

CIMINO, *Art. 21 Costituzione ed i limiti a sequestro dei contenuti (multimediali) nelle pubblicazioni telematiche e nei prodotti editoriali*, in *Dir. inf.*, 2009.

Coffey v. Midland Broadcasting Co., D. C. Mo., 1934.

Cohen v. Facebook Inc., 252 F. Supp. 3d 140; Cain e Gonzalez v. Twitter, 17 Civ. 122, PAC, S.D.N.Y. 2017.

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

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

COMMISSIONE EUROPEA, *A multi-dimensional approach to disinformation, Report of the independent High-level Group on fake news and online disinformation*, 2018.

COMMISSIONE EUROPEA, *Code of Practice on Disinformation*, ottobre 2018.

COMMISSIONE EUROPEA, *Commission Communication for tackling online Disinformation: a European approach*, COM, 2018.

COMMISSIONE EUROPEA, *Final report of the High-Level Expert Group on Fake News and Online Disinformation*, 12 marzo 2018.

COMMISSIONE EUROPEA, *Impact assessment of the Digital Markets Act*, 8 marzo 2021, <<https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-markets-act>>.

COMMISSIONE EUROPEA, *Lotta ai contenuti illeciti online. Verso una maggiore responsabilizzazione delle piattaforme online*, COM (2017) 555, 28 settembre 2017.

COMMISSIONE EUROPEA, *Strategia per il mercato unico digitale in Europa*, COM(2015) 192, 6 maggio 2015.

COMMISSIONE EUROPEA, *Tackling online disinformation*, 7 luglio 2020.

con nota di BIRRITTERI, *Diffamazione e facebook: la cassazione conferma il suo*
con nota di MAURI.

Conclusioni del Consiglio su *Shaping Europe's Digital Future,* 8711/20, 9 giungo 2020.

CORN, TAYLOR, *Sovereignty in the Age of Cyberspace,* in *American Journal of International Law*, 2017.

Corte Cost., 13 luglio 1988, n. 826 in *consultaonline*.

Corte Cost., 13 maggio 1987, n. 153 in *consultaonline*.

Corte Cost., 13 maggio 1987, n. 153 in *consultaonline.*

Corte Cost., 14 luglio 1981, n. 148, in *consultaonline.*

Corte Cost., 15 luglio 1976, n. 202 in *consultaonline.*

Corte cost., 16 marzo 1962, n. 19, in *giurcost.org.*

Corte Cost., 2 aprile 1969, n. 84, in *consultaonline*.

Corte cost., 23 giugno 1956, n. 2, in *giurcost.org;* Corte cost., 18 marzo 1962, n. 19, in *giurcost.org.*

Corte Cost., 24 marzo 1993, n. 112 in *consultaonline.*

Corte cost., 24 marzo 1993, n. 112, in *consultaonline*.

Corte Cost., 8 luglio 1971, n. 168, *giurcost.org.*

Corte Cost., 9 giugno 1972, n. 105 in *consultaonline.*

Corte Cost.,9 luglio 1974, n. 225, in *consultaonline*.

Corte di Appello Milano, Sez. impr., 7 gennaio 2015, n. 29, in *Dir. ind*., 2016, con nota di IASELLI, *Caso Yahoo! Video: la Corte di Appello di Milano non vede responsabilità nell'operato dell'internet provider*.

Corte Giustizia dell'Unione Europea, C-324/09, l'Oréal SA e a.c. eBay International AG, in *AIDA*, 2011, con nota di NORDEMANN, *Liability of Social Networks for IP Infringements (Latest News): The Eu Law Regime after l'Oréal/eBay*, 12 luglio 2011

Corte di Giustizia dell'Unione Europea, Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, Grande Sezione, 13 maggio 2014.

Corte di Giustizia dell'Unione Europea, Grande sezione, 23 marzo 2010, cause riunite C-236/08, C-237/08 e C-238/08, Google France SARL, Google Inc. c Luis Vuitton SA, Luteciel SARL, Google Frace SAL c Centre national de recherche en

relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL.

Corte di Giustizia dell'Unione Europea, sez. III, Glawischnig-Piesczek c. Facebook Ireland, 3 ottobre 2019.

Corte di Giustizia dell'Unione Europea, sez. III, SCARLET c. SABAM, 24 novembre 2011.

Corte Europea dei diritti dell'uomo, Delfi AS c. Estonia, Grande Camera, Application n. 64569/09, 2015.

Corte Europea dei Diritti dell'Uomo, *Editorial board of Pravoye Delo e Shtekel v Ukraina*, nr. 33014/05, 4 maggio 2011.

Corte Europea dei Diritti dell'Uomo, K.U v. Finland, Application No. 2872/02, 2008.

Corte Europea dei diritti dell'uomo, Magyar Tartalomszolgaltatok Egyesulete and Index.hu ZRT v Hungary, Application No. 22947/13, 2016.

Corte Europea dei Diritti dell'Uomo, *Stoll v Svizzera*, nr. 69698/01, 10 dicembre 2007.

Corte Internazionale di Giustizia, *Corfu Channel Case,* (United Kingdom of Great Britain and Northern Ireland v Albania, 1949.

COSTANTINI, *Diritto penale e libertà di espressione in Internet,* in *Dir. pen. cont. – Riv. Trim,* 2/2019.

COUZIGOU, *securing cyber space: the obligation of States to prevent harmful international cyber operations*, in *International review of law, computer and technology*, n. 1, 2018.

Cubby, Inc. v. CompuServe, Inc., 776 F. Supp., S.D.N.Y. 1991, paras 135, 141.

