RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0221 • articolo sottoposto a peer review • pubblicato in anteprima il 29 mag. 2025

Camilla Lobascio

Micro-targeting politico e protezione dei dati personali. Il Regolamento (UE) 2024/900

L'ampio ricorso agli strumenti digitali promette di rendere più efficienti i processi decisionali, ma solleva interrogativi rilevanti circa l'impatto di tali tecnologie sui diritti e sulle libertà fondamentali. Ciò avviene in particolare in materia di protezione dei dati personali, specie quando i dati sono usati a fini politici, come nelle campagne elettorali, momento in cui gli utenti possono essere esposti a contenuti mirati in condizioni di vulnerabilità e senza piena consapevolezza della natura sponsorizzata del messaggio. Tali dinamiche rischiano di influenzare opinioni e scelte politiche in modo potenzialmente manipolatorio. In risposta a queste criticità, il Regolamento (UE) 2024/900 ha introdotto norme armonizzate sull'uso di tecniche di targeting e diffusione dei messaggi pubblicitari che implicano il trattamento di dati personali nel contesto della pubblicità politica online. Tuttavia, il regolamento si concentra sulla pubblicità politica, senza intervenire su altre forme di comunicazione potenzialmente manipolatorie, come le campagne di disinformazione o di guerra ibrida, che sfruttano algoritmi e sistemi di raccomandazione per ottenere visibilità. Fra le piattaforme digitali interessate dalla normativa, Google ha deciso di sospendere la pubblicità politica, mentre Meta non ha ancora adottato una posizione ufficiale. Resta il rischio che la normativa, pur nata con finalità di tutela, possa finire per restringere lo spazio del dibattito politico online.

Micro-targeting – Datificazione – Elezioni – Privacy – Regolamento 2024/900 – Diritti neurali

Political micro-targeting and data protection regulation: Regulation (EU) 2024/900

The widespread use of digital tools promises to make decision-making processes more efficient, but raises relevant questions about the impact of such technologies on fundamental rights and freedoms, in particular with regard to the protection of personal data, especially when data are used for political purposes, as in election campaigns, when users may be exposed to targeted content in vulnerable conditions and without full awareness of the sponsored nature of the message. Such dynamics risk influencing opinions and political choices in a potentially manipulative way. In response to these critical issues, Regulation (EU) 2024/900 introduced harmonised rules on the use of targeting techniques and dissemination of advertising messages involving the processing of personal data in the context of online political advertising. However, the regulation focuses on political advertising, without intervening on other potentially manipulative forms of communication, such as disinformation or hybrid warfare campaigns, which exploit algorithms and recommendation systems to gain visibility. Among the digital platforms affected by the regulation, Google has decided to suspend political advertising, while Meta has not yet adopted an official position. The risk remains that the legislation, although born with protective purposes, may end up restricting the space for online political debate.

Micro-targeting – Datification – Elections – Privacy – Regulation 2024/900 – Neural rights

L'Autrice è dottoranda di ricerca presso il Dipartimento di Giurisprudenza dell'Università degli studi di Macerata

Questo contributo fa parte della sezione monografica *EMFA under the spotlight: towards a common regulatory framework to foster media pluralism?* Part II - a cura di Elda Brogi

1. La mercificazione dei dati

È ampiamente riscontrata la diffusione di un modello di business[1] che prevede l'erogazione di servizi a titolo gratuito, senza la previsione di un corrispettivo pecuniario, subordinatamente all'acquisizione del consenso per il trattamento dei dati personali degli utenti. Tale modello risulta particolarmente prevalente nelle interazioni online, pur non essendo esclusivamente ad esse circoscritto, ed è stato favorito dal progresso delle nuove tecnologie, che forniscono tecniche sempre più pervasive e sofisticate di raccolta, monitoraggio e sfruttamento dei dati personali. La fornitura di beni e servizi costituisce infatti un'occasione preziosa per accedere alle potenzialità economiche dei cosiddetti *big data*[2]. L'*Autorité de la Concurrence* in Francia e il *Bundeskartellamt* in Germania hanno congiuntamente sottolineato come la creazione di valore sia strettamente connessa allo sviluppo di nuove tecniche in grado di estrarre "informazioni preziose da enormi quantità di dati (spesso non strutturati)". In questo contesto, i *big data* risultano strettamente collegati ai *big analytics*, ovvero alla capacità dei sistemi informatici di affrontare problemi complessi attraverso l'analisi di grandi volumi di dati grazie all'uso di algoritmi avanzati[3]. I dati personali costituiscono ricchezza e alimentano dunque l'economia digitale. A conferma di ciò, il d.lgs. 4 novembre 2021, n. 173 ha introdotto all'interno del Codice del Consumo (d.lgs. 6 settembre 2005, n. 206) il Capo I *bis* denominato "*Dei contratti di fornitura di contenuto digitale e di servizi digitali*". L'art 135-*octies* (*Ambito di applicazione e definizioni*), si occupa della fattispecie dello scambio di contenuti/servizi con dati personali a fronte del pagamento di una somma di denaro. Il GDPR riconosce che l'interessato (o consumatore) si trova in una posizione di svantaggio nel rapporto contrattuale, motivo per cui il Capo III del regolamento gli attribuisce specifici diritti, tra cui la possibilità di gestire e controllare la diffusione delle proprie informazioni personali. Nonostante ciò, lo sfruttamento economico dei dati personali rimane una questione problematica: il *footprint* digitale degli individui è gestito dalle grandi *digital companies*, che lo utilizzano per influenzare opinioni e comportamenti in molteplici ambiti. Questa dinamica è aggravata dalla formazione di oligopoli, che non solo limitano la concorrenza ma consolidano il potere delle piattaforme, riducendo

1. Per una definizione di modello di business si può far riferimento alla descrizione di G. Donna: "Le numerose definizioni proposte, pure differenziandosi sul piano lessicale, convergono nell'identificare nel modello di business l'illustrazione di come un'azienda intende creare valore. 'Business models are stories that explains how enterprises work … to deliver value to customers, entice customers to pay for value and convert those payments to profits'" in Donna 2018.
2. Thobani 2019.
3. Gobbato 2019.

ulteriormente il margine di controllo dei consumatori sui propri dati e sulla loro stessa esperienza digitale[4].

Nel mercato dei dati costituito da piattaforme online e motori di ricerca, la mercificazione delle persone, o la loro riduzione a materia prima, come afferma S. Zuboff, si riferiscono al fenomeno in cui le persone sono trattate principalmente come risorse da sfruttare per fini economici o di controllo[5]. Non sorprende che sia stato evidenziato come sia del tutto legittimo affermare che le informazioni (e quindi i dati), oltre a supportare e ottimizzare gli scambi economici e le transazioni convenzionali, stiano assumendo il ruolo di un vero e proprio fattore di produzione, comparabile a terra, capitale e lavoro[6].

