ApertaContrada
RIFLESSIONI SU SOCIETÀ, DIRITTO, ECONOMIA

di **Giancarlo Pennetti**
pubblicato il 02/11/2026

Giancarlo Pennetti, La libertà di espressione del pensiero *on line*. Disinformazione e rischi per la democrazia fra digitale ed AI.

1. La libertà di manifestazione del pensiero nella dimensione del digitale.

La crisi della democrazia costituzionale nell'ordinamento nazionale e negli altri paesi europei e negli U.S.A. tocca inevitabilmente anche il tema della libertà di manifestazione del pensiero e della disinformazione *on line* con i connessi rischi per l'assetto democratico. Anche nell'ambito degli studi sul cd. costituzionalismo digitale, cioè inerenti l'impatto che la tecnologia digitale ha sui valori e principi costituzionali, trova peculiare risalto il tema della libertà di manifestazione del pensiero quale diritto fondamentale e pilastro della democrazia, della quale condivide l'attuale fase di crisi[1].

[1] cfr. D. Scopelliti, *Poteri privati e responsabilità pubbliche dei social network al tempo della democrazia digitali* in federalismi.it n.7/2024, pag. 242 che definisce il costituzionalismo digitale un movimento di pensiero volto ad estendere le garanzie degli individui e le tecniche di limitazione del potere proprie del costituzionalismo moderno ai giganti della rete. In questa falsariga si sviluppa pure il pensiero di O. Pollicino in *Costituzionalismo digitale- Pensare la democrazia al tempo dell'I.A.,* Bologna, 2025, secondo cui il costituzionalismo, tradizionalmente argine agli abusi dei poteri pubblici, soprattutto statali, oggi deve fare i conti con poteri privati sempre più forti -in competizione con quelli pubblici- quali quelli digitali, piattaforme, fornitori di infrastrutture e sviluppatori di sistemi di intelligenza artificiale, capaci di influenzare la società in forme addirittura superiori a quello di molte autorità pubbliche. Il costituzionalismo digitale deve quindi <<ricondurre anche questi nuovi poteri entro un orizzonte di responsabilità costituzionale, imponendo vincoli sostanziali, diritti fondamentali, principio di proporzionalità, non discriminazione, e procedurali, come trasparenza, *accountability*, possibilità di contestazione>>. Infatti, <<l'architettura tecnica è già una forma di normatività e lasciarla priva di limiti equivale ad accettare una zona franca del potere>>, tanto più in presenza di quel moltiplicatore di rischio rappresentato dalla intelligenza artificiale. Di qui la necessità d'un costituzionalismo capace di anticipare gli abusi e non solo di reagire ad abuso perpetrato (cfr. intervista dell'autore a Il Dubbio del 29 gennaio 2026).

La libertà di espressione - nata come classica libertà negativa, poiché lo Stato non avrebbe potuto ingerirsi nell'esercizio della stessa da parte dei cittadini[2] - ha poi palesato, in ragione della sua natura funzionale alla realizzazione del principio democratico, una struttura circolare, acquisendo sempre più i caratteri di una libertà positiva. Essa infatti innesca un dialogo che va a beneficio non solo del singolo che esprime il proprio pensiero ma anche dell'intera società[3]. In quest'ottica, la libertà di espressione è dunque "garanzia sociale" di partecipazione e integrazione culturale: non solo del diritto di esprimersi qui si tratta, ma anche del diritto ad utilizzare ogni mezzo disponibile[4], ivi inclusa la rete, nonché del diritto ad essere informati[5], quale presupposto imprescindibile per il funzionamento del meccanismo rappresentativo.

Nei decenni ormai alle nostre spalle *Internet* si è affermato come strumento fondamentale di esercizio della libertà di espressione, intesa sia come libertà di informare e sia come libertà di informarsi grazie alla possibilità di accesso a informazioni plurali e diversificate. Ne è derivata una estensione degli spazi di

[2] Da cui il comma 1 dell'art. 21 della Costituzione che recita: *Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto ed ogni altro mezzo di diffusione*.

[3] cfr. V. Capuozzo e A. Tacente, *Uno sguardo comparato tra Spagna ed Italia in materia di sovranità digitale e libertà di espressione on line* in Interferenze digitali, sicurezza e diritti-Tra diritto internazionale e diritto interno, pag. 433- 434, Napoli, 2025; G. AMATO, voce *Libertà* (diritto costituzionale) in Enciclopedia del Diritto, Milano, 1981 pagg. 285 e 286; Esposito C. *La libertà di manifestazione del pensiero nell'ordinamento italiano*, in Rivista italiana per le scienze giuridiche, 1958, pagg. 49 e ss.

[4] cfr. F. Casarosa, *Libertà di espressione e contrasto ai discorsi d'odio, Handbook sulle tecniche di interazione giudiziale nell'applicazione della Carta dei diritti fondamentali dell'UE*, European University Institute, 2020, p. 3.

[5] La Corte costituzionale ha in più occasioni sottolineato come l'art. 21 della Costituzione riconosce e garantisce la libertà di manifestare il proprio pensiero con qualsiasi mezzo di diffusione, specificando che «tale libertà ricomprende tanto il diritto di informare, quanto il diritto di essere informati» (Corte costituzionale, sentenza n. 112 del 1993, punto 7 del considerato in diritto) nonchè le pronunce nn. 202 del 1976, 148 del 1981 e 826 del 1988.

discussione pubblica e di partecipazione democratica. Questo processo di ampliamento del "digitale" ha tuttavia portato ad un mutamento dello spazio pubblico e dei rapporti tra potere pubblico, soggetti privati e diritti i quali -in ragione dell'emersione del problema, divenuto via via più imponente, delle modalità di gestione dei contenuti *on line*- sono diventati più vulnerabili a causa della messa in discussione delle garanzie da cui sembravano stabilmente assistiti. Come è stato rilevato[6], i problemi toccano in generale la discussione pubblica *on line* e più in particolare le piattaforme che consentono l'accesso e la circolazione -con modalità virali- di informazioni. Parliamo della necessità di contemperare la libertà di espressione con la salvaguardia di altri diritti fondamentali e in definitiva del cuore stesso del processo democratico, del suo farsi e della conseguente necessità di assicurare a tutti sia la libera formazione di un convincimento personale e sia la -altrettanto libera- possibilità di dissentire. Questa dunque la sfida davanti a cui gli ordinamenti democratici si trovano per effetto del tumultuoso sviluppo scientifico e tecnologico in atto: piattaforme, motori di ricerca, social network infatti collegano chi esprime il proprio pensiero o informazioni e colui che le riceve.

2. I nuovi guardiani del cyberspazio, piattaforme social, condizionamento algoritmico ed AI.

I nuovi guardiani del cyberspazio controllano le porte di accesso alle informazioni presenti in rete, regolano e filtrano con i propri algoritmi il flusso dei dati imponendo

[6] cfr. G. Pitruzzella, *Il Costituzionalismo digitale tra Stati Uniti e Europa* in Unione Europea e diritti, fasc. n.2 del 2025, pagg. 1-2 nonché M. Ferrario, *Piattaforme digitali e interferenze statali: la tutela della libertà di espressione al vaglio della Corte EDU* in DPCE online n.3 del 2025, pagg. 1541-1542.

al medesimo l'ordine da essi unilateralmente stabilito[7]. Un ristretto numero di privati, gestori dei nuovi strumenti tecnologici rimuove, seleziona ed organizza questo flusso dei contenuti e può amplificare o attenuare la rilevanza di opinioni e informazioni stabilendone o negandone la priorità, il tutto tenendo ben presente il proprio interesse al profitto d'impresa, specialmente con riguardo ai contenuti pubblicitari. Trattasi di poteri privati che, per effetto della forza economica posseduta, incidono sulle libertà fondamentali dei singoli.