D'ALFONSO, *Verso una maggiore responsabilizzazione dell'hosting provider tra interpretazione evolutiva della disciplina vigente, innovazioni legislative e prospettive de jure codendo,* in *Federalismi.it,* n. 2/2020.

DA EMPOLI, *Gli ingegneri del caos. Teoria e Tecnica dell'internazionale populista*, Venezia, 2019.

DALE, *Napoleon is Dead,* 2006.

DALLA CASA, *Napoleone è Morto! La Fake News che mandò in tilt la borsa di Londra,* in *Wired.it*, 28 luglio 2017.

Daniel v. Dow Jones and Co., 520 N.Y.S., 1987.

Decreto Semplificazione e innovazione digitale, DL. 76/2020.

DEPARTMENT OF DEFENCE (US DOD), *Memorandum of chiefs of military services: joint terminology for cyberspace operations*.

DI RESTA, SHAFFER, RUPPEL, SULLIVAN, MATNEY, FOX, ALBRIGHT, JOHNSON, *The Tactics and Tropes of the Internet Research Agency,* in *New Knowledge*, 2019.

DIAKOPOULOS, *Algorithmic Accountability Reporting: On the Investigation of Black Boxes*, in *Columbia Journalism School*, 2014.

Dichiarazione congiunta dello Special Rapporteur delle Nazioni Unite e dei Rappresentanti dell'OSCE e dell'OAS sulla promozione della libertà di espressione, 28 dicembre 2005, <www.osce.org/fom/27455?download=true>>.

Dichiarazione del Comitato dei Ministri del Consiglio d'Europa sulla libertà di comunicazione su Internet, principio n. 3, 28 maggio 2003.

DIOTALLEVI, *Internet e social network, tra "fisiologia" costituzionale e "patologia" applicativa,* in *Giurisprudenza di merito*, n. 12, 2012.

Direttiva 2000/31/CE, art 15.

Dissenting opinion del Giudice Holmes al primo Emendamento; US SUPREME COURT, *Reno, attorney general of the united states, et al. v. American Civil Liberties Union et al.*, 1997.

Dissenting opinion del Giudice Katzomann, Force v. Facebook, Inc. No. 18-397, 2nd Cir. 2019.

DIZIKES, *study: on twitter, false news travels faster than true stories*, in *MIT News*, 2018.

Do v. America Online, Inc. 783, So. 2d. 1010, 2001, dissenting opinion Judge Lewis.

DUFFY, *Websites that paddles disinformation make millions of dollars in Ads*, in *New Study Fields, CNN*, <<https://222.cnn.com/2019/08/18/tech/adsvertising-disinformation-money-reliable-sources/index.html>> [https://perma.cc/R7KY-28FF].

EDWARDS, *Role and Responsibility of internet intermediaries in the field of copyright and related rights*, 2011.

Enciclopedia Treccani, <<https://www.treccani.it/enciclopedia/blog/ >>.

ESPOSITO, *La libertà di manifestazione del pensiero*, Milano, 1958.

EUROPEAN COMMISSION, *JRC Technical Reports, JRC Digital Economy Working Paper 2018-02, the digital transformation of news media and the rise of disinformation and fake news*, aprile 2018.

Facebook e democrazia, il dibattito dopo le parole di Orlando al Foglio, in *Il Foglio*, 2016, << https://www.ilfoglio.it/politica/2016/12/28/news/facebook-democrazia-orlando-foglio-dibattito-censura-bufale-112766/ >>.

Facebook: comunicazione con più persone e individuabilità della vittima, in *Dir.* FERRARIS, *Postverità e altri enigmi*, Bologna, 2017, pp. 72-76.

FIANDACA, MUSCO, *Diritto penale. Parte speciale*, vol. I, Zanichelli, 2012.

Fields v. Twitter, No. 16-cv-00213-WHO, 2017.

FLAUSS, *The European Court of Human Rights and the Freedom of Expression*, in Indiana law journal, vol. 84, issue 3, 2009.

FLETCHER, CORNIA, GRAVES, NIELSEN, *Measuring the Reach of "Fake News" and Online Disinformation in Europe,* in *Reuters Institute for the Study of Journalism, University of Oxford*, 2018.

FLICK, *Falsa identità su internet*, in *Dir. informaz. e informatica*, 2008.

FOÀ, *Pubblici poteri e contrasto alle fake news. Verso l'effettività dei diritti aletici?,* in *federalismi.it rivista di diritto pubblico italiano, comparato, europeo*, n 11/2020.

FOCARELLI, *Le contromisure nel diritto internazionale,* Milano, 1994.

Force v. Facebook, Inc. No. 18-397, 2nd Cir., 2019.

Force v. Facebook, No. 18-397, 2nd Cir. 2019, p. 25 con nota di PANTAZIS, *Zeran v. America Online, Inc.: Insulating Internet Service Providers from Defamation Liability*, in *Wake Forest L. Rev.*, 1999.

FRIGERIO, *Responsabilità dell'hosting provider: la Cassazione conferma la distinzione tra attivo e passivo,* in *www.filodiritto.it*, 2019.

FRITTS, *Internet libel and communication decency act: how the courts erroneously interpreted Congressional intent with regard to liability of internet service providers*, in *Kentucky Law Journal*, vol. 93, issue 3, 2005.

FUMO, *Bufale elettroniche, repressione penale e democrazia*, in *Media Laws*, 2018.

G7 Declaration on Responsible States behavior in Cyberspace, 11 aprile 2017, <<http://www.esteri.it/mae/resource/doc/2017/04/declaration_on_cyberspace.pdf >>.