Ma quali sono le implicazioni giuridiche della mercificazione associata alla *datification*[7] delle persone? Quali sono le conseguenze legali quando la mercificazione è incentivata, in maniera più o meno consapevole, dall'uso diffuso dei social network e dei motori di ricerca? Risulta impossibile al momento fornire una risposta definitiva ai quesiti posti, poiché la complessità del fenomeno della mercificazione associata alla *datification* delle persone è oggetto di dibattito e riflessioni giuridiche in evoluzione costante. La trasformazione dei dati personali in beni di valore economico, e la conseguente mercificazione degli individui attraverso le loro tracce digitali, solleva molteplici questioni di stampo sia legale che etico che non possono essere pienamente risolte con una normativa univoca. In aggiunta a ciò è utile ricordare che, nel regolamentare la tecnologia, è difficile non imbattersi nel cosiddetto dilemma di Collingridge[8]. Questo fenomeno descrive la situazione in cui, dal momento dell'emergere di un'innovazione tecnologica alla sua regolamentazione, passa molto tempo a causa di una certa esitazione dei regolatori, i quali non agiscono tempestivamente per mancanza di informazioni più specifiche sul funzionamento della tecnologia di riferimento. Pertanto, nel momento in cui tali informazioni diventano disponibili, le normative rischiano di essere già obsolete, poiché non più allineate con i progressi tecnologici. Ci troviamo, infatti, di fronte sia ad un problema di mancanza di informazioni (il che significa che gli impatti non possono essere facilmente previsti fino a quando la tecnologia non è ampiamente sviluppata e utilizzata dalla popolazione) sia a un problema di potere (il controllo o il cambiamento diventano difficili quando la tecnologia è ormai profondamente radicata). Le iniziative regolamentari adottate finora dall'Unione europea, sebbene apprezzabili, non forniscono ancora una risposta completa alle sfide poste dalla mercificazione dei dati personali, incentivata, spesso inconsapevolmente, attraverso l'uso diffuso dei social network e dei motori di ricerca. Le tecnologie emergenti e l'economia basata sui dati, in particolare i modelli di business che si fondano sulla raccolta e l'analisi delle attività online degli utenti, hanno richiesto vari interventi da parte dell'Unione europea per promuovere la libera circolazione dei dati personali, garantendo al contempo una protezione agli individui. A tal proposito, la normativa eurounionale, attraverso il GDPR, il *Digital Services Act* e il *Digital Markets Act*, il *Data Act* e il *Data Governance Act*, mira a facilitare il flusso libero dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali. Questi interventi sono stati necessari perché ai fenomeni descritti si affianca una sorveglianza di massa continua e pervasiva, resa

4. Morace Pinelli 2024.
5. Zuboff 2019.
6. Califano 2021.
7. Per una definizione interdisciplinare di *datification* si può far riferimento a quella fornita da Mejias–Couldry 2019: "Datafication is not just the making of information, which, in one sense, human beings have been doing since the creation of symbols and writing. Rather, datafication is a contemporary phenomenon which refers to the quantification of human life through digital information, very often for economic value. This process has major social consequences. Disciplines such as political economy, critical data studies, software studies, legal theory, and – more recently – decolonial theory, have considered different aspects of those consequences to be important. Fundamental to all such approaches is the analysis of the intersection of power and knowledge".
8. Genus–Stirling 2018, pp.61-69.

possibile dalla diffusione capillare di Internet e dall'attività delle piattaforme digitali predominanti. Queste raccolgono e analizzano enormi quantità di dati, rafforzando il controllo sugli utenti e influenzando dinamiche economiche, sociali e politiche. Questo sistema solleva importanti questioni giuridiche relative alla tutela della privacy, alla protezione dei dati personali e alla conformità alle normative vigenti, quali il GDPR. Infatti, la raccolta, l'elaborazione e la commercializzazione dei dati personali senza un consenso esplicito rappresentano una violazione dei diritti fondamentali degli individui, incluso il diritto alla riservatezza[9].

2. La trasformazione della sfera pubblica e politica come effetto della diffusione della rete

Il fenomeno della mercificazione dei dati personali e la crescente centralità dell'economia digitale hanno effetti che travalicano il solo ambito giuridico ed etico, influenzando in modo significativo anche la sfera pubblica e politica. Il sistema descritto non si limita ad operare per finalità commerciali, ma si estende anche a scopi politici e sociali, soprattutto nel contesto delle piattaforme digitali, dove il controllo dei dati può influenzare opinioni, comportamenti e dinamiche collettive. L'avvento di Internet ha amplificato le tendenze alla disintermediazione e alla privatizzazione della sfera pubblica, adattandole alle caratteristiche distintive del mezzo di diffusione. La rete ha quindi favorito l'emergere di nuove relazioni sociologiche, incastonate nella cornice dello scambio di informazioni tramite apparati tecnologici, inaugurando un sistema di "autocomunicazione di massa"[10]. Questo paradigma sembra soppiantare le modalità comunicative tradizionali, contraddistinte da verticalità e unidirezionalità, con forme di interazione più orizzontali e partecipative[11]. La diffusione di termini come *e-democracy* (democrazia elettronica), *e-government* (governo elettronico) e *e-participation* (partecipazione elettronica) riflettono una crescente aspirazione verso una "comunità" digitale[12]. Internet in passato ha dimostrato il suo valore democratico, come illustrato nella sentenza *Reno v. American Civil Liberties Union* (1997)[13], e ha svolto un ruolo essenziale nella mobilitazione contro regimi autoritari, come dimostrato dai movimenti in Africa settentrionale. Anche altri studi come quelli di M. Margolis e G. Moreno-Riaño[14], esplorano come Internet, grazie alla sua capillarità, possa favorire una democrazia più partecipativa. Risulta infatti particolarmente interessante analizzare come la comunicazione politica si sia evoluta grazie al web. Da un lato la comunicazione politica online rappresenta una rivoluzionaria opportunità di stabilire un contatto diretto e su larga scala con l'elettorato, poiché grazie ai social network i politici possono ora intrattenere un dialogo immediato e continuo con gli elettori, e, nei casi della pubblicazione di contenuti online in maniera organica (esenti quindi dal pagamento di un servizio pubblicitario di diffusione del contenuto offerto dalla piattaforma) si possono superare le barriere economiche precedentemente imposte dalle elevate spese di comunicazione tradizionale (stampa cartacea, televisione, radio, manifesti…). Questa possibilità consente ai rappresentanti politici di veicolare il proprio messaggio in modo più efficiente e capillare, riducendo significativamente i costi associati alla pubblicità e alla propaganda elettorale. Dall'altro lato va sottolineato come i processi democratici stiano subendo, a livello globale, un'erosione di quell'elemento essenziale per la loro vitalità: la sfera pubblica. Il populismo contemporaneo si configura come una nuova e potente macchina da guerra mediatica, capace di trasformare reazioni emotive private in apparenti manifestazioni di opinione pubblica. Siamo immersi in una vera e propria rivoluzione audiovisiva, in cui la mente umana è costantemente *over-stimulated* dai mezzi digitali. Di conseguenza, l'autonomia cognitiva dell'utente non può considerarsi del tutto immune