Le piattaforme e i motori di ricerca promuovono la profilazione individuale mediante algoritmi di conferma che, sulla base dei precedenti accessi e contatti posti in essere dall'utente creano le cc.dd. *echochambers*. Ovviamente, la continua esposizione ad un solo atteggiamento di pensiero, polarizza - radicalizzandole - le posizioni e - liberate da qualsiasi contraddittorio - le *fake* dilagano nel gruppo. Si realizzano così comunità chiuse nelle proprie opinioni e certezze: una tribalizzazione delle opinioni. Sono i fenomeni patologici della disinformazione, del condizionamento algoritmico dei contenuti e della polarizzazione della discussione pubblica. Più recentemente poi la disinformazione ha trovato ulteriore linfa nello sviluppo e diffusione dei sistemi di AI "generativa" (*machine learning* e *deep learning*). Tali sistemi creano immagini, video, testi molto realistici in grado di dar vita a *deepfake* altamente disinformanti, la cui diffusione e uso può pregiudicare i processi democratici. Spesso la diffusione è affidata alla creazione di falsi *account* gestiti in modo automatizzato col preciso obiettivo di diffondere non solo materiali disinformanti ma anche "discorsi d'odio". Sotto altro profilo, la diffusione si basa sul ruolo della AI nel contesto della gestione

[7] cfr. A. Lamberti *La libertà di manifestazione del pensiero "in trasformazione"* in Riv. A.I.C. fasc. n.3/2025, pag. 340 nonché cfr. M.E. Bucalo, *La libertà di espressione: nuovi limiti e nuovi controlli* in www.treccani.it, 2023, paragrafo 2.

dei contenuti operata dalle piattaforme digitali. Questi sistemi, tipici dei *social network*, sono detti di "raccomandazione", perché sulla base di dati e informazioni raccolte sulle preferenze di ciascun utente, ne predicono il gradimento con riferimento a nuovi contenuti ed elementi. Si garantisce così all'utente di ricevere i contenuti più rispondenti ai propri valori, al proprio orientamento ideologico e politico. Tali sistemi giocano un ruolo centrale in generale nella diffusione delle informazioni e perfino nella formazione della stessa coscienza pubblica poiché influenzano e strutturano le preferenze degli utenti e ne orientano le scelte a livello sia individuale e sia collettivo[8].

[8] cfr. O. Pollicino e P. Dunn*, Disinformazione e intelligenza artificiale nell'anno delle global elections: rischi (ed opportunità)* in federalismi.it n.12/2024, pagg. 4-7. Per questi AA. è opportuno definire la nozione di disinformazione precisando anzitutto che quella scelta, a suo tempo, dall'*High Level Group on fake news and online disinformation* (HLEG) istituito dalla Commissione europea, abbraccia tutta una serie di modalità che le piattaforme pongono in essere al fine di plasmare il convincimento personale. Le espressioni *fake news* o *deepfake* sono state a suo tempo ritenute inadeguate dall'HLEG dato che la disinformazione comprende tutte quelle forme di manifestazione della libertà di espressione che si sostanziano di quelle informazioni false, inaccurate o fuorvianti, artificiosamente create, le quali siano presentate e diffuse con lo scopo precipuo di trarre un profitto di carattere economico, politico o ideologico e/o di provocare un danno a livello pubblico, ivi inclusa l'ingerenza nei processi elettorali e democratici. Così intesa, la nozione di disinformazione include non tanto quelle condotte che l'ordinamento riconosce come apertamente illecite (p.e. la diffamazione o la calunnia), ma, piuttosto, tutti quei casi in cui la produzione e diffusione di contenuto falso non integra, di per sé, una fattispecie illecita ma produce, comunque, un potenziale danno ai principi e valori democratici. Questi ultimi sono i casi più delicati per il legislatore nazionale ed europeo, in quanto impongono la necessità di contemperare gli interessi pubblici al corretto funzionamento dello stato democratico con la necessità di non arrecare uno sproporzionato nocumento alla libertà individuale dei consociati a porre in essere condotte che l'ordinamento ritiene, di per sé, lecite. Papa Leone XIV con la recente, importante lettera enciclica del maggio del corrente anno *Magnifica Humanitas -Sulla custodia della persona umana nel tempo dell'intelligenza artificiale* ha condannato l'uso delle piattaforme digitali e dei sistemi di AI "per costruire narrazioni distorte e confondere i confini tra vero e falso, mescolando dati ed opinioni" (capitolo IV, "La verità come bene comune" punto 132 "Verità e democrazia"). Il Pontefice rileva come la possibilità di "manipolare contenuti, immagini e filmati espone i cittadini a prospettive parziali o fuorvianti" e che

3. Le tutele della libertà di espressione, in particolare di quella *on line:* trattati, giurisprudenza, regolamenti europei, diritto interno.

Quanto alle tutele, a livello europeo il diritto alla libertà di espressione è stato positivamente dichiarato prima nel trattato di Maastricht, mediante rinvio ai diritti garantiti dalla Convenzione europea dei diritti dell'Uomo, in particolare all'art. F n.2 del titolo I tra cui è compreso quello alla libertà di espressione. Poi, con il Trattato di Lisbona, ha assunto valore di trattato anche la Carta dei diritti fondamentali dell'Unione Europea che, all'art. 11, paragrafo 2, sancisce il diritto alla libertà di espressione, inclusa la libertà di ricevere o di comunicare informazioni e idee con esclusione della possibilità di ingerenza da parte delle autorità pubbliche e senza limiti di "frontiera". Si prescrive pure che la libertà dei media e il loro pluralismo siano rispettati. L'art. 52 della Carta stabilisce che eventuali limitazioni alla libertà d'espressione e diffusione di informazioni sul *web* vanno introdotte con legge e nel rispetto del principio di proporzionalità; ciò affinché detta libertà sia in equilibrio con

ciò tocca la dimensione culturale e morale "poiché la qualità della comunicazione pubblica dipende direttamente dalla fiducia sociale e incide su di essa". La verità dei fatti, nel discorso pubblico, non si fonda solo sul riscontro delle fonti e sulla responsabilità argomentativa ma anche e ancor più sulla relazione, sui legami fiduciari e pratiche condivise nell'onesto confronto con gli altri. Per il Pontefice, solo la ricerca condivisa della verità dei fatti, quale vero e proprio "bene comune", può fondare una comunicazione giusta. Di qui il ripudio del "puro potere privo di verità" che impone, ora scopertamente, ora sottilmente, ciò che vuole che gli altri considerino vero, così trascurando di considerare che solo la consapevolezza della sacralità e inviolabilità di ogni essere umano -maturata dalla ragione e dalla coscienza- fonda la verità (punto 133 dell'Enciclica). Questa enciclica si colloca in continuità con la Dottrina sociale della Chiesa e -pur priva di potere normativo diretto- contribuisce alla definizione di principi condivisi e alla delineazione dei profili di responsabilità tecnologica. Cfr. S. Attolini, *L'enciclica Magnifica Humanitas e la governance globale dell'I.A.: autorità morale e normatività non coercitiva,* in federalismi.it del 16 settembre 2026.

gli altri valori costituzionali[9]. La giurisprudenza della Corte di giustizia dell'U.E., a sua volta, ha sempre considerato la libertà di espressione come uno dei principi fondamentali dell'ordinamento giuridico europeo e –nelle materie della *privacy*, del diritto d'autore, del diritto all'oblio- nelle proprie pronunce, ha bilanciato le esigenze di protezione di tali interessi e della libertà di espressione operando secondo la tecnica del caso per caso, evitando rigide gerarchie predeterminate fra diritti. A livello di Convenzione Europea dei Diritti dell'Uomo, poi, la protezione della libertà di espressione ha trovato collocazione nell'art. 10 della Convenzione. Fatte salve le restrizioni previste dalla legge (relative ai settori della sicurezza nazionale e dell'amministrazione della giustizia), il diritto alla libertà di espressione e alla ricezione e diffusione delle informazioni viene pertanto garantito. Poiché l'art. 52 della carta di Nizza stabilisce che i diritti in essa previsti coincidono con quelli garantiti dalla CEDU, il significato e la portata sono identici a quelli della Convenzione e ne consegue che, in caso di conflitto fra più libertà, è necessario il bilanciamento perché la CEDU non gerarchizza i diritti che prevede[10].