GAETA, *La protezione dei dati personali nell'internet of things: l'esempio dei veicoli autonomi*, in *Dir. informaz. e informatica*, fasc. 1, 1.2.2018.

GARZONIO, *Responsabilità degli ISP rispetto al trattamento automatizzato dei dati personali con finalità di comunicazione politica: applicabilità del GDPR alle piattaforme social*, in *Media Laws*, 2019.

GELLI *False recensioni su TripAdvisor: accolta l'azione inibitoria promossa dal ristoratore diffamato*, in *Corr. giur*., 2016.

GENERAL ASSEMBLY, *Group of Governamental Experts of Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/70/174, 22luglio 2015.

GERMANI, *la minaccia della disinformazione: panoramica introduttiva*, in ID. (a cura di), *Disinformazione e manipolazione delle percezioni, Una nuova minaccia al Sistema-Paese*, Roma, 2017.

Gertz v. Robert Welch, Inc, 418 U.S., 1974.

GIACCARDI, *Media, Significato e Realtà Sociale: per un approccio comparativo all'analisi dei testi pubblicitari*, in *Vita e Pensiero*, 1993.

GOLDSMITH, *Cybersecurity treaties: a sceptical view*, in *Hoover Institution at Stanford University*, 2011.

GORODNICHENKO, YURIY, THO PHAM, AND OLAKSANDER TALAVERA, *Social media, sentiment and public opinions: evidence from #Brexit and #USElection*, Working Paper 24631, Cambridge, MA: National Bureau of Economic Reserach, may 2018.

GREY, *The first amendment and the dissemination of socially worthless untruths*, in *Florida State University Law Review*, vol. 36, issue 1, 2008.

GROSS, RENWICK, *Fact-Checking and the EU referendum,* in *Constitution Unit*, 2016.

GROSSO, *Responsabilità penale per i reati commessi col mezzo della stampa*, Milano, 1969.

GUERINI, Fake News *e Diritto Penale, La Manipolazione Digitale del Consenso nelle Democrazie Liberali*, Torino, 2020.

GULLO, *Delitti contro l'onore,* in PIERGALLINI-VIGANÒ, (a cura di), *Reati contro la persona,* Estratto dal VII volume del *Trattato teorico-pratico di diritto penale*, diretto da PALAZZO-PALIERO, Torino, 2015.

GULLO, *Diffamazione e legittimazione all'intervento penale, Contributo a una riforma dei delitti conto l'onore,* Roma, 2013.

GULLO, *Diffamazione e pena detentiva,* in *Diritto penale contemporaneo* (online), 2016.

HABERLE, *Diritto e Verità,* 2000.

HAMILTON, *beyond ballot-stuffing: current gaps in international law regarding foreign state hacking to influence a foreign election*, in *Wisconsin international law journal*, 2017.

HANSEN, JIM, *Doxing Democracy: Influencing Elections via cyber Voter influence*, in *Contemporary politics*, 2018.

HARRIS, O'BOYLE,WARBRICK, *Law on the European Convention on Human Rights*, 4ª ed., Oxford, 2018.

HASEN, *Cheap Speech and What it has done (to american democracy)*, vol. 16, in *first emendament, law Review*, 2017.

HERDEGEN, *Possibile legal framework and regulatory models for enhanced inter-State cooperation*, in *German Yeerbook of International Law*, 2015.

HOUSE OF COMMONS CULTURE, MEDIA AND SPORT SELECTED COMMITTEE, *Disinformation and fake news: interim report*, 2018.

HOWARD, WOOLLEY , CALO, *Algorithms, bots, and political communication in the US 2016 Election: the challenge of automated political communication for law and administration*, in *journal of information technology and politics*, n. 2, 2018.

HUMAN RIGHTS COMMITTEE, *art 19: freedom of opinion and expression*, general comment n. 34, 12 settembre 2011.

HUMAN RIGHTS COMMITTEE, *General Comment n. 25. The right to participate in public affairs, voting rights, and the right to equal access to public service (Art. 25)*, UN Doc. CCPR/C/21/Rev.1/Add.7, 12 luglio 1996.

HUMAN RIGHTS COMMITTEE, *General Comment n. 36 (2018) on Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life*, UN Doc. CCPR/C/GC/36, 30 ottobre 2018.

IASSELLI, *Responsabilità del provider: la Cassazione detta rilevanti principi di diritto*, in <<https://www.altalex.com/documents/news/2019/03/20/diritto-d-autore-responsabilita-dell-hosting-provider>>.

ICJ, Advisory Opinion on the Threat or Use of Nuclear Weapons, 1966.
ICJ, *Armed Activities in the Territory of Congo*, 2005.

ICJ, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America), 1986.

INTERNATIONAL LAW COMMISSION, *Articles on Responsibility of States for Internationally Wrongful Acts*, 2001.

JOHNSON, *Defamation in Cyberspace: A Court Takes a Wrong Turn on the Information Superhighway in Stratton Oakmont, Inc. v. Prodigy Services Co*., in *Arkansas Law Rev*iew, 1997.

Joint Declaration on Freedom of Expression and Fake News, Disinformation and propaganda, Org. Sec and Co-operation Eur, 3 marzo 2017.

KELLER, *Make Google The Censor*, in *New York Times*, 12 giugno 2017.

KIELY, FARLEY, *Fact: Trump TV Ad Misleads on Biden and Ukraine*, in *Factcheck.Org*, 2019, << https://www.factcheck.org/2019/10/fact-trump-tv-ad-misleadson-biden-and-ukraine/>>.