9. Caso 2021.
10. Castells 2009.
11. Caruso 2023.
12. Longo 2021.
13. *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).
14. Margolis–Moreno-Riaño 2009.

da potenziali conseguenze preoccupanti[15]. Questo fenomeno è particolarmente insidioso poiché sfrutta la vulnerabilità dei cittadini, ai quali, attraverso tecniche di micro-targeting, vengono somministrate informazioni appositamente costruite per manipolare e strumentalizzare tali fragilità. In tal modo, il dibattito pubblico viene sostituito da una simulazione manipolatoria, che mina le fondamenta stesse della democrazia partecipativa[16]. Le piattaforme online forniscono dunque all'utente una mera illusione di partecipazione in uno spazio pubblico, poiché esse in realtà rinchiudono la persona nel privato delle proprie vulnerabilità ed emozioni[17].

3. Sistemi di raccomandazione, *neural rights* e impatto sulle decisioni

Nel contesto descritto i sistemi di raccomandazione sono diventati onnipresenti su Internet, offrendo agli utenti suggerimenti personalizzati su prodotti e servizi e impattando in maniera significativa sui margini di profitto delle aziende. Ad esempio, Amazon ha riferito che il 35% delle sue vendite proviene dai suoi sistemi di raccomandazione, mentre Netflix nel 2012 ha riportato che il 75% dell'attività di visione dei contenuti derivava da raccomandazioni. I sistemi di raccomandazione influenzano dunque le scelte degli utenti più dei pari e degli esperti, riducendo lo sforzo decisionale[18]. Gli algoritmi sono responsabili di classificare, estrarre, predire, processare dati e così facendo plasmano il mondo in un modo invece che in un altro. Il *ranking* dei contenuti che ci appaiono una volta collegati al nostro *feed* sui social, o nei risultati di un motore di ricerca, non rappresenta solamente una capacità classificatoria ma va a costituire un insieme di strategie all'interno delle quali è insito il potere[19]. Il riferimento, in primo luogo, è all'organizzazione unilaterale dei contenuti proposti sulle piattaforme digitali, che implica una selezione attraverso l'ordine di presentazione, classifiche (*ranking*) e raccomandazioni. Questi processi vengono gestiti dalle stesse piattaforme secondo criteri di rilevanza che tendono a privilegiare determinati contenuti a scapito di altri, basandosi sull'attenzione e sulle emozioni che tali contenuti suscitano. Di conseguenza ciò esercita un primo impatto culturale evidente, poiché le piattaforme digitali, in tale contesto, assumono un ruolo di potere come creatrici di cultura, elaborando unilateralmente i processi di selezione e promozione di ciò che viene discusso o sperimentato sensorialmente (attraverso immagini o suoni) online. In secondo luogo, ci si riferisce anche alla predisposizione unilaterale dei meccanismi di raccolta dei dati cognitivi necessari per tali attività, che si traduce in una gestione altrettanto unilaterale dei processi di catalogazione e, per certi scopi, perfino di denominazione della realtà[20].

Vi sono tuttavia delle restrizioni sulla commerciabilità dei dati che sono frutto delle normative vigenti in materia di protezione dei dati personali, con particolare attenzione alla regolamentazione dei requisiti per il consenso al trattamento, il quale deve essere "libero". Come è noto, tali disposizioni giuridiche bilanciano due interessi contrapposti: da un lato, la promozione della libera circolazione dei dati nel contesto di uno sviluppo del mercato unico dei dati; dall'altro, la salvaguardia dei dati personali, riconosciuta tra i diritti fondamentali nell'ordinamento dell'Unione europea[21].

15. Mancarella 2022.
16. Origgi 2018.
17. Le immagini e i video (spesso generati con tecniche di intelligenza artificiale e diffusi su piattaforme come Facebook, TikTok, Instagram…) che vengono proposti dai politici nelle loro campagne di comunicazione digitali sono infatti sempre più comunemente legati alla volontà di suscitare sentimenti forti, come rabbia, indignazione o paura, piuttosto che persuadere, ovvero ricercare di far cambiare idea a un oppositore.
18. I dati sono stati estrapolati da Nguyen–Hui–Harper et al. 2014. La ricerca non è recente, ma è lecito interpretare questi dati come una indicazione dell'impatto dei sistemi sofisticati di intelligenza artificiale nel produrre ranking di contenuti, che, negli ultimi 10, anni si è accentuato.
19. Garzonio 2021.
20. Orlando 2022-a.
21. Thobani 2019.

Attualmente, il diritto alla privacy include non solo il diritto alla riservatezza, ma anche un più ampio diritto al controllo sui propri dati personali. Si parla ora di *informational privacy*, un concetto ampiamente discusso che riflette la complessità e l'interconnessione della privacy con l'economia dell'informazione. L'*informational privacy* si riferisce alla tutela delle informazioni personali nel quadro delle attività economiche e tecnologiche moderne, dove i dati rappresentano una risorsa fondamentale[22]. Grazie all'intelligenza artificiale, tutti i tipi di dati personali possono essere utilizzati per analizzare, prevedere e influenzare il comportamento umano, trasformandosi così in merci di valore. Informazioni che un tempo non venivano raccolte o erano considerate scarti (i cosiddetti "dati di scarto" o *exhaust data*) sono ora diventate una risorsa preziosa[23].

L'algoritmo costituisce un elemento chiave nell'elaborazione automatizzata dei dati, inclusi quelli destinati a scopi commerciali. Tuttavia, la profilazione[24] tramite algoritmi racchiude in sé una problematica di difficile risoluzione: si configura come uno strumento di marketing vantaggioso sia per le imprese che per i consumatori, ma solleva problematiche relative alla violazione della privacy[25]. S. Rodotà, con riferimento alla navigazione sulla rete Internet e all'uso del social network Facebook, riteneva che solo ed esclusivamente l'anonimato[26] consentisse di "sottrarsi a interferenze nella propria vita che si traducano in aggressioni particolarmente gravi, in discriminazioni, molestie, limitazioni della libertà di espressione, esclusione da circuiti comunicativi"[27].