Nel solco di questa giurisprudenza, l'U.E. ha preso pertanto ad occuparsi sul piano regolatorio del nuovo spazio digitale di esercizio della libertà di manifestazione del pensiero, in tal modo palesando la volontà di andare oltre i sistemi autonomi di moderazione posti in essere dai privati fondati su codici di condotta e strumenti algoritmici recanti meccanismi di segnalazione (*flagging*) al fine di individuare e eventualmente rimuovere contenuti non in linea con i propri *standards*. In una prima

[9] cfr. R. Mastroianni, *I nuovi confini della libertà di informazione nel diritto dell'Unione europea,* in Rivista A.I.C. n.3/2025, pag. 234 e ss.
[10] cfr. V. Capuozzo e A. Tacente, *Uno sguardo comparato tra Spagna ed Italia in materia di sovranità digitale e libertà di espressione on line*, op. cit. pagg.434 e ss.

fase dunque il regolatore eurounitario ha introdotto regole ispirate a strumenti di *soft law* -quali il Codice di Condotta di contrasto all'incitamento all'odio del maggio 2016 sottoscritto da diverse piattaforme e le Linee Guida sulla disinformazione elaborate in occasione della pandemia da Covid-19 del giugno 2020- entrambi esempi di co-regolamentazione e collaborazione volontaria con i privati operatori. In una seconda successiva fase il regolatore eurounitario ha poi fatto ricorso anche a strumenti di *hard law* e cioè ad atti normativi vincolanti destinati a disciplinare le responsabilità delle piattaforme[11] pervenendo prima all'adozione del Regolamento (UE) 2022/1925 del Parlamento Europeo e del Consiglio, del 14/9/2022, noto come *Digital Services Act* (DSA) e del Regolamento (UE) 2022/2065 del Parlamento Europeo e del Consiglio, del 14/10/2022, noto come *Digital Markets Act* (DMA) ed infine, nel 2024, al Regolamento U.E. 2024/1689 del Parlamento europeo e del Consiglio, il cd. *AI Act*. Mentre quest'ultimo regolamento assicura la concorrenza rispetto ai mercati digitali e quindi delle stesse piattaforme, il primo invece ha rappresentato forse la risposta più seria della U.E. volta a rendere più sicuro lo spazio digitale. Il DSA ha apprestato strumenti di contrasto al potere delle piattaforme di maggiori dimensioni, fissando altresì un quadro di norme per le piattaforme *on line* a protezione della libertà di espressione e stabilendo obblighi -estesi anche al contrasto alla disinformazione a fini elettorali- di trasparenza e responsabilità in funzione di moderazione dei contenuti illeciti; ciò al fine di impedire o porre fine alla trasmissione di contenuti illegali. Viene fissato un dovere di diligenza per un ambiente *on line* trasparente e sicuro ed il *provider* diventa responsabile per i contenuti pubblicati con l'onere di provare l'assenza di responsabilità a suo carico. Vengono previsti pure rimedi azionabili dagli

[11] Cfr. M. Ferrario, *Piattaforme digitali e interferenze statali: la tutela della libertà di espressione* etc., op. cit. pagg. 1541-1542.

utenti avverso le decisioni delle piattaforme. Tale intervento regolatorio ha rappresentato un recupero di presenza del ruolo delle istituzioni politiche sovranazionali, al fine di evitare che le piattaforme *on line*, benché soggetti privati, di fatto esercitassero a proprio piacimento poteri sostanzialmente pubblicistici. Vi è però chi[12], nel citato approccio regolatorio finalizzato alla moderazione dei contenuti in rete, ha visto una nuova declinazione del costituzionalismo digitale che cerca di risolvere i problemi di opacità frequentemente presenti nei meccanismi algoritmici propri dei nuovi poteri attraverso soprattutto la predisposizione di garanzie procedurali, cioè di nuovi obblighi in materia di dovere di diligenza per un ambiente *on line* trasparente e sicuro[13]. Ad esempio, a carico delle piattaforme *on line* e per i motori di ricerca molto grandi vengono fissati obblighi "avanzati" e "speciali" (vedi artt. 34-35 DSA) di identificazione e mitigazione dei rischi di sistema conseguenti alla diffusione di contenuti illegali, alla tutela dei diritti fondamentali e all'integrità del dibattito democratico, imponendo a tali soggetti di adattare gli algoritmi al fine di limitare la diffusione di contenuti illeciti senza pregiudizio alcuno dei diritti fondamentali. Si cerca cioè di costituzionalizzare il potere privato, che incide direttamente sui processi democratici senza essere sottoposto ai controlli tradizionali, esercitato dai giganti del digitale al fine di adeguarne l'impatto, nell'ecosistema digitale, alla tutela dei valori democratici e dello stato di diritto[14]. Il

[12] cfr. O. Pollicino, *Di cosa parliamo quando parliamo di costituzionalismo digitale?* in Quaderni costituzionali, 3, 2023, pagg. 569-594.
[13] cfr. O. Pollicino, *Regolazione e innovazione tecnologica nell'ordinamento della rete* in Rivista A.I.C. n.2/2025, pagg.149 e 152.
[14] cfr. O. Pollicino, *Regolazione e innovazione tecnologica nell'ordinamento della rete* op. cit. pag.155. L'autore richiama i principi di non negoziabilità dei diritti fondamentali che i poteri digitali sono giuridicamente obbligati a rispettare. Il costituzionalismo digitale europeo non parte dalla neutralità tecnologica bensì dalla centralità della persona, dalla dignità e dall'eguaglianza sostanziale (vedi intervista citata alla nota 1).

DSA sembra per un verso aver introdotto una prima responsabilizzazione trasversale delle piattaforme e per altro verso però, con esso, si prevedono per lo più misure di amministrativizzazione dell'esercizio del potere privato lasciando tuttavia alle piattaforme una certa mano libera nel decidere quali contenuti possano circolare o meno e dal potere attribuito alle stesse, in entrambi i casi, di rimuovere o limitare i contenuti, senza dover passare attraverso alcun vaglio né giurisdizionale né di altra sede istituzionale titolata al bilanciamento con i diritti fondamentali dei cittadini, imposto invece alle autorità pubbliche quando adottano provvedimenti aventi effetti del tutto analoghi[15].

Anche il Regolamento 1689/2024 (*AI Act*)) stabilisce un quadro giuridico di sviluppo, immissione sul mercato, messa in servizio e uso di sistemi di AI volto a promuovere un'intelligenza artificiale antropocentrica e affidabile con divieto di pratiche di potenziale impatto negativo sui diritti fondamentali (art. 5), l'imposizione di *standards* di trasparenza (art. 13) e obblighi di vigilanza (art. 25). Il modello di responsabilità delineato si sostanzia sul principio della valutazione preventiva del rischio in funzione anticipatoria di successivi interventi normativi[16]. Per completezza va comunque segnalato che il Consiglio della Unione Europea, di recente, con il cd. Pacchetto *Digital Omnibus on AI* ha approvato un regolamento che razionalizza e

[15] cfr. sul punto, A. Lamberti, *La libertà di manifestazione del pensiero "in trasformazione"*, op. cit. pagg. 341 e ss.

[16] cfr. L. Califano in *La strategia normativa della U.E. per un nuovo ordine digitale* in federalismi.it n.15/2025, pagg. 14 e ss. Indirettamente l'AI Act è andato a disciplinare una materia che è la vera nuova frontiera della disinformazione elettorale dato che l'intelligenza artificiale offre immense possibilità per esempio di produzione di contenuti deepkfake. Infatti la classificazione introdotta dall'AI Act i sistemi volti a influenzare l'esito di elezioni, referendum e comportamenti di voto rientrano nella fascia di rischio più alta (sul punto cfr. L. De Carlo, *Il contrasto alla disinformazione nei procedimenti elettorali: studi comparatistici tra Italia e Spagna* in in Disinformazione digitale, Modelli algoritmici e valori democratici op. cit. pag.285).

semplifica alcune norme relative all'intelligenza artificiale, apportando modifiche al l'*AI Act*. In particolare la data di entrata in vigore per le disposizioni relative ai sistemi di AI ad alto rischio ai sensi dell'Allegato III dell'AI Act, fissata per il 2 agosto 2026, è stata posticipata almeno di un anno e mezzo (al 2 dicembre 2027) proprio relativamente alle applicazioni dell'AI più "sensibili", perché capaci di incidere su salute, sicurezza e diritti fondamentali delle persone[17].