KILOVATY, *Doxfare: politically motivated leakes and the future of the norm on non-intervention in the era of weaponized information*, in *Harvard National Security journal*, 2018.

Klayman v. Zuckerberg, 753, D.C. Circ., 2014.

La notizia più condivisa sul referendum? È una bufala, in *Pagella Politica*, 2016, <<https://pagellapolitica.it/blog/show/148/la-notizia-pi%C3%B9-condivisa-sul-referendum-%C3%A8-una-bufala >>.

LABUNSKI, *The second constitutional convention: how the american people can take back their government*, 2000.

LAM, *a slap on the wrist: combatting Russia's Cyber attack on the 2016 U.S. Presidential election*, in *Boston College law review*, 2018.

Legge Federale russa No. 31-FZ del 2019 e Legge Federale russa No. 27-FZ del 2019.

Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General, U.N. Doc. A/69/723, 13 gennaio 2015.

LEWIS, *multilateral agreements to constraint cyberconflict*, in *arms control today*, 2010.

LOEWENSTEIN, *Militant Democracy and Fundamental Rights*, in *American Political Science Review*, 1937.

LOIODICE, voce *L'informazione (diritto alla)*, in *Enc. dir.*, XXI, Milano, m 197.

LONGO, *Diffamazione via mass media e social network, tutele e risarcimenti*, in *Altalex.*, 2020, <<https://www.altalex.com/documents/news/2020/02/28/diffamazione-via-mass-media-social-network-tutele-risarcimenti>>.

LONGO, *Diffamazione via mass media e social network, tutele e risarcimenti*, in *Altalex.*, 2020, <https://www.altalex.com/documents/news/2020/02/28/diffamazione-via-mass-media-social-network-tutele-risarcimenti>.

LUCARELLI, *Blue Whale, parla Matteo Viviani de Le Iene: "Sì, i video russi sono falsi ma il pericolo c'è"*, in *il fatto quotidiano*, 7 giugno 2018.

MAGNANI, *Libertà di espressione e fakenews, il difficile rapporto tra verità e diritto. Una prospettiva teorica,* in *Costituzionalismo.it*, 2018.

MALGERI, *Il furto di "identità digitale": una tutela "patrimoniale" della personalità,* in *La giustizia penale nella "rete", le nuove sfide della società dell'informazione nell'epoca di Internet,* FLOR, FALCINELLI, MARCOLINI (a cura di), 2015.

MANTOVANI, *Manuale di diritto penale*, parte generale, 10ª ed., Padova, 2017.
MANZINI, *Trattato di diritto penale italiano*, V ed., Torino, 1986.

MANZINI, *Trattato di diritto penale italiano*, vol. VI, Torino, 1983.

MAURI, *Applicabile l'art. 57 c.p. al direttore del quotidiano online: un revirement giurisprudenziale della Cassazione, di problematica compatibilità con il divieto di analogia*, in *DPC*, 2019.

MAZZANTI, *Reati elettorali*, (voce), in *Enc. Dir.,* XIV vol., Milano, 1965.

MCKUNE, *An analysis of the International code of conduct for Information Security*, in *the citizen lab*, 2015.

MEZZANOTTE, *Fake news nelle campagne elettorali digitali. Vecchi rimedi o nuove regole?,* in *Federalismi.it*, 2018.

MICELI, *Profili evolutivi della responsabilità in Rete: il ruolo degli Internet Service Providers tra prevenzione e repressione*, in *Media Laws*, 2017.

MONTI, *Il Code of Practice on Disinformation dell'UE: tentativi in fieri di contrasto alle fake news*, in *Media Laws*, 2019.

MONTI, *Le "bufale" online e l'inquinamento del public discourse*, in PASSAGLIA - POLETTI (a cura di), *Nodi virtuali, legami informali: Internet alla ricerca di regole*, Pisa, 2017.

MONTI, *The New Populism and Fake News on the Internet: How Populism Along with Internet New Media is Transforming the Fourth Estate*, in *StalsResearchPaper*, 2018.

MORTATI, *Istituzioni di diritto pubblico*, vol. II, Padova, 1976.

NARDELLI, SILVERMAN, *Movimento Cinque Stelle Primo In Europa A Diffondere Notizie False E Propaganda Russa*, in *buzzfeddnews.com*, 2016, <<https://www.buzzfeednews.com/article/albertonardelli/movimento-cinque-stelle-primo-in-europa-a-diffondere-notizie >>.

NATIONAL INTELLIGENCE COUNCIL, *Foreign threats to the 2020 US Federal Elections*, 10 marzo 2021.

NATOLI, *La tutela dell'onore e della reputazione in internet: il caso della diffamazione anonima*, in *Eur. dir. priv.*, 2001.

New York Times v. Sullivan, 376, U.S., 1964.

NEWMAN,FLETCHER, KALOGEROPOULOS, LEVY, KLEIS NIELSEN, *Reuters Institute Digital News Report 2017*, in *Reuters institute for the study of journalism*.

NICASTRO, *Libertà Di Manifestazione del Pensiero e tutela della personalità nella giurisprudenza della Corte Costituzionale*, in *CorteCostituzionale.it*, 2015.

NIGRO, *Diritti civili e politici, la responsabilità degli internet service providers e la convenzione europea dei diritti umani: il caso Delfi AS*, in *Diritti Umani e Diritto Internazionale*, 2015, vol. 9, n. 3.

NUÑEZ, *Disinformation legislation and freedom of expression*, in *UC Irvine Law Review*, vol. 10, issue 2, 2020.

OCSE, *Free media against propaganda*, <<https://www.osce.org/fom/319286>>.