Infatti, la mancanza di anonimato nell'ecosistema online ha favorito la formazione delle cosiddette *echo chambers*, traducibili come camere d'eco o casse di risonanza, ovvero quegli spazi di navigazione online (come il *feed* di un social network o la homepage) in cui agli utenti vengono mostrati, con regolarità, contenuti simili a quelli con cui hanno già interagito (tramite like, condivisione, click o tempo trascorso in lettura). Un ambiente online personalizzato attraverso il micro-targeting genera bolle di filtraggio[28] o *filter bubbles*, termine coniato da Pariser nel contributo *The filter bubble: What the Internet is hiding from you*, che descrive l'esposizione sistematica degli utenti a informazioni simili per contenuti, con l'effetto di limitare l'incontro con fonti di origine diversa, il che ha per conseguenza l'intensificazione della polarizzazione politica e ideologica. Questo fenomeno è causa di instabilità politica e sociale e aumenta la persuasività di notizie false e teorie complottiste[29]. Una delle esternalizzazioni più preoccupanti di questi fenomeni è rappresentata dalla polarizzazione sociale, che descrive la tendenza a stringere legami solo con persone percepite come simili, escludendo o guardando con sospetto chi è diverso. Un esempio emblematico di questo processo si osserva nel crescente divario tra Democratici e Repubblicani negli Stati Uniti: tra il 1994 e il 2014,

22. Faralli 2019.
23. Lagioia–Sartor 2020.
24. Per una definizione esaustiva di "profilazione" si può far riferimento alla seguente: "la profilazione è una tecnica di trattamento (parzialmente) automatizzato di dati personali e/o non personali, finalizzata alla creazione di conoscenza predittiva mediante la scoperta di correlazioni tra i dati e la costruzione di profili, che possono essere poi utilizzati per assumere decisioni. Un profilo è un insieme di dati correlati che rappresentano un soggetto (individuale o collettivo). La costruzione di profili è il processo di scoperta di schemi ricorrenti e sconosciuti tra i dati, all'interno di grandi insiemi di dati, che possono essere utilizzati per creare profili. L'applicazione di profili consiste nell'identificazione e rappresentazione di uno specifico individuo o gruppo come corrispondente a un determinato profilo, e nel processo decisionale basato su tale identificazione e rappresentazione". Tratto da Bosco–Creemers–Ferraris 2015. Traduzione da Lagioia–Sartor 2020.
25. Bianca 2019.
26. Al tema dell'anonimato online si collega la sentenza Corte europea dei diritti dell'uomo, 7 dicembre 2021, *Standard Verlagsgesellschaft mbH c. Austria* (No. 3), ric. 39378/2015.
27. Rodotà 2012.
28. Pariser 2012.
29. European Data Protection Supervisor, *Online manipulation and personal data*, Opinion 3/2018.

i sentimenti di inimicizia e disapprovazione reciproci sono più che raddoppiati. Questa polarizzazione ostacola la creazione di un capitale sociale che sia inclusivo e capace di "collegare" gruppi diversi, impedendo di fatto una coesione sociale effettiva e costruttiva[30]. In ambito costituzionale, si ritiene che l'evoluzione tecnologica e le trasformazioni nel mercato delle comunicazioni richiedano oggi un approccio diverso per l'analisi del diritto all'informazione, rispetto a quello originariamente previsto dai redattori degli articoli 15 e 21 della Costituzione[31]. Sin dalle sue prime decisioni, la Corte costituzionale ha sempre evidenziato l'importanza fondamentale dell'art. 21, definendolo "pietra angolare dell'ordine democratico" (C. Cost, 17 aprile 1969, n. 84). Partendo da questo principio, la Corte ha affermato che l'art. 21 tutela non solo il "diritto di informare" – ossia l'aspetto attivo della libertà di comunicazione – ma anche il "diritto all'informazione" dei cittadini, essenziale per la corretta formazione dell'opinione pubblica, su cui si basa la democrazia. Il riconoscimento di questo "profilo passivo" della libertà di informazione e il suo legame con il principio democratico implica che tutti i mezzi di comunicazione di massa devono rispondere all'"interesse generale" all'informazione, il quale richiede un pluralismo delle fonti.

Gli studi di Richards[32] aggiungono una nuova chiave di lettura al fenomeno descritto, poiché sottolineano che la consapevolezza di essere costantemente sorvegliati cambia radicalmente il comportamento e le modalità di espressione delle persone, generando un effetto inibitore (*chilling effect*) sulla libertà individuale. In questo contesto, emergono rischi significativi legati alla distorsione comportamentale e alla discriminazione. Le persone il cui comportamento non viene solo influenzato, ma addirittura manipolato attraverso una comunicazione personalizzata, rischiano di diventare diverse da ciò che sarebbero state senza tale manipolazione. La comunicazione mirata sfrutta specifiche vulnerabilità decisionali e comportamentali, alterando profondamente le scelte. Quando si parla di contrastare queste pratiche, ci si riferisce alla necessità di opporsi allo sfruttamento delle vulnerabilità, così come alle pratiche che promuovono la radicalizzazione, la polarizzazione e l'amplificazione di determinati messaggi[33]. Le affermazioni di Richards, se applicate al marketing con finalità politiche, rafforzano l'idea per cui il corretto svolgimento del confronto politico su cui si fonda il sistema democratico (e il tanto discusso diritto all'informazione) stia entrando in una profonda crisi. Viene riconosciuto che la psicografia ha rivoluzionato il marketing degli ultimi anni, permettendo di tracciare un "profilo psicografico" che può essere inferito a partire dai dati di navigazione online di una persona, le tracce che lascia sui social networks, gli acquisti online e i suoi movimenti se usa un telefono cellulare (ad esempio, tramite cookies[34]). Attraverso gli algoritmi e la classica tecnica statistica di analisi di regressione, si riescono a stimare le relazioni tra le differenti variabili, costruendo un profilo psicografico e facendo predizioni sui comportamenti futuri[35]. Queste attività entrano in contrasto con il diritto all'*autodeterminazione informativa*, ovvero al controllo sulla circolazione dei dati riferiti alla singola persona[36]. La "libertà informatica", come descriveva V. Frosini già nel 1981, ha sia un profilo negativo che uno positivo: il primo è "il diritto di non rendere di dominio pubblico certe informazioni di carattere personale", il secondo esprime invece "la facoltà di esercitare un diritto di controllo sui dati concernenti la propria persona che sono fuoriusciti dalla cerchia della privacy per essere divenuti

30. S.Calzolaio 2024-a.
31. Donati 2018.
32. Richards 2015.
33. Orlando 2022-b.
34. I cookies sono stringhe di testo che vengono posizionate e archiviate sul dispositivo dell'utente dai siti web visitati (noti come "prime parti" o publisher) o da siti o server web differenti (definiti "terze parti"). Questi cookies vengono poi ritrasmessi ai siti di origine durante le visite successive, permettendo di riconoscere l'utente e memorizzare informazioni utili per migliorare l'esperienza di navigazione.
35. Origgi 2018.
36. Bologna 2021.

elementi di input di un programma elettronico"[37]. Nel volume *Armi di distruzione matematica. Come i big data aumentano la disuguaglianza e minacciano la democrazia*, O'Neill[38] solleva una dura critica per quanto concerne l'affidabilità e l'oggettività solo apparente degli algoritmi. Ella avverte che tali strumenti, spesso frutto di una programmazione superficiale, possono essere portatori di pregiudizi insidiosi e dare origine a previsioni di dubbia veridicità. A tal proposito, emblematica è la menzione del software PredPol, impiegato dalla polizia di Los Angeles per la predizione dei crimini, che ha destato non poche preoccupazioni. Oltre a ciò, O'Neill pone l'accento sul potenziale uso distorto degli algoritmi, come dimostrato dallo scandalo Volkswagen, in cui un software è stato utilizzato per alterare fraudolentemente le rilevazioni delle emissioni inquinanti[39].