Sul versante del diritto interno, poi, a parte la summenzionata disposizione costituzionale e il limite esterno del buon costume (art. 21 comma 6 Cost.), vale ricordare come la giurisprudenza costituzionale pur tutelando la libertà d'espressione -ritenuta un diritto assolutamente fondamentale ed inviolabile[18]- la abbia però sempre bilanciata con gli altri beni e interessi garantiti dalla Costituzione, quali la reputazione, l'onore, la riservatezza, la tutela dei minori o il segreto di Stato e quello giudiziario. La Corte Costituzionale ha poi adattato l'interpretazione dell'art. 21 Cost. all'evoluzione tecnologica estendendo progressivamente la tutela della libertà di espressione in via ordinaria prima a tutti i mezzi di comunicazione di massa (stampa, televisione, cinema etc.) e poi a quella sul *web*. Anche la giurisprudenza ordinaria ha intrapreso un percorso di confronto con le implicazioni della libertà di espressione del

[17] cfr. P.L. Pisa, *Intelligenza artificiale. Slittano le regole UE sulle app ad alto rischio. Ora mancano i capitali* in "La Repubblica A&F" del 29 giugno 2026, pag.13. Più specificatamente, il 2 agosto è rimasto fermo come data di avvio dell'efficacia degli obblighi di trasparenza verso il pubblico presidiati dall'art. 50 AI Act (vedi nota n.33) e del pari il 2 agosto si attiva anche il sistema sanzionatorio. Relativamente ai sistemi ad alto rischio, per via del tempo richiesto per convertire i requisiti generali in specifiche tecniche operative, si è stabilito il rinvio al 2 dicembre 2027 per i casi dell'allegato III, tra cui istruzione, lavoro, credito e giustizia e al 2 agosto 2028 per i sistemi incorporati in prodotti già regolati come i dispositivi medici e le macchine (fonte: www.agendadigitale.eu del 30 luglio 2026).

[18] Corte cost., sent. n. 126/1985; Corte cost., sent. n. 168/1971.

pensiero nello spazio *on line* adattando i principi tradizionali alle nuove tecnologie e ai nuovi diritti emergenti[19]. Infine, con norme statali anche di recepimento di specifiche direttive europee, il Legislatore è intervenuto sulla protezione della reputazione *on* line, sulla tutela della riservatezza e sulla regolazione dei contenuti digitali, sulla tutela dei minori dal cd. cyberbullismo (L. n.71/2017 modificata con L. n.70/2024 e D. Lgs. n.123/2023 e D. Lgs. n.99/2025) e sull'adeguamento del Codice della Privacy (d. Lgs. n.196/2003), al Regolamento UE sulla protezione dei dati *(General Data Protection Regulation- GDPR*) n.679 del 2016[20] avvenuta col decreto legislativo n.101 del 2018 ed è stata pure creata, con D.L. n.82/2021, l'Agenzia per la Cybersicurezza Nazionale (ACN) a tutela degli interessi nazionali nel cyberspazio[21].

[19] Cfr. Così V. Capuozzo e A. Tacente, *Uno sguardo comparato tra Spagna ed Italia in materia di sovranità digitale e libertà di espressione on line*, op. cit. pagg.448 e ss. che ricordano Cass., sez. III n. 6902/2012 che ha esteso alle informazioni sul *web* l'applicazione dei principi sui parametri di verità, continenza e pertinenza per il diritto di cronaca, che discende dalla libertà di espressione nonché Sezioni Unite Penali della Corte di Cassazione n. 23469/2016 che hanno ulteriormente chiarito che le manifestazioni *online*, pur ricadendo nell'ambito di protezione dell'art. 21 Cost., devono rispettare i limiti posti dal sistema dei diritti fondamentali.

[20] Secondo L. Durst, *Oltre la disinformazione: il problema della manipolazione nel quadro della regolazione algoritmica europea* in Disinformazione digitale, Modelli algoritmici e valori democratici a cura di L. Califano, F. Fabrizzi e G. Sartor, Milano 2026, pagg. 84 e 85, l'importanza del GDPR consiste nel fatto che dalla sua disciplina si ricavano tutti i "principi costituzionali" regolatori della società digitale: principi di *accountability* (responsabilizzazione dei soggetti che trattano dati/servizi), dell'approccio *by-design* e *by-default* (integrare la tutela dei dati personali fin dalla progettazione di un sistema e per impostazione predefinita, devono essere trattati esclusivamente i dati personali necessari per la specifica finalità del trattamento e per il periodo strettamente necessario, garantendo inoltre la non eccessività di tutti i dati raccolti), del principio di trasparenza, della valutazione di impatto sui diritti fondamentali e del rischio connesso, della supervisione umana (o *human in the loop*) e dei diversi diritti riconosciuti al soggetto. In questo regolamento, pur mancando richiami espliciti a forme di manipolazione, ha cruciale rilievo l'art. 4 che reca la definizione di "profilazione" e l'art. 22 dal quale è possibile dedurre il cd. principio "di non esclusività" della decisione algoritmica.

[21] Secondo alcuni autori che hanno approfondito i temi della funzione pubblica di cybersicurezza, anche se la disinformazione non è di per sè un attacco informatico può però essere strumentale a garantire l'efficacia dell'attacco. Le strategie di disinformazione, se volte ad accrescere la *human*

Sempre con riferimento al nostro diritto interno deve necessariamente essere segnalata la Legge Statale del 23/09/2025 n.132 (Disposizioni e deleghe al Governo in materia di intelligenza artificiale). Sulla scia delle previsioni dell'AI *Act* e ponendosi in una posizione non attuativa ma semmai integrativa dello stesso, essa ha introdotto nuove figure di reato e aggravanti volte a contrastare inedite forme di aggressione ai beni giuridici realizzate con lo strumento dell'intelligenza artificiale; per esempio la nuova fattispecie di reato di *Illecita diffusione di contenuti generali o manipolati artificialmente* (art. 612-quater c.p.).[22] La legge ha altresì previsto un articolo inerente specificamente l'impiego dei sistemi di intelligenza artificiale nell'ambito dell'informazione. Infatti l'articolo 4 (Principi in materia di informazione e di riservatezza dei dati personali), al comma 1, dispone che l'uso dei sistemi di A.I. nell'informazione avviene <<senza recare pregiudizio alla libertà e al pluralismo dei mezzi di comunicazione, alla libertà di espressione e all'obiettività, completezza, imparzialità e lealtà dell'informazione>>. Ancorchè senza fare espressa, diretta menzione del diritto ad essere informati correttamente -e quindi a non essere disinformati- il Legislatore ha comunque enunciato un principio di tutela della libertà di espressione e del pluralismo dei mezzi di comunicazione, oltre che di "qualità" dell'informazione stessa, con specifico riguardo all'uso della A.I., a conferma, in definitiva, della centralità del diritto fondamentale ad essere informati anche nell'ecosistema digitale. Detta disposizione deve a sua volta essere letta in

vulnerability fino al punto di ledere concretamente specifici beni, diritti e valori, già oggi assumono effettivo rilievo in ambito di cybersecurity (cfr. G. Barozzi Reggiani, *La qualificabilità della disinformazione quale problema di cybersicurezza* in Disinformazione digitale, Modelli algoritmici e valori democratici, op. cit., pagg. 71 – 73).