OECD Directorate for Science, *Technology and Industry, Committee for Information, Computer and Communications Policy, the role of internet intermediaries in advancing public policy objectives- Forging partnerships for advancing policy objectives for the Internet economy*, Part II, 22 June 2012.

OECD, *The Economic and Social role of internet intermediaries*, aprile 2010.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI), *assessing russian activities and intentions in recent US elections*, ICA 2017.01D, 6 gennaio 2017.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, 2017.

OHCHR, *Freedom of Expression Monitors Issue Joint Declaration on 'Fake News', Disinformation and Propaganda*, 2017.
Organization of American States, Inter-American Commission on Human Rights, Special Rapportuer for Freedom of Expression, *Guide to guarantee freedom of expression regarding deliberate disinfomation in electoral contexts*, 2019.

PADOVANI, *Menzogna e diritto penale*, Pisa, 2014.

PAGALLO, *Cyber force and the role of sovereign States in Informational warfare*, in *philosophy and technology*, n 3, 2015.

Pagella Politica per AGI, *Referendum e fact checking: la notizia più condivisa è una bufala*, in *AGI*, 2016, <<https://www.agi.it/politica/referendum/referendum_e_fact_checking_la_notizia_pi_condivisa_una_bufala-1289280/news/2016-12-02/ >>.

PAGLIARO, voce *Falsità personale*, in *Enc. Dir.*, Milano, 1967.

PALICI DI SUNI, *Fake news e referendum*, in *Federalismi.it*, n. 11/2020.

Palmucci v. Twitter, 18-cv-03947-WHO, N.D. Cal., 2019.

PANATTONI, *Il sistema di controllo successivo: obbligo di rimozione dell'ISP e meccanismi di notice and take down*, in *Dir. pen. cont.*, 2018, n. 5.

PAOLONI, *Le Sezioni Unite si pronunciano per l'applicabilità alle testate telematiche delle garanzie costituzionali sul sequestro della stampa: ubi commoda, ibi et incommoda?*, in *Cass. pen.*, 10, 2015.

PARISER, *The filter bubble. What the Internet is Hiding from you*, New York, 2011.

PARK, YOUM, F*ake news from a legal perspective: The United States and South Korea compared*, in *Southwestern Journal of International Law*, vol XXI, n. 1, 2019.

PARLAMENTO EUROPEO, POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS, *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*, 2019.

PARLAMENTO EUROPEO, *Risoluzione del 15 giugno 2017 sulle piattaforme on line e il mercato unico digitale*, 2016/2276(INI).

PARLAMENTO EUROPEO, Risoluzione sull'adapting commercial and civil law rules for commercial entities operating online, 2020/2019(INL).

PARLAMENTO EUROPEO, Risoluzione sull'Digital Service Act and fundamental right issues posed, 2020/2022(INL).

PARLAMENTO EUROPEO, Risoluzione sull'improving the functioning of the Single Market, 2020/2018(INL).

PARMENIDE, *Sulla Natura*, frammento 1.

PAYNE, *Teaching old law news tricks: applying and adapting State responsibility to cyber operations*, in *Lewis and Clark law review*, n. 2, 2016.

PCA, Islands of Palmas arbitration case (Netherlands v United States of America), 1928.

PCIJ, SS Lotus case (France v Turkey), series A n. 10, 1927.

PCMag, encyclopedia: proxy server <<https://www.pcmag.com/encyclopedia/term/proxy-server >>.

PERINI, *Fake news e Post-Verità tra diritto penale e politica criminale,* in *Dir. pen. cont.*, 20 dicembre 2017.

PERON, *Internet, regime applicabile per i casi di diffamazione e responsabilità del Direttore,* in *Responsabilità civile e previdenza,* n. 1, 2011.

PERRONE, *fake news e libertà di manifestazione del pensiero: brevi coordinate in tema di tutela costituzionale del falso*, in *Nomos le attualità nel diritto*, 2018.

PETRINI, *Diffamazione on line: offesa recata "con altro mezzo di pubblicità" o col mezzo della stampa?*, in *Dir. pen. proc*., 1, 2017.

PICOTTI, *I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali,* in *Giur. mer.*, 2012, n. 12.

PISA, *La responsabilità del direttore di periodico on line tra vincoli normativi e discutibili novità giurisprudenziali*, in *Dir. pen. proc*., 3/2019.

PISAPIA, *La nuova disciplina della responsabilità per i reati commessi a mezzo della stampa,* in *Riv. It. Dir. proc. pen*., 1958.

PITRUZZELLA, *La libertà di informazione nell'era di Internet*, in *media laws*, 1/2018.

PITRUZZELLA, POLLICINO, *Disinformation and Hate Speech a European Constitutial Perspective*, 2020.

PITRUZZELLA, POLLICINO, QUINTARELLI, *Parole e Potere, Libertà di Espressione, Hate Speech e Fake News*, Egea, 2017.

POLLICINO, *La prospettiva costituzionale sulla libertà di espressione nell'era di Internet*, in *Media Laws*, 1/2018 p. 79.

POLLICINO, *Tutela e pluralismo nell'era digitale: ruolo e responsabilità degli Internet service providers*, in *Consulta Online*, 2014.

PRAISER, *Filter Bubble: how the new personalized web is changing what we read and we think*, New York, 2011.

Press Release, White House, *Statement by the president on Actions in Response to Russian Malicious Cyber Activity and Harassment*, 29 dicembre 2016, <<https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity >>.

PROKOP, ANDREW, *All of Robert Muller's Indictments and Plea Deals in The Russia Investigation So Far*, in *Vox*, 2018.