Il crescente interesse verso i diritti neurali (e la cosiddetta "identità psichica" presente anche nell'art. 4 del GDPR) può fungere da argine contro l'uso scorretto dei dati personali particolari come quelli neurali, e l'elaborazione di quadri giuridici ed etici che integrino innovazione e diritto di beneficiare del progresso scientifico sono degni di attenzione[40]. Un gruppo di neuroscienziati della Columbia University, guidato dal dottor R. Yuste, ha identificato quattro neurodiritti fondamentali da tutelare: il diritto alla privacy mentale e al consenso, il diritto all'identità personale e al libero arbitrio, il diritto all'accesso equo al potenziamento mentale, e il diritto di tutela dagli errori algoritmici[41]. In questo contesto è utile citare anche il caso del Cile, patria del primo tentativo al mondo di istituire un regime di neurodiritti. La legislazione che ha modificato la costituzione cilena, come sottolineato da Liv e Greenbaum[42], è stata presentata come un passo innovativo verso il riconoscimento di nuovi neurodiritti. Tuttavia, come indicano gli autori, ciò non si è realmente realizzato. I legislatori si sono occupati di introdurre un emendamento costituzionale composto da due parti: la prima, di natura dichiarativa, afferma che i progressi scientifici e tecnologici dovrebbero giovare all'umanità e rispettare il diritto alla vita e all'integrità fisica e mentale; la seconda, di carattere operativo, impone invece una regolamentazione giuridica di tali progressi, con particolare attenzione alla "integrità mentale", intesa come protezione dell'attività cerebrale e delle informazioni da essa derivate. È importante notare come la vera innovazione dell'emendamento costituzionale cileno non risieda tanto nel riconoscimento di un nuovo diritto di "integrità mentale" come neurodiritto in sé, quanto piuttosto nell'istituzione di un nuovo contesto giuridico definito da misure regolatorie.

Nonostante le misure rigorose che le aziende dovrebbero adottare dopo il caso *Cambridge Analytica*[43], non a caso società di produzione di analisi psicografiche, e l'attenzione normativa sui diritti dei soggetti profilati grazie all'entrata in vigore del GDPR, i dati degli utenti che circolano sui social

37. Frosini 1981.
38. O'Neill 2017.
39. Amato Mangiameli 2022.
40. Gulotta–Caponi Beltramo 2021.
41. Yuste–Goering–Agüera y Arcas et al. 2017.
42. Liv–Greenbaum 2024.
43. Chester e Montgomery sintetizzano la vicenda relativa al fenomeno Cambridge Analytica: "In March 2018, The New York Times and The Guardian/Observer broke an explosive story that Cambridge Analytica, a British data firm, had harvested more than 50 million Facebook profiles and used them to engage in psychometric targeting during the 2016 US presidential election. The scandal erupted amid ongoing concerns over Russian use of social media to interfere in the electoral process. The new revelations triggered a spate of congressional hearings and cast a spotlight on the role of digital marketing and 'big data' in elections and campaigns. The controversy also generated greater scrutiny of some of the most problematic tech industry practices – including the role of algorithms on social media platforms in spreading false, hateful, and divisive content, and the use of digital micro-targeting techniques for 'voter suppression' efforts. In the wake of these cascading events, policymakers, journalists, and civil society groups have called for new laws and regulations to ensure transparency and accountability in online political advertising". In Chester–Montgomery 2019.

network restano ancora il "petrolio" ambito anche dai protagonisti dell'agone politico. In particolare, si nota un nuovo interesse, anche a fini politici, per la profilazione dei minori, soprattutto in vista del loro primo voto[44]. Anche per questa ragione, alcuni Paesi hanno iniziato, seppur in modo embrionale, a estendere alcune regole già applicate alla stampa e alla televisione anche ai media digitali, con l'obiettivo di limitare il controllo sui dati da parte delle aziende del settore. Un esempio è dato dalla Spagna e dalla Francia, che hanno deciso di applicare ai media online regole come il silenzio elettorale prima dell'apertura dei seggi, il divieto di diffondere sondaggi o exit poll prima delle elezioni e le limitazioni relative alla pubblicità politica durante le campagne elettorali[45].

4. *Targeting* politico e protezione dei dati personali, tentativi di soluzione europei

Dal punto di vista della privacy, la profilazione presenta implicazioni significative: nel contesto normativo italiano è stata storicamente considerata un'attività di trattamento dei dati particolarmente rischiosa. Inoltre, questa viene concepita come una finalità autonoma, indipendente e specifica, che richiede una base giuridica chiara ed adeguata al fine di essere considerata legittima[46].

In tal senso, l'Unione europea ha avviato diverse iniziative che hanno lo scopo di mitigare le manipolazioni sui processi democratici nel contesto digitale. Una delle prime e più significative è stata l'introduzione del Regolamento Generale sulla Protezione dei Dati (GDPR), entrato in vigore nel 2018, in cui vengono indicate le basi giuridiche per il trattamento dei dati nella società digitale, volte ad assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche all'interno dell'Unione. Questo regolamento si dimostra anche un elemento chiave nella strategia dell'Ue per la regolamentazione del digitale e aiuta a prevenire e contrastare le pratiche di disinformazione e di manipolazione che si basano sull'uso improprio dei dati personali. Il GDPR mira infatti a rafforzare la protezione e il controllo dei dati personali dei cittadini, sia all'interno dell'Ue che oltre i suoi confini, introducendo diritti che si collegano alla sfera dell'identità online dell'individuo (come il diritto all'oblio, alla cancellazione, alla limitazione e alla rettifica) e procedure per prevenire le violazioni dei dati e limitare gli effetti dannosi della perdita, divulgazione non autorizzata o accesso illecito ai dati[47]. Tra i principi fondamentali della normativa sulla protezione dei dati personali, vi è l'obbligo secondo cui il titolare del trattamento debba sempre identificare una base giuridica adeguata prima di iniziare qualsiasi attività di trattamento dei dati, la quale costituisce la condizione necessaria per la liceità del trattamento stesso. In base alla definizione del Regolamento, l'uso del consenso come base giuridica per il trattamento dei dati dipende strettamente dalla presenza dei requisiti necessari per renderlo valido, ovvero liberamente prestato. Il titolare del trattamento deve quindi verificare che tutti i requisiti previsti dalla normativa siano soddisfatti. In definitiva, è essenziale che il consenso garantisca all'interessato un vero controllo sul trattamento dei propri dati personali e sulle modalità di esecuzione, evitando che tale controllo risulti solo apparente o illusorio[48].