[22] Cfr. F. Fabrizzi, *La cura contro la disinfomazione. Rimedi giuridici (e non) per contrastarne la diffusione* in Disinformazione digitale, Modelli algoritmici e valori democratici, op. cit. pagg. 43 – 44.

collegamento con l'art.3 (principi generali) della stessa legge il cui comma 4, prevede che l'uso dei sistemi di A.I. <<non deve pregiudicare lo svolgimento con metodo democratico della vita istituzionale e politica e l'esercizio delle competenze e funzioni delle istituzioni territoriali sulla base dei principi di autonomia e sussidiarietà e non deve altresì pregiudicare la libertà del dibattito democratico da interferenze illecite, da chiunque provocate, tutelando gli interessi della sovranità dello Stato nonché i diritti fondamentali di ogni cittadino riconosciuti dagli ordinamenti nazionale ed europeo>>. Dal collegamento fra le due norme si evince la volontà del legislatore ordinario di garantire un'ampia tutela della libertà di espressione e di informazione nell'ambito della discussione pubblica di natura specificamente politico-istituzionale. Dette libertà, in quanto tasselli fondamentali della "libertà del dibattito democratico", rappresentano pertanto un bene costituzionale "comune" da preservare, ponendolo al riparo da possibili "interferenze illecite" poste in essere mediante sistemi di AI.

4. Le patologie del sistema mediatico digitale. In particolare la disinformazione nella comunicazione politica on line.

Information disorder (Disordine informazionale). È questa la definizione della nuova patologia del sistema mediatico digitale[23]. Già da sola, l'infodemia – cioè la diffusione virale di informazioni- danneggia il processo democratico poiché viene meno la coerenza logica del discorso. Le informazioni infatti hanno una propria logica, una propria temporalità e una propria dignità al di là del binomio verità/menzogna. Anche

[23] *Information disorder* è espressione che prende in considerazione fenomeni fra loro eterogenei: dalla limitazione del diritto all'informazione generale, alla manipolazione dell'opinione pubblica da parte di Paesi ostili, passando per la destabilizzazione politico-sociale e l'infiltrazione nel circuito dell'informazione e della sicurezza pubblica. Al riguardo cfr. F. Fabrizzi, *La cura contro la disinformazione. Rimedi giuridici (e non) per contrastarne la diffusione* in Disinformazione digitale, Modelli algoritmici e valori democratici, op. cit. pag.37.

le *fake news* sono anzitutto informazioni e hanno esercitato il loro effetto prima ancora che abbia inizio un processo di verifica. Esse sfrecciano davanti alla verità e non vengono più raggiunte da questa e pertanto il tentativo di combattere l'infodemia con la verità è destinato al fallimento[24]. Le problematiche esposte toccano in profondità il delicato legame fra disinformazione, comunicazione politica e procedimento elettorale. Del resto, secondo L'Autorità Garante delle Comunicazioni, a partire dal 2023, la televisione non è più il principale mezzo di informazione per gli italiani. Uno su due utilizza la Rete per informarsi e il 50,5% di coloro che sono iscritti ad un *social network* dichiara di venire a conoscenza di notizie e informazioni sui *social* prima che su altri mezzi di comunicazione. Solo poco più del 17% dichiara di leggere i quotidiani, mentre circa un quarto dei cittadini fruisce delle notizie dalla versione digitale dei mezzi editoriali tradizionali. Inoltre, come segnalato -e commentato- di recente, [25] la stessa Autorità delle Comunicazioni[26], nella propria recente Relazione annuale del 2026, ha segnalato come l'intelligenza artificiale, della quale è ormai innervato l'ecosistema digitale, non sia solo un nuovo oggetto da regolare, che si affianca alla televisione e alle piattaforme digitali, bensì una nuova tecnologia trasversale che modifica il funzionamento dell'intero ecosistema dell'informazione. Infatti, a parte l'impatto sulla produzione dei contenuti, l'AI -prima ancora- seleziona, organizza e dà loro visibilità. Le notizie da proporre, l'ordine di incontro delle fonti e la risposta unitaria che scaturisce da questa molteplicità di materiali, produce una

[24] cfr. Buyng-chul Han, in *Infocrazia-Le nostre vite manipolate dalla rete*, Torino, 2023, pag.59.
[25] Cfr. O. Pollicino, *La costituzione dell'AI, AGCOM: che pluralismo resta se le fonti non arrivano più ai cittadini?* In www.agendadigitale.eu del 20 luglio 2026.
[26] La Relazione Annuale 2026 sull'attività svolta e sui programmi di lavoro presenta dati e rendiconti sull'azione di lavoro condotta dall'Autorità per le garanzie nelle comunicazioni (AGCOM) nel periodo compreso tra il 1° maggio 2025 e il 30 aprile 2026.

vera e propria "rappresentazione sintetica della realtà". L'infrastruttura tecnologica condiziona quindi ormai la riconoscibilità delle fonti e la libertà del cittadino di accedere a una pluralità di opinioni. Si può avere una pluralità teoricamente sterminata di fonti e, allo stesso tempo, una concentrazione elevatissima di infrastrutture che decidono quali di esse divengano concretamente visibili. Se teoricamente non c'è alcun impedimento ad esprimersi, può però diventare molto difficile essere ascoltati, trovati o riconosciuti come fonte. La menzionata Relazione riassume tutto ciò con l'espressione "mediazione algoritmica". Il pluralismo, inteso come reperibilità delle fonti, dipende quindi dalle condizioni tecnologiche poste a monte[27]. Trattasi di fenomeno e questione che assume rilievo particolare con i servizi di AI integrati nei motori di ricerca. La sintesi operata da quest'ultimo può precludere all'utente il raggiungimento delle fonti originarie. La facilitazione dell'accesso si basa sulla selezione dei materiali e nell'implicita rilevanza di essi così stabilita. L'accesso finisce cioè per condizionare la comprensione. La dimensione costituzionale del problema consiste proprio in questo, poiché le porte attraverso cui i cittadini raggiungono l'informazione sono gestite dai nuovi guardiani di cui si è detto nelle pagine precedenti. La sintesi generativa può rendere meno percepibile la pluralità dalla quale è stata ricavata; può attenuare contrasti e sfumature; può non rendere immediatamente comprensibile quali fonti siano state utilizzate e perché altre siano state escluse.

Per venire poi al tema della comunicazione politica, i partiti politici - dalla cui crisi era scaturito l'incremento dell'utilizzo di nuovi strumenti di informazione politica quali la televisione prima e la Rete poi- i movimenti e gli stessi singoli candidati fanno ormai

[27] Così sempre O. Pollicino in agendadigitale.eu, op. cit.

sempre più ricorso alle piattaforme per studiare i comportamenti dei votanti, indirizzarli con contenuti specifici e influenzare in definitiva la scelta elettorale[28]. Si preferiscono, pertanto, forme di comunicazione diretta e per molti versi disintermediata[29]. Oltretutto i *social*, come già chiarito, facilitano la formazione delle cosiddette comunità recintate e -anche mediante profilazione- inducono in molti utenti un atteggiamento passivo nel reperimento delle informazioni. Cresce inoltre l'influenza dei *social media* proprio sulla comunicazione politica[30]. Quest'ultima

[28] cfr. L. Califano, F. Fabrizzi e G. Sartor, *Information disorder e sistema democratico* Editoriale in federalismi.it n.15/2025, pagg. 6 e 7.

[29] C. Bertoldi, *Profilazione e micro-targeting a scopo politico-elettorale nella prospettiva del diritto costituzionale,* pagg.86 e ss. in federalismi.it n.3 del 2026 ricorda come l'avvento di *Internet*, nella prima fase, quella dell'*Internet* partecipativo, avesse alimentato un rapporto di scambio intenso e costante tra l'individuo e i diversi attori politici, determinando l'affermarsi di processi di inclusione in una sfera pubblica rinnovata e diversa. Trattasi della fase anteriore all'emersione delle piattaforme digitali e dei *social network* caratterizzato principalmente da una comunicazione orizzontale. Le trasformazioni intervenute negli anni successivi, segnate dallo sviluppo del mobile Internet e dall'introduzione di architetture algoritmiche e logiche di profilazione, hanno poi profondamente modificato le dinamiche della sfera pubblica digitale.