PUENTE, *il grande inganno di internet*, Milano, 2019.

RAITANO, *Le notizie false che cambiano il mondo*, in *Altraeconomia.it*, 1 aprile 2018.

RAMAJOLI, *I pericoli del marketplace of idea. Considerazioni sparse a latere di due sentenze della Corte di Giustizia in tema di assegnazione delle frequenze radiotelevisive*, in *Media Laws*, n. 1/2018.

Rapporto del Consiglio dei diritti umani sulla promozione e protezione del diritto alla libertà di opinione e di espressione, UN Doc. A/HRC/17/27, 16 maggio 2011.

REDAZIONE ALTALEX, *Cybercrime: sostituzione di persona mediante furto di identità digitale*, in *Altalex.*, 2019, <<https://www.altalex.com/documents/news/2019/04/12/sostituzione-di-persona-mediante-furto-di-identita-digitale>>.

REDAZIONE DI DIRITTO.IT, *Oblio: informazione, verità, pertinenza e continenza*, in *Diritto.it*, 2019, <<https://www.diritto.it/oblio-informazione-verita-pertinenza-e-continenza/>>.

Reno, attorney general of the united states, et al. v. American Civil Liberties Union et al., 521 U.S., 1997.

Report of Special Rapporteur on the Promotion and protection of the right to freedom of opinion and expression, Frank la Rue on the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet, A/HRC/17/27, 16 May 2011.

RESTA, *Identità personale e identità digitale*, in *Dir.Informatica*, fasc.3, 2007.

Restatement second of torts, 1977.

Reynaldo Gonzalez v. Twitter Inc., Google Inc. e Facebook Inc.

RICCIO, *La responsabilità civile degli internet providers*, in *Media Laws*, 2012, p. 210; SICA, *Responsabilità del provider: per una soluzione "equilibrata" del problema*, in *Corr. giur*., 2013.

Risoluzione dell'Assemblea Generale 70/237, adottata il 23 dicembre 2015, paragrafo 5, UN Doc. A/RES/70/237.

RODOTÀ, *Il diritto alla verità*, in Il diritto di avere diritti, Bari-Roma, 2012.

RODOTÀ, *Quattro paradigmi per l'identità*, in *Il diritto di avere diritti*, Bari, 2012.

RODRIGUEZ RENGIFO, *Internet Intermediaries Liability: Participative Networking Platforms and Harmful Content*, in *Researchgate.net*, 2016.

RODRIGUEZ, *Disinformation Operations Aimed at (Democratic) Elections in the context of Public International Law: The conduct of the Internet Research Agency during the 2016 US Presidential Elections*, in *International Journal of Legal Information*, 2019.

ROLAND, *Rethinking Defamation Liability for Internet Service Providers*, in *Suffolk University Law Review*, 2001.

RONTALDO, PELUSO, *La tutela del diritto d'autore nel settore audiovisivo e la responsabilità degli ISP*, in *Dir. Autore*, 2015.

SARTOR., *L'intenzionalità degli agenti software e la loro disciplina giuridica*, in *Researchgate.net*, 2002.

SAVARESE, *Dalla Bugia alla Menzogna: la Postverità e l'impossibilità del Diritto,* in *Nomos le attualità nel diritto*, 2018.

SCANNICCHIO, VECCHIO, I *limiti della neutralità: la Corte di giustizia e l'eterno ritorno dell'hosting attivo*, in *www.filodiritto.it*, 2019;

SCHMITT, *In defense of Sovereignty in Cyberspace*, 2018, <<https://www.justsecure.org/55876/defense/>>.

SCHMITT, *Virtual disenfranchisement: cyber election meddling in the grey zone of international law*, in *Chicago journal of international law*, n. 1, 2018, p. 43; WATTS, RICHARD, *Baseline territorial sovreignity and cyberspace,* in *Lewis and Clark Law Review*, n. 3, 2018.

SCHWAB, *The fourth industrial revolution*, in world economic forum, Ginevra, 2016.

SCOPINARO, *Diffamazione via Internet: applicabilità della circostanza aggravante relativa all'uso del mezzo della pubblicità,* in *Riv. It. Dir. proc.*, 2001.

SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE, SENATE, *Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, vol. 5, 116th congress, 1st session.

Senate Report, No. 104-230 para 194.

SHACKELFORD, ANDERS, *State responsibility for cyberattacks: competing standards for a growing problem*, in *Georgetown journal of international law*, 2011.

SHERIDAN, *Zeran v. AOL and the effect of section 230 of the Communications Decency Act upon liability for defamation on the Internet*, in *Albany Law Review*, 1997.

SICA, D'ANTONIO, *Professioni e responsabilità civile*, Bologna, 2006.

SICA, *Il commercio elettronico. Profili giuridici*, Torino, 2001.

SIDERITS, *Defamation in Cyberspace: Reconciling Cubby, Inc. v. Compuserve, Inc. and Stratton Oakmont v. Prodigy Services Co.*, in *Marquette Law Review*, 1996.

Smith v. California 361 U.S. 147, 1959.

SOARES, *The fake news machine: inside a town gearing up for 2020*, in *CNN*, <https://money.cnn.com/interactive/media/the-macedonia-story/> [https;//perma.cc/VW93-G6AF].

SPADARO, *Contributo per una teoria della Costituzione*, 1994.

SPECIAL COUNSEL ROBERT S. MUELLER, III, *Report on The Investigation into Russian Interference In The 2016 Presidential Election*, 2019.