Per ciò che concerne invece le attività elettorali, il GDPR al considerando 56 recita: "Se, nel corso di attività elettorali, il funzionamento del sistema democratico presuppone, in uno Stato membro, che i partiti politici raccolgano dati personali sulle opinioni politiche delle persone, può esserne consentito il trattamento di tali dati per motivi di interesse pubblico, purché siano predisposte garanzie adeguate". Si nota dunque come la normativa europea abbia riconosciuto in questa sede l'importanza del trattamento dei dati personali da parte dei partiti politici durante le attività elettorali per il buon funzionamento del sistema democratico. In tale contesto, è stato sostenuto che consentire agli attori politici il trattamento dei dati personali a fini di propaganda elettorale costituisca un

44. Ziccardi 2020.
45. Stegher 2023.
46. Banterle 2018.
47. Giacomini 2023.
48. Cassano–Colarocco–Gallus–Micozzi 2018.

"dovere democratico". Tuttavia, è altresì essenziale bilanciare questa esigenza con limiti rigorosi atti a prevenire un utilizzo invasivo e distorto degli strumenti impiegati per tali finalità[49].

L'art. 22 del GDPR, intitolato "Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione"[50], prevede che, tranne per determinate eccezioni, le decisioni prese in seguito a trattamenti automatizzati di dati personali non possono basarsi su "categorie particolari di dati", ovvero su quelle categorie di dati personali particolarmente sensibili che si ritrovano nell'art. 9 del GDPR, come ad esempio lo stato di salute, il credo religioso, la convinzione politica o l'appartenenza sindacale. Il "diritto alla conoscibilità" dell'algoritmo[51] è strettamente connesso al "diritto di ricevere un'informativa" rispetto al trattamento dei dati effettuato dal titolare, a cui fa riferimento l'art. 13 del medesimo Regolamento Ue[52]. Le linee guida europee sul processo decisionale automatizzato[53], tuttavia, hanno adottato un approccio più prudente nell'interpretare questi riferimenti. Viene infatti riconosciuto che l'interessato ha il diritto di essere informato circa l'esistenza di tali processi decisionali e di ricevere "informazioni significative sulla logica utilizzata", permettendogli così di comprendere la ragione dei trattamenti, specialmente quando le conseguenze potrebbero essere particolarmente rilevanti. Eppure, è importante notare che, nonostante queste indicazioni, non viene esplicitamente menzionato il concetto di *explainability* in modo diretto nel testo normativo[54]. Considerando che i modelli basati sulla monetizzazione dei dati sono ormai una realtà nei mercati dei servizi digitali, la dottrina più attenta si sta interrogando su quale possa essere la base giuridica, ai sensi dell'articolo 6 del GDPR, per legittimare tali trattamenti. In particolare, sono emersi dubbi riguardo alla liceità del trattamento di dati che vanno oltre quelli strettamente necessari per la fornitura del servizio[55]. Un esempio significativo è, come già sottolineato, quello rappresentato dai dati di navigazione degli utenti raccolti dalle piattaforme social, utilizzati per finalità come la pubblicità comportamentale e la personalizzazione dei contenuti[56]. Si rende necessario considerare anche i diritti, strettamente connessi fra loro, alla rettifica e alla cancellazione dei dati, postulati dall'art. 16 e 17 del Regolamento. Ai sensi dell'art. 16, all'interessato spetta il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo, nonché

49. Sborlini 2022.

50. L'art. 22 dispone che "l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona". La norma non si applica nel caso in cui la decisione automatizzata: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato. Nei casi di cui alle lettere a) e c), "il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, a meno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione".

51. S.Calzolaio 2017.

52. Mancarella 2022.

53. European Commission 2018.

54. Spiller 2021.

55. Nel contesto descritto è evidente come l'adozione di dati anonimizzati o sintetici (e teoricamente non più personali perché non riconducibili a una persona identificata o identificabile) non sia sempre una soluzione adeguata (si pensi al microtargeting o a studi in ambito medico che incentrano l'attenzione su pazienti specifici). In concreto, se l'uso di dati completamente anonimi o sintetici può ridurre sostanzialmente il rischio di reidentificazione, questa potrebbe non essere una soluzione in tutte le circostanze, poiché in taluni casi, "the truthfulness of the data is lost". Per approfondimenti: Stalla-Bourdillon–Thuermer–Walker et al. 2020,

56. Di Cerbo 2022.

quello di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa. Non a caso, il considerando n. 65 del Regolamento tratta congiuntamente il diritto alla rettifica dei dati e quello alla loro cancellazione: entrambi, infatti, sono collegati al diritto individuale alla corretta rappresentazione della "personalità digitale", ovvero alla tutela della cosiddetta "reputazione digitale" (*web reputation*), di cui oggi sempre più frequentemente si invoca la tutela in sede civile e penale[57].

Nel 2018, l'Ue ha inoltre lanciato il *Code of Practice on Disinformation*, un codice di condotta (*soft law*) poi rafforzato nel 2022, sulla disinformazione che si occupa di stabilire una serie di impegni volontari per le piattaforme online aderenti[58]. Tra questi impegni, vi è la promessa di migliorare la trasparenza della pubblicità politica e di prevenire la diffusione di fake news. Riconoscendo l'importanza della pubblicità politica nel plasmare il dibattito pubblico e l'opinione dei cittadini, il codice rafforzato impone ai firmatari di adottare misure di trasparenza più stringenti. Queste misure sono volte a garantire che gli utenti possano identificare chiaramente e facilmente gli annunci politici. In particolare, i firmatari devono implementare un sistema di etichettatura più efficace che evidenzi chiaramente quando un contenuto è un annuncio politico, includendo dettagli essenziali come l'identità dello sponsor, la spesa pubblicitaria sostenuta per l'annuncio e il periodo durante il quale l'annuncio è visibile[59]. Il processo di autoregolamentazione dei social network si colloca all'interno di una strategia promossa dalla Commissione europea, che mira a coinvolgere gli stakeholder nella definizione dei principi e delle direttive necessari per creare una disciplina comune in questo ambito. L'iniziativa punta a lasciare agli stessi social network la responsabilità di implementare le regole più adatte alla loro natura e struttura. Il progetto includeva anche una roadmap per la verifica e l'aggiornamento delle regole adottate dai vari social network coinvolti, garantendo così una continua evoluzione e adeguamento delle normative[60].