[30] Il rischio che i *social network* potessero minare trasparenza e genuinità del gioco elettorale, in tal modo condizionando il gioco democratico, è apparso subito chiaro a partire dal noto caso *Cambridge Analytics,* in cui venne dimostrato che *Facebook* si era ingerito nelle elezioni americane del 2016. Una vicenda resa possibile dalle evidenti lacune regolative di quella fase storica in cui, complice una illusoria persistente fiducia in una presunta neutralità tecnologica (rivelatasi invece una forma di *governance* privatizzata che trasferisce alle *corporations* decisioni fondamentali), la trasparenza, il controllo e i meccanismi di responsabilità erano completamente assenti. Sul punto cfr. G. Stegher, *La comunicazione politica nella digital era* in Disinformazione digitale etc., pagg.241-244 e ss. e ancora D. Scopelliti, in *Poteri privati e responsabilità pubbliche dei social network* etc., op. cit., pag. 231 nonché L. Torchia, *Lo Stato digitale- Una introduzione*, Bologna 2025, pagg.43-45, che ricostruisce la vicenda di Cambridge Analytica destinata a passare alla storia come il primo caso rilevante di uso della tecnologia per fini di manipolazione dei processi politici (ed elettorali: nella specie la campagna presidenziale americana del 2016 e nello stesso anno la campagna referendaria britannica che porto alla Brexit). Il trattamento algoritmico dei dati permise alla società Cambridge Analytica di predire non solo il tipo di servizio o prodotto che poteva essere proposto con successo a ciascun utente profilato, ma anche il tipo di messaggio politico che avrebbe più facilmente influito sull'utente come elettore. A tale riguardo chiarisce l'Autrice come il *microtargeting* politico consenta di fare campagne elettorali in cui si può far vedere ciascun messaggio solo agli elettori che, in base alla profilazione, lo accoglieranno

sempre più raramente prevede il contraddittorio tra i giornalisti e gli esponenti politici titolari di rilevanti cariche pubbliche o candidati alle stesse, che preferiscono invece affidare i loro messaggi unicamente alle piattaforme *social*. Si tratta del punto di arrivo dei processi di disintermediazione che hanno interessato la comunicazione e l'informazione nello spazio pubblico modificando la dinamica di formazione dell'opinione pubblica anche tramite l'ingresso nella discussione pubblica *on line* di soggetti privati e proprietari di piattaforme *social*, capaci di creare consenso veicolando messaggi semplici, brevi, schematici e di immediata comprensione a prescindere dalla loro fondatezza. Ne scaturisce, oltre che l'opacità del processo formativo della pubblica opinione - stante la carente trasparenza degli algoritmi- anche un mutamento della relazione tra rappresentanti e rappresentati, rinvenibile sia nel linguaggio utilizzato, spesso impostato al fine di toccare le corde emotive dell'utente e sia nel complessivo nuovo modo di interagire che tende a valorizzare la componente decidente della democrazia più che quella dialettica, parlamentare. La dimensione digitale del dibattito è ormai idonea ad influenzare fortemente la formazione dell'opinione pubblica. È un dato cui va rivolta una attenzione proporzionata alla consapevolezza che, in democrazia, il tema della formazione del consenso, e quindi la tutela del diritto ad essere informato del cittadino, sia nelle fasi che precedono l'espressione della volontà popolare sia durante lo svolgimento della "legislatura", è di particolare rilevanza, stante la sua centralità nella legittimazione di

positivamente senza che questi siano in grado di capire quale sia il programma complessivo del candidato e senza possibilità di verifica fattuale del singolo messaggio e della coerenza delle posizioni del candidato. In tal modo l'elettorato viene frazionato in piccoli gruppi a composizione interna omogenei e si evita il confronto in un dibattito pubblico aperto. La vicenda in questione trasmise all'opinione pubblica l'immagine della Rete quale vera e propria terra di nessuno, del tutto priva di regole.

un sistema che è basato sulla volontà popolare[31]. La stessa Corte costituzionale (sentenze n. 112 del 1993 e n. 155 del 2002) ebbe a suo tempo a chiarire che "i principi fondanti del nostro Stato esigono che la nostra democrazia sia basata su una libera opinione pubblica e che sia in grado di svilupparsi attraverso la pari concorrenza di tutti alla formazione della volontà generale"[32].

E' evidente che appare quanto meno singolare la situazione creatasi con riferimento alla comunicazione politica sulla Rete, cioè quella di un giornalismo partecipativo sostanzialmente deregolamentato -a differenza di quello televisivo, disciplinato dalla legge- attivo in rete e che si ritiene legittimato ad operare, spesso con continuità e con una linea editoriale, sulla base della mera libertà di manifestazione del pensiero, laddove invece si pone in essere informazione professionale a tutti gli effetti. La tutela del "diritto ad essere informati" – declinato ormai tuttavia da molti come "interesse generale a non essere disinformati" oppure come "diritto a una corretta informazione" o ancora «diritto a essere informati correttamente e a non essere ingannati»[33] - dovrebbe essere il *prius* anche per l'informazione in rete, compresa la comunicazione politica *on line* che di fatto è sempre propaganda, di parte, promossa e realizzata da singoli esponenti politici o partiti e che si sviluppa soprattutto sulle

[31] Anche D. Porena, *Social network, e-democracy e costituzionalismo digitale* in federalismi.it del 16/1/2026, pagg.167 e ss. evidenzia i non trascurabili elementi di alterazione nella formazione del consenso attraverso le piattaforme *social* definite "officine del consenso" capaci "di assorbire una mole enorme di dati, di elaborarli e di restituirli nella forma di una propaganda politica personalizzata in base alle inclinazioni dell'elettore-bersaglio."

[32] cfr. A. Papa, *Disintermediazione dell'informazione e della comunicazione politica nelle democrazie digitali* in federalismi.it n.15/2025, pagg. 19 – 22.

[33] cfr. R. Zaccaria e E. Albanesi in *Forum del gruppo di Pisa su Il ruolo dei social network al cospetto della libertà di manifestazione del pensiero e del diritto a informare e ad essere informati*, fascicolo n.1/2026. In tal senso cfr. pure L. Catanzano, *Libertà di espressione e verità artificiali. Quale marketplace of ideas nella società dell'algoritmo?*, in Riv. Med. Laws, I, 2025, pp. 60 ss.

piattaforme digitali che consentono una interlocuzione diretta tra politici -spesso gli stessi *leader* dei partiti - ed elettori, scavalcando non solo il sistema dei media ma anche le strutture di partito. Una comunicazione disintermediata, giudicata più rispondente alle attuali dinamiche relazionali e al modo d'essere dei movimenti contemporanei. Quando poi il leader politico è allo stesso tempo titolare di cariche pubbliche, ne deriva pure una notevole confusione fra comunicazione istituzionale e comunicazione politica in senso stretto che nessuna norma, relativamente alla Rete, tiene separate[34].

Ovviamente, l'irruzione della A.I., soprattutto di tipo generativo, con la sua velocissima diffusione, pone varie questioni soprattutto nel delicato settore dell'informazione dato che la propaganda e la disinformazione trovano in questo tipo di sistemi un ulteriore veicolo di inquinamento del dibattito democratico. A parte la citata infodemia, si va dal rischio "Epistemia" (definita "la confortevole illusione di conoscenza prodotta dall'interazione con l'I.A. generativa dei grandi modelli linguistici, là dove la plausibilità simulativa del discorso fluente e la coerenza narrativa sostituiscono l'efficienza cognitiva e l'affidabilità dei dati")[35] fino alla capacità di produrre grandi quantità di *output* testuali, visivi o multimodali, cioè contenuti del più vario genere. Anche a prescindere dal fatto che l'*AI Act*, a seconda della tipologia di sistemi, classifica gli stessi per livelli di rischio e obblighi di trasparenza diversificati, l'integrazione dell'AI generativa nel dibattito politico, nell'informazione e nella formazione del consenso pone domande importanti sulla manipolazione dell'opinione pubblica e sull'impatto delle tecnologie predittive nei processi

[34] cfr. A. Papa, *Disintermediazione dell'informazione e della comunicazione politica nelle democrazie digitali,* op. cit. pagg.24 – 26.
[35] Voce Epistemia in Vocabolario Treccani *on line*, neologismi, 2026.

elettorali[36]. Ulteriore interrogativo è pure quello inerente lo statuto giuridico di questi contenuti e cioè se essi siano o meno coperti da tutela costituzionale come manifestazioni di pensiero e – eventualmente - entro quali limiti[37].