SPECIAL COUNSEL ROBERT S. MUELLER, III, U.S. DEPARTMENT OF JUSTICE, *Report on The Investigation into Russian Interference in the 2016 Presidential Election*, Washington DC, 2019.

Special Eurobarometer 477: *democracy and elections*, <<https://data.europa.eu/euodp/en/data/dataset/S2198_90_1_477_ENG>>.

SPIVAK, *Facebook Immune from Liability Based on Third-Party Content*, in *Lawfare*, 2017; TATE, *Maybe Someone Dies: The Dilemma of Domestic Terrorism and Internet Edge Provider Liability*, in *Boston College Law Review*, 2019.

STAMPANONI BASSI, *Sostituzione di persona commessa nella rete internet*, IN *Cass. pen.*, n. 1, 2014.

Stato dell'Unione 2018, Discorso annuale sullo stato dell'UE pronunciato dal presidente Juncker al Parlamento europeo, 12 settembre 2018,<<https://ec.europa.eu/info/sites/info/files/soteu2018-speech_en_0.pdf>>,<<https://ec.europa.eu/info/priorities/state-union-speeches/state-union-2018_it>>.

STEWART, *Facebook is refusing to take down a Trump and making false claims about Joe Biden*, in *Vox*, 2019,_<< https://www.vox.com/policy-and-politics/2019/10/9/20906612/trump-campaign-ad-joe-biden-ukraine-facebook >>.

Stop alle Fake News su Intagram. Ci pensa una Startup italiana, in *CORCOM*, 29 agosto 2019, <<https://www.corrierecomunicazioni.it/digital-economy/instagram-piu-trasparente-ci-pensa-una-startup-italiana/>>.

Stratton Oakmont, Inc. v. Prodigy Servs Co. No. 31063/94, 1995 N.Y. Misc.

SUFFIA, ZICCARDI, *Fake news guerra dell'informazione ed equilibri democratici,* in *Federalismi.it*, 2020.

SUNSTEIN, *A cosa servono le costituzioni. Dissenso politico e democrazia discorsiva*, Bologna, 2009, pp. 17 e ss; SPADARO, *Contrasto alle fake news e tutela della democrazia,* in *dirittifondamentali.it*, 1/2019.

SUSTEIN, *#republic. La Democrazia all'epoca dei social media*, Bologna, 2017.
Tallinn Manual on International Law applicable to cyber warfare, II edizione, Cambridge University Press, 2017.

TAMBIAMA MADIEGA, Commissione europea, *Briefing EU Legislation in Progress, European Parliamentary Research Service*, Digital Services Act, marzo 2021.

THE UNITED STATES DEPARTMENT OF DEFENCE, OFFICE OF PUBLIC AFFAIRS, *Russian National Charged with Interfering in U.S. Political System*, 19 October 2018, << https://www.justice.gov/opa/pr/russian-national-charged-interfering-us-political-system >>.

TORRISI, ZITELLI, *Blue Whale: la leggenda urbana, gli errori delle Iene e come i media dovrebbero parlare di suicidio,* in *Valigia Blu*, 3 giugno 2017.

TOSI, *Contrasti giurisprudenziali in materia di responsabilità civile degli hosting provider- passivi e attivi- tra tipizzazione normativa e interpretazione evolutiva applicata alle nuove figure soggettive dei motori di ricerca, social network e aggregatori di contenuti*, in *Riv. dir. ind.*, 2017.

TOSI, *Contrasti giurisprudenziali in materia di responsabilità civile degli hosting provider - passivi e attivi - tra tipizzazione normativa e interpretazione evolutiva applicata alle nuove figure soggettive dei motori di ricerca, social network e aggregatori di contenuti*, in *Rivista Di Diritto Industriale*, 2017.

TOSI, *responsabilità civile degli hosting provider e inibitoria giudiziale dei contenuti digitali illeciti equivalenti tra assenza dell'obbligo di sorveglianza ex ante e ammissibilità' ex post*, in *Il diritto degli affari*, n. 1/20.

Tribunale Bari, 13 giugno 2006, in *Dir. internet*, 2006.

Tribunale Bari, Sez. Molfetta, 18 febbraio 2003, n. 23, in *Dir. Giust*., 14 giungo 2003.

Tribunale Catania, 29 giugno 2004, in *Dir. inf*., 2004.

Tribunale Catania, 29 giugno 2004, in *Resp. civ. prev*., 2005, con nota di BUGIOLACCHI, *La responsabilità dell'host provider alla luce del d.lgs. n.70 del 2003: esegesi di una disciplina "dimezzata"*.

Tribunale Firenze, 25 maggio 2012, in *Dir. informaz. informatica*, 2012, con nota di SCANNICCHIO, *La responsabilità del motore di ricerca per la funzione "auto-complete" – che sottolinea come le diffide dei terzi non siano sufficienti a far sorgere, in capo al provider, l'obbligo di intervento, dal momento che si tratta, pur sempre, di prospettive unilaterali*.

Tribunale Milano Sez. XI, pen., ord. 21 giugno 2010, n. 157, in *Guida, dir*., 2010, n. 44.

Tribunale Milano, 2 marzo 2009, caso RTI c. RCS, in *Dir. inf*., 2009.

Tribunale Milano, 25 gennaio 2011, in *Resp. civ. prev*.

Tribunale Milano, 25 maggio 2013, in *Resp. civ. prev*., 2013, p. 119, con nota di BUGIOLACCHI, *Evoluzione dei servizi di hosting provider, conseguenze sul regime di responsabilità e limiti dell'attuale approccio case by case*.

Tribunale Milano, 25 marzo 2013.