La *disinformation* e la *misinformation* sono state inserite tra i rischi sistemici per i processi democratici dall'Ue anche nel Regolamento Ue n. 2065/2022 (*Digital Services Act*), il quale, al considerando 104 statuisce che la disinformazione o le attività di manipolazione e abuso rappresentano rischi sistemici concreti ed effettivi per la democrazia e la società[61]. Il regolamento mira a responsabilizzare maggiormente le piattaforme digitali e a creare un ambiente online più sicuro, richiedendo politiche chiare sui contenuti falsi e manipolati e fornendo maggiore trasparenza sul funzionamento degli algoritmi utilizzati. Il DSA vuole essere uno strumento di aggiornamento e modernizzazione della normativa contenuta nella Direttiva e-commerce, adeguandola agli sviluppi tecnologici e sociali degli ultimi vent'anni, contribuendo a sviluppare condizioni di maggiore sicurezza in rete e riponendo un particolare accento sulle garanzie di tutela degli utenti e sulla protezione della loro libertà di espressione. Per raggiungere questi obiettivi, la Commissione europea ha introdotto obblighi specifici per le grandi piattaforme tecnologiche, note come *big tech*. Queste aziende sono tenute ad assumersi una maggiore responsabilità per quanto riguarda i contenuti illegali o dannosi che vengono diffusi sulle loro piattaforme. L'approccio adottato si basa sulla necessità di bilanciare la libertà di espressione con la protezione degli utenti, cercando di ridurre la diffusione di contenuti nocivi senza limitare ingiustamente la libera circolazione delle idee e delle informazioni[62]. Come descritto, le attività delle piattaforme online infatti non influenzano solo le relazioni economiche e commerciali, ma

57. Allegri 2018.
58. Per porre un argine alla manipolazione dell'informazione sulle piattaforme digitali, il 13 febbraio 2025, la Commissione europea e lo European Board for Digital Services (Comitato Europeo per i Servizi Digitali) hanno approvato l'integrazione ufficiale del Codice di condotta volontario sulla disinformazione nel quadro del *Digital Services Act* (DSA).
59. Commissione europea 2022.
60. Bonini 2020.
61. Ladu–Maccabiani 2023.
62. Flaminio 2022.

rivestono anche un ruolo decisivo nella comunicazione politica e sociale. Non sorprende più che la comunicazione sui social media abbia superato quella dei media televisivi e giornalistici, raggiungendo un pubblico più ampio e diversificato. Il contesto attuale non riguarda solo la sorveglianza dei poteri pubblici sugli individui, ma anche la sorveglianza dei poteri monopolistici privati (*big tech*) nella sfera privata e persino la sorveglianza "alla pari" tra individui, che assumono ruoli reciproci di produttori e consumatori di contenuti all'interno della stessa community[63]. Nello specifico, l'articolo 26 del DSA, intitolato "Pubblicità sulle piattaforme online", estende i diritti degli utenti dei servizi digitali i quali devono essere messi nella condizione di poter identificare chiaramente, in modo conciso e inequivocabile, e in tempo reale, quando un post costituisce una pubblicità. Devono essere informati su ciò che concerne: la persona fisica o giuridica per conto della quale è presentata la pubblicità, chi paga per la pubblicità (se diverso dall'inserzionista) e i parametri utilizzati per determinare a chi viene mostrata la pubblicità, con la possibilità di modificarli quando ciò è applicabile. Analogamente, l'articolo 27, intitolato "Trasparenza dei sistemi di raccomandazione", mira a garantire una maggiore trasparenza per i consumatori, cercando di riequilibrare l'asimmetria informativa nei rapporti *business to consumer* (B2C)[64]. Questo articolo introduce il diritto degli utenti di richiedere la modifica dei criteri di personalizzazione dei contenuti mostrati loro. I gestori delle piattaforme sono obbligati a specificare, in un linguaggio chiaro e comprensibile, i principali parametri utilizzati nei loro sistemi di raccomandazione e le ragioni per cui vengono suggerite determinate informazioni. Inoltre, gli utenti devono poter accedere a opzioni che permettano loro di modificare tali parametri in qualsiasi momento tramite una sezione dedicata dell'interfaccia della piattaforma, determinando autonomamente a quali informazioni dare priorità[65]. Per inquadrare correttamente da un punto di vista giuridico la tecnologia a monte del funzionamento degli algoritmi, il *machine learning*, ed evitare interpretazioni avventate, come l'idea di una "personalità elettronica", è sufficiente considerare che l'output ottenuto dall'applicazione di un algoritmo (processo) sui dati disponibili (input) non costituisce una regola generale, ma piuttosto un risultato specifico, così come specifico è l'input di partenza. Questo carattere "dal particolare al particolare" permette di classificare questi software di machine learning come procedure di tipo induttivo o inferenziale, e non come sussuntive (dal generale al particolare) o astrattive (dal particolare al generale). In tal senso, il *machine learning* richiama la definizione contenuta nell'art. 2727 del Codice Civile riguardante le presunzioni: "le presunzioni sono le conseguenze che la legge o il giudice trae da un fatto noto per risalire a un fatto ignorato", e, citando O'Neil: "(…) *an algorithm – an opinion formalized in code*"[66].

Il considerando 69 del DSA descrive il caso in cui le inserzioni pubblicitarie vengano presentate ai destinatari attraverso tecniche di targeting mirate ai loro interessi e vulnerabilità, con la possibilità concreta che queste vadano a generare effetti negativi significativi con ripercussioni su interi gruppi, contribuendo ad alimentare campagne di disinformazione e discriminando fasce vulnerabili della popolazione. Le piattaforme online, essendo particolarmente suscettibili a tali dinamiche amplificano i rischi in tal senso. Di conseguenza, i fornitori di queste piattaforme dovrebbero astenersi dall'utilizzare tecniche di profilazione che si basano su categorie particolari di dati personali, come stabilito all'articolo 4, punto 4), e all'articolo 9, paragrafo 1, del GDPR. Il regolamento riconosce che la potenzialità di creare dei danni aumenta rispettivamente all'aumentare delle dimensioni del pubblico di utenti delle piattaforme online. Per mitigare questi rischi, il DSA prevede obblighi aggiuntivi per le piattaforme online molto grandi (quelle con 45 milioni o più di utenti attivi mensili medi nell'Ue). Tra gli obblighi imposti a queste piattaforme si ritrova la necessità di condurre una valutazione annuale dei rischi sistemici significativi causati dai loro servizi e dall'uso che ne viene fatto nell'Unione. Il concetto di "rischi sistemici" si riferisce, tra l'altro, alla diffusione di contenuti

63. Caggiano 2021.

64. Pizzetti–Calzolaio–Iannuzzi et al. 2024.

65. Di Cerbo 2024.

66. Imbruglia 2022.

illegali, alle esternalità negative sui diritti umani e alla manipolazione intenzionale dei loro servizi (articolo 26(1)). Quando vengono identificati rischi sistemici, le piattaforme molto grandi devono adottare misure di mitigazione ragionevoli, proporzionate ed efficaci, come l'adattamento dei loro sistemi di raccomandazione[67]. Si legano al DSA le linee guida rilasciate dalla Commissione e destinate alle piattaforme online e ai motori di ricerca di grandi dimensioni[68], il cui obbiettivo è quello di ridurre i rischi sistemici online che possono influenzare l'integrità dei processi elettorali (è stata prestata una attenzione particolare anche alle passate elezioni del Parlamento europeo dello scorso giugno 2024[69]). Le linee guida suggeriscono misure di mitigazione e pratiche ottimali che le piattaforme e i motori di ricerca di grandi dimensioni dovrebbero adottare prima, durante e dopo gli eventi elettorali.