5. Gli strumenti, normativi e non, di contrasto alla disinformazione nella comunicazione politica on line. Proposte finali.

Con riferimento alla regolamentazione interna della propaganda politica *on line*, la legge n.28 del 2000, di regolamentazione dell'accesso paritario ai mezzi di comunicazione radio-televisivi da parte delle forze politiche durante le campagne elettorali e referendarie e per la comunicazione politica, non offre margini sufficienti per una applicazione estesa all'ambiente del *web*, caratterizzato oltretutto dalla moltiplicazione dei canali comunicativi. Quest'ultimo aspetto, in una con l'incontrollabilità dell'eccesso delle fonti informative cui si può attingere, è alla base di quanti reclamano oggi nuove norme di legge capaci di fronteggiare il moltiplicarsi delle piattaforme che trasmettono informazioni con posizioni di dominanza. Negli ultimi anni l'AGCOM, svolgendo un ruolo di supplenza, ha posto in essere atti di impulso e coordinamento -tra gli attori della informazione *on line*- promuovendo l'autoregolamentazione volontaria degli operatori per contrastare la disinformazione e le lesioni della correttezza, imparzialità e pluralismo dell'informazione. Fra i risultati di questa attività si possono ricordare le Linee Guida per la parità di accesso alle piattaforme on line nella campagna elettorale del 2018, ispirate ai principii di imparzialità ed equità espressi nella citata legge n.28/2000, nelle condizioni di acceso

[36] cfr. O. Pollicino, *Regolazione e innovazione tecnologica nell'ordinamento della rete* in Rivista A.I.C. n.2/2025, pagg. 158 – 164.
[37] cfr. V. Baldini, *Plurime valenze della libertà di manifestazione del pensiero e suoi limiti: una questione sempre attuale* in Consulta on line 2025, fascicolo II del 4/8/2025, pagg.1247 e ss.

ai mezzi di comunicazione per tutti i soggetti politici. Analogo intervento è stato poi posto in essere dall'AGCOM nella campagna elettorale delle elezioni europee del 2019 sempre per favorire l'autoregolamentazione degli operatori. Entrambi gli interventi di autoregolamentazione erano scaturiti dal lavoro svolto dal "Tavolo tecnico per la garanzia del pluralismo e della correttezza dell'informazione sulle piattaforme digitali" istituito dalla citata Autorità.[38] In parallelo all'AGCOM va rammentato pure il ruolo del Garante per la protezione dei dati personali, il quale però non interviene sulla veridicità dei contenuti bensì sulla disinformazione riferita al trattamento illecito di dati personali a fini di propaganda politica in violazione del GDPR. Un intervento di settore che non riguarda la ben più ampia disinformazione virale, che non impiega dati personali specifici.[39]

L'Unione Europea, dal canto suo, al fine di garantire la correttezza del dibattito pubblico e dei processi democratici elettivi, ha innalzato il livello di trasparenza che i fornitori e gli utenti di determinati sistemi di A.I. devono garantire. Da qui scaturisce, in primo luogo, l'obbligo contenuto nell'art. 50 dell'*AI Act*, che prevede che le persone fisiche devono essere informate del fatto di stare interagendo con sistemi di A.I.[40],

[38] Sul ruolo giocato dall'AGCOM a garanzia del pluralismo e della correttezza dell'informazione sulle piattaforme digitali cfr. A Dominici, *Comunicazione e nuove tecnologie: la propaganda politica on line nella Costituzione*, in Disinformazione digitale etc. op. cit., pagg. 303-307.
[39] Cfr. L De Carlo in *Il contrasto alla disinformazione nei procedimenti elettorali: spunti comparatistici tra Italia e Spagna*, in Disinformazione digitale Modelli algoritmici e valori democratici etc. op. cit., pag. 289.
[40] L'art. 50 in parola è disposizione che, in applicazione del principio di trasparenza, introduce obblighi di riconoscibilità per interazioni e contenuti generati o manipolati dall'AI. E' norma trasversale perché opera a prescindere dalla classificazione del rischio. Si applica ai sistemi di AI che: -interagiscono direttamente con esseri umani -tipo *chatbot* e assistenti virtuali- quando l'utente potrebbe credere di aver a che fare con una persona reale; -generano o manipolano contenuti testuali, visivi, audio, cioè la AI generativa; -producono *deepfake* (contenuti falsi ma realistici) o

fermo restando che questi ultimi, se "allenati" a farlo, possono aiutare l'azione di contrasto dei rischi di disinformazione quando p.e. individuano i profili falsi (i cd. *troll*) o quando individuano e identificano contenuti falsi o comunque manipolati mediante A.I.[41]. Tale consapevolezza sembra essere alla base dell'approccio tenuto dal regolatore eurounitario in materia di disinformazione, sostanziatosi con l'adozione, nel dicembre 2023, del Pacchetto sulla difesa della democrazia europea, nel quale è presente anche una Raccomandazione per la tutela dei processi elettorali nell'UE, che riconosce espressamente il ruolo giocato dall'AI nella diffusione della disinformazione e la manipolazione delle informazioni. Queste attività ormai, a causa delle nuove tecnologie, si sviluppano in modo massiccio e veloce anche per effetto delle ingerenze di attori stranieri[42] che costituiscono, secondo l'U.E., una grave minaccia, potendo compromettere le istituzioni e i processi democratici, impedendo ai cittadini di prendere decisioni informate o sospingendoli verso l'astensionismo.

La Commissione Europea, a tali fenomeni, risponde articolatamente:

- col rafforzamento delle democrazie europee, per rendere più difficile agli autori delle minacce l'uso delle piattaforme *on line*, soprattutto costringendo queste ultime ad assumersi la responsabilità del contrasto alla manipolazione delle informazioni. Sotto questo profilo vanno ricordati il Codice di buone pratiche dell'UE sulla disinformazione del 2018, rafforzato nel 2022 e integrato nel 2025 quale codice di condotta sulla disinformazione; poi il menzionato

contenuti informativi di interesse pubblico generati o manipolati dall'AI. Gli obblighi previsti dalla normativa entreranno in vigore il 2 agosto 2026.

[41] cfr. O. Pollicino e P. Dunn, *Disinformazione e intelligenza artificiale nell'anno delle global elections: rischi (ed opportunità),* op. cit. pagg. 17 e ss.