Tribunale Milano, 31 marzo 2011, in *Resp. civ. prev*., 2011, con nota di PERON, *Sulla diffamazione commessa tramite motore di ricerca*.

Tribunale Milano, Sez. civ.,16 ottobre 2004, n. 11848, in *Dir. Inf*., 2004.

Tribunale Milano, Sez. Spec. Prop. Ind. e Intellettuale, 7 giugno 2011, n. 7680, caso RTI c. Italia Online (IOL), in *Dir. inf*., 2011.

Tribunale Milano, Sez. Spec. Prop. Ind. e Intellettuale, 7 giugno 2011, in *Dir. inf*., 2011.

Tribunale Milano, sez. spec. prop. ind. e intellettuale, 9 settembre 2011, n. 10893, in *Riv. dir. ind*., 2012, con nota di SARACENO, *Note in tema di violazione del diritto d'autore tramite Internet; la responsabilità degli Internet service provider*.
Tribunale Monza, Sez. IV civ., 2 marzo 2010, n. 770, in *www.dejure.it.*

Tribunale Napoli Nord, 10 agosto 2016.

Tribunale Napoli Nord, sez. civ., II, 3 novembre 2016, in *Giur. it*., 2017, con nota di BOCCHINI, *La responsabilità di Facebook per la mancata rimozione di contenuti illeciti*; Tribunale. Torino, sez. impr., 7 aprile 2017, n. 1928, in *Danno resp*., 2018.

Tribunale Napoli, Sez. II, civ., ord., 4 novembre 2016, n. 9799.

Tribunale Padova, ord., 1 ottobre 2009, in *Foro.it*., 2009, I, 3225.

Tribunale Pescara, 5 marzo 2018, n. 652, in *www.dejure.it*.

Tribunale Pinerolo, 30 aprile 2012.

Tribunale Pistoia, 16 dicembre 2015, n. 5665, in *www.dejure.it.*

Tribunale Roma, 11 febbraio 2010, in *Dir. inform. e informatica*, 2010.

Tribunale Roma, 11 febbraio 2010, reclamo caso RTI c. You Tube, in *Dir. inf.*, 2010.

Tribunale Roma, 11 luglio 2011, PFA Film s.r.l. c. Google Italia s.r.l. e Yahoo! Italia Inc.

Tribunale Roma, 15 dicembre 2009, caso RTI c. You Tube, in *Dir. inf.*, 2009.

Tribunale Roma, 16 dicembre 2009; Tribunale Roma, 11 febbraio 2010.

Tribunale Roma, 17 agosto 2011; Cass. pen., sez. III, 3 febbraio 2014, n. 3672, in *www.dejure.it*.

Tribunale Roma, 5 maggio 2016, n. 24707, RTI Italia c. Kit Digital France.

Tribunale Roma, sez. impr., 27 aprile 2016, n. 8437, in *Riv. dir. ind.*, 2017.

Tribunale Torino, 11 giugno 2020.

Tribunale Torino, 23 giugno 2014, in *www.marchiebrevettiweb.it*.

Tribunale Trani, 14 ottobre 2008, in *Danno resp.*, 2009.

Tribunale. Milano, 20 gennaio 2011, n. 7680, in *Dir. ind.*, 2012, con nota di BELLAN, *Per una reasonable liability: critiche alla responsabilità oggettiva dei provider e tutela dei diritti su internet*; Tribunale Torino, 5 maggio 2014, in *www.marchiebrevettiweb.it*.

Tribunale. Napoli Nord, sez. II civ., 3 novembre 2016.

TUCKER, GUESS, BARBERÁ, VACCARI, SIEGEL, SANOVICH, STUKAL,NYHAN*Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature*, 2018.

U.S. Supreme Court, *Packingham v North Carolina*, 582 U.S., 2017, pp. 1730, 1736.

US Court of Appeals for the District of Columbia Circuit, *Liberty Lobby, Inc. v. Dow Jones e Co*., 823 F.2d, 1988.

VAN DE VELDE, *The law of cyber interference in elections*, in *Yale Law School*, 2017.
VAN DE VELDE, *The law of cyber interference in elections*, in *Yale Law School*, 2017.

VIGEVANI, Sub *art 49*, in BARTOLE, BIN (a cura di), *Commentario Breve della Costituzione*, Padova, 2008.

VOSOUGHI, ROY, ARAL, *the spread of true and false news online*, in *Science*, 2018.
WALTON, *Duties owed: low intensity cyberattacks and liability for transboundary Torts in international law*, in *Yale law journal*, 2017.

WANLESS, *How Europe Can Tackle Influence Operations and Disinformation*, in *Carnegie Europe*, 2021.

Whistleblower: Cambridge Analytica shared data with Russia, *Euractive.com*, 2018.

WOOLLEY AND HOWARD, *computational propaganda worldwide: Executive Summary, computational propaganda research project*, working paper n. 2017.11, 2017.

ZAFESOVA, *Istigazioni 'social' al suicidio, panico in Russia per le chat della morte. Ma è solo un brutto scherzo*, in *LaStampa*, 4 giugno 2016.

ZENCOVICH, *Il diritto di essere informati quale elemento del rapporto di cittadinanza, in il diritto dell'informazione e dell'informatica*, n. 22/2006.

Zeran v. America Online, Inc. 129 F. 3d, 4th Cir., 1997.

ZICCARDI, *Furto di identità*, in *Dig. Disc. Pen*., IV, Torino, 2011.

ZICCARDI, *Tecnologie per il potere*, Milano, 2019.

ZIEGLER, *Domaine Réservé,* in *Oxford Public International Law*, 2013.