[42] Cfr. sulla questione della disinformazione e ingerenze di paesi terzi, O. Pollicino e P. Dunn in *Disinformazione e intelligenza artificiale nell'anno delle global election* etc. op cit. pagg.7-10.

regolamento sui servizi digitali, DSA, che contiene norme che impongono alle piattaforme e ai motori di ricerca di rendere lo spazio online trasparente e sicuro per gli utenti, di proteggere i diritti fondamentali e di combattere la disinformazione, nonchè il summenzionato regolamento *AI Act* che affronta la manipolazione delle informazioni facilitata dall'AI attraverso l'approccio basato sul rischio; infine il regolamento UE relativo alla trasparenza e al *targeting* (invio di annunci personalizzati) della pubblicità politica 2024/900[43]

[43] Sul regolamento europeo sulla pubblicità politica 2024/900, che introduce, al fine di una maggiore trasparenza, doveri di etichettatura dei messaggi politici *on line* e il preventivo consenso dell'utente alla sua profilazione, cfr. A. Papa, *Il Regolamento europeo sulla pubblicità politica, ovvero del difficile tentativo di regolamentare la propaganda on line (e non solo)* in Disinformazione digitale Modelli algoritmici e valori democratici etc. op. cit., pag. 219- 232. la quale sottolinea come, il legislatore europeo (composto qui dal Parlamento europeo e dai rappresentanti dei governi nazionali in consiglio) ha voluto disciplinare uno strumento proprio del dibattito democratico: la propaganda politica resa in modo "professionale", non certo l'opinione espressa a titolo personale dal soggetto politico. Cfr. pure G. Stegher, *La comunicazione politica nella digital era* sempre in Disinformazione digitale etc., pagg. 249- 252. L'A. dopo aver ricordato la prima fase "liberistica" della UE sulla comunicazione politica *on line*, cessata, all'indomani della scoperta della falsa rappresentazione di neutralità tecnologica delle piattaforme, in favore della fase della cd. autoregolazione, rivelatasi poi altrettanto inadeguata, si sofferma sulla terza fase, quella caratterizzata dall'attuale regolazione vincolante che ha dato vita ad una espansione normativa e ad una complessa stratificazione di regole. A questa terza fase, da cui sono scaturiti il DSA *Act* e il DMA *Act*, va ricondotto pure il regolamento UE 2024/900 anch'esso finalizzato, in relazione alla comunicazione politica, alla protezione dei diritti individuali e collettivi nello spazio digitale e che ai primi due si affianca puntando a creare un ecosistema digitale più trasparente, responsabile e democratico, bilanciando la libertà di espressione con la necessità di un controllo rispetto a rischi paventati o concreti. L'intervento regolatorio si basa sulla presa d'atto dei rischi derivanti dalla potenziale alterazione delle informazioni e delle possibili interferenze di attori internazionali nei processi elettorali nonché dell'innato conflitto fra il ricorso alla intelligenza artificiale per la profilazione e la necessità di un ambiente informativo ispirato a maggiore democraticità. Esso è espressione di una nuova concezione della sovranità digitale, intesa come la capacità delle istituzioni di esercitare un controllo effettivo sui processi di formazione dell'opinione pubblica. Per quanto invece attiene al *targeting,* deve darsi conto d'una ulteriore versione tecnologicamente più raffinata, che mira a plasmare le preferenze dell'elettore, denominata *neurotargeting* ed è l'ultima evoluzione delle forme di pubblicità profilata. Con essa si mira a sapere come reagisce il cervello dell'elettore a determinati stimoli inconsci. A tal fine si crea un messaggio politico inconscio personalizzato al fine di aggirare il giudizio razionale e in questo modo si traccia una mappatura emotiva dell'elettore in relazione agli

ed il Regolamento UE 2024/1083 dell'11 aprile 2024 di protezione dei giornalisti e del pluralismo e indipendenza dei media nella Unione Europea;

- con una più ampia alfabetizzazione digitale e mediatica dei cittadini consentendo loro di navigare nell'ambiente dell'informazione sensibilizzandoli sui rischi di manipolazione delle informazioni e aiutandoli a riconoscere e contrastare questa minaccia;[44]
- con la denuncia delle tattiche di manipolazione delle informazioni e di ingerenza da parte di attori stranieri garantendo la preparazione delle opportune difese in caso di attacchi informatici;
- con lo Scudo Europeo per la democrazia, proposto nel novembre 2025 e approvato il 15 settembre di quest'anno dal Parlamento Europeo con raccomandazioni volte a rafforzare l'operatività dello Scudo stesso, nell'ambito del quale si punta alla salvaguardia dell'integrità dello spazio dell'informazione, con l'accento posto sul contrasto alla manipolazione delle informazioni, alle

stimoli provocati. E' chiaro che queste tecniche incidono sull'uguaglianza del voto in senso sostanziale nonchè sulla sua libertà (art. 48 Cost.), palesemente messa a rischio. Anche C. Bertoldi, *Profilazione e micro-targeting a scopo politico-elettorale etc,* op. cit., pagg.117 e ss., considera il citato regolamento un fattore di rafforzamento dell'integrità del processo elettorale, un elemento di contrasto alla disinformazione nonchè di garanzia d'una maggiore trasparenza della pubblicità politica in rete. La trasparenza in particolare è ritenuta condizione necessaria per sostenere un dibattito politico e campagne politiche equi e aperti, come pure elezioni o referendum liberi e regolari e per combattere la manipolazione dell'informazione e le interferenze, nonché le interferenze illecite anche da paesi terzi.

[44] Una strategia di contrasto alla disinformazione che fa leva su meccanismi psicologici e cognitivi è il cd. *prebunking*. Trattasi d'una sorta di vaccinazione attitudinale preventiva e consiste nell'esporre le persone a esempi o tecniche di disinformazione in modo da aiutarli e abituarli a riconoscerli e a respingerli in futuro. Oltre a ciò ovviamente occorre comunque una seria ed efficace educazione digitale che metta al centro del discorso la salvaguardia del pluralismo quale fondamento del costituzionalismo contemporaneo. Nei termini esposti cfr. F. Fabrizzi, *La cura contro la disinfomazione. Rimedi giuridici (e non) per contrastarne la diffusione* in Disinformazione digitale etc. op. cit. pagg. 52 – 55.

ingerenze straniere e alle campagne di disinformazione, essenziale per garantire che le persone possano esprimere liberamente le loro opinioni e avere accesso a informazioni affidabili.

Questo, in sintesi, il quadro europeo, all'interno del quale - nel 2027 - cadranno importanti appuntamenti elettorali in Francia (elezioni presidenziali e assemblea nazionale), Spagna (elezioni amministrative e di rinnovo assemblee legislative) ed in Italia (elezioni politiche). Anche alla luce di tali scadenze, ad avviso di chi scrive, troverebbe nel nostro Paese piena giustificazione una normativa di legge, di "servizio pubblico", che rendesse obbligatori confronti *on line* in contraddittorio dei titolari di cariche istituzionali o politiche con gli organi di informazione o con gli avversari politici. In tal modo propaganda politica e governo delle istituzioni troverebbero spazi distinti e separati, sì da consentire all'opinione pubblica di farsi un'idea più precisa e consapevole dell'attività istituzionale e dei suoi esiti. Una normativa siffatta, che dovrebbe coinvolgere trasversalmente sul piano dell'iniziativa tutti i partiti politici, concretizzerebbe un positivo esempio di reintermediazione, di ripristino del ruolo dei partiti quali *trait d'union* tra cittadini e istituzioni nel segno anche dell'art. 49 della Costituzione.

Quanto ai *social*, basati su algoritmi e profilazione, ormai potenziati dall'AI, assodato che l'impostazione del flusso continuo di contenuti aggiornati che scorre sulla pagina *web* (cd. *feed*) condiziona molto il reperimento delle informazioni e la libera formazione delle opinioni degli utenti -senza dire dei minori, a forte rischio dipendenza e vulnerabilità psicologica- con riduzione di capacità critica e scarsa tensione verso la ricerca della verità, sembra necessario spingere o obbligare le piattaforme a promuovere usi della AI orientati verso il pluralismo informativo e il

miglioramento del dibattito pubblico intervenendo nelle fasi di sviluppo e *design* dei sistemi di raccomandazione in modo da arricchire l'ecosistema informazionale e ridurre gli effetti collaterali connessi alle camere dell'eco[45]. L'intento, in questo caso, è quello –almeno- di ridurre l'attuale sostanziale censura praticata nei confronti delle opinioni difformi, rispetto a quella "preferita" dall'utente, rimuovendo così ogni sorta di limitazioni del pluralismo. Una misura volta a promuovere la capacità di formarsi una opinione critica assicurando effettività sia alla libertà di informare e sia al diritto ad essere informati.

[45] cfr. O. Pollicino e P. Dunn, *Disinformazione e intelligenza artificiale nell'anno delle global elections: rischi ed opportunità,* op. cit., pagg.18 e ss.