Sulla base degli sforzi precedentemente descritti, la Commissione europea ha adottato diverse misure per tutelare la libertà e il pluralismo dei media nell'Ue, oltre a promuovere la libera circolazione dei servizi. Questi interventi hanno portato all'approvazione dell'European Media Freedom Act (EMFA), entrato in vigore il 7 maggio 2024. Le nuove norme saranno applicate completamente a partire dall'8 agosto 2025[70]. Per ciò che concerne la presente ricerca, è utile segnalare come il regolamento proponga un meccanismo per evitare che le grandi piattaforme online, come Facebook, X (ex Twitter) o Instagram possano limitare o rimuovere arbitrariamente i contenuti dei media indipendenti. Le piattaforme saranno obbligate a distinguere tra fonti indipendenti e non indipendenti. In caso di intenzione di rimuovere o limitare un contenuto, i media verranno informati e avranno 24 ore per rispondere. Solo dopo la risposta, o in sua assenza, la piattaforma potrà procedere alla rimozione o limitazione del contenuto se questo non rispetta le condizioni della piattaforma. I media potranno inoltre ricorrere a un organo di risoluzione delle controversie extragiudiziale e richiedere un parere dell'European Board for Media Practices (nuovo organo dell'Ue composto da regolatori nazionali, che sarà istituito dal regolamento EMFA)[71]. Accanto a questo regolamento è utile citare anche il *Digital Markets Act* (DMA) che introduce una regolamentazione innovativa e incisiva. Il regolamento intende stabilire una normativa *ex ante* che affianchi e integri la tradizionale disciplina antitrust, con l'obiettivo di promuovere la concorrenza in mercati sempre più dominati dalle *big tech*. In particolare, esso prevede nuovi e stringenti obblighi per le imprese considerate *gatekeeper* (controllori dell'accesso al settore dei servizi e delle piattaforme online), che, grazie alla loro posizione di forza, possono erigere barriere all'ingresso di nuove aziende in mercati come il social networking, il cloud computing e la messaggistica[72].

Risulta interessante citare anche l'esempio dell'ordinamento francese che ha introdotto una normativa specifica per contrastare la manipolazione dell'informazione digitale, soprattutto in relazione all'esercizio dei diritti democratici. Nel dicembre 2018, infatti, è stata promulgata la legge n. 1202, conosciuta come *Loi relative à la lutte contre la manipulation de l'information*. Lo stesso giorno, il 22 dicembre 2018, è stata approvata anche la legge organica n. 1201, composta da soli due articoli, che ha coordinato la normativa con alcune disposizioni di rilevanza costituzionale. La normativa tenta di offrire una regolamentazione complessiva per combattere la disinformazione, sia nell'ambito digitale che nei media tradizionali, soprattutto quando questi ultimi sono influenzati

67. Cauffman–Goanta 2021.
68. Orientamenti della Commissione per i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi sull'attenuazione dei rischi sistemici per i processi elettorali a norma dell'articolo 35, paragrafo 3, del Regolamento (UE) 2022/2065. Data di applicazione: 26 aprile 2024.
69. Secondo il *Digital Services Act* (DSA), i servizi con oltre 45 milioni di utenti attivi nell'Ue hanno l'obbligo di affrontare i rischi legati alle elezioni, garantendo al contempo la protezione dei diritti fondamentali, come la libertà di espressione.
70. Vedi la pagina web della Commissione europea *Un nuovo slancio perla democrazia europea*.
71. V. Comunicato stampa del Parlamento europeo.
72. Donati 2021.

da Stati stranieri. L'obiettivo principale è proteggere il sistema democratico francese da manipolazioni esterne che potrebbero destabilizzarlo oltre il normale dibattito politico[73].

In conclusione, nel contesto europeo, il comune patrimonio culturale ha portato i paesi dell'area occidentale, con una tradizione radicata nel costituzionalismo, a sviluppare spontaneamente "principi comuni" all'interno della loro legislazione. La possibilità di un'ulteriore convergenza tra i vari ordinamenti europei sembra strettamente legata alla specificità del contesto europeo, caratterizzato dalla cooperazione multilivello tra istituzioni operanti a livello internazionale, sovranazionale e nazionale. Questa cooperazione si manifesta, da un lato, nella condivisione di istituti giuridici tra le diverse normative nazionali e, dall'altro, attraverso una serie di convenzioni regionali di natura internazionalistica che, in un processo virtuoso, si nutrono delle diverse espressioni di questa tradizione comune, le riflettono, le elaborano e le sintetizzano, reintegrandole successivamente nei singoli ordinamenti nazionali come risultato di esperienze condivise[74].

5. Il regolamento europeo in materia di targeting e trasparenza della pubblicità politica (2024/900)

L'11 marzo 2024 il Consiglio ha adottato un nuovo regolamento europeo relativo alla trasparenza e al targeting della pubblicità politica, volto a contrastare la manipolazione delle informazioni e le ingerenze straniere nelle elezioni. Le nuove norme riguardano la trasparenza e il targeting della pubblicità politica in relazione a un'elezione, a un referendum o a un processo legislativo a livello dell'Ue o in uno Stato membro. Queste non pregiudicano il contenuto dei messaggi di pubblicità politica né altri aspetti relativi alla pubblicità politica, come lo svolgimento di campagne politiche, che rimangono soggette alle norme nazionali specifiche degli Stati membri[75]. In questa sede, l'attenzione sarà posta sulle disposizioni relative alla protezione dei dati personali e ad aspetti di natura costituzionale.

I comma 2 e 3 dell'art.1 del regolamento forniscono interessanti spunti di riflessione, indicando oggetto e obbiettivi del regolamento, occupandosi di escludere "opinioni politiche e altri contenuti editoriali soggetti alla responsabilità editoriale, indipendentemente dal mezzo attraverso cui sono espressi" a patto che non sia previsto un pagamento specifico o altra remunerazione per "la loro preparazione, collocazione, promozione, pubblicazione, consegna o diffusione da parte di terzi o in relazione a tali attività" assieme a "opinioni politiche espresse a titolo personale" le quali "non sono considerate pubblicità politica". Il regolamento dunque non va ad interferire con l'art. 21 della Costituzione italiana, il quale si occupa di garantire la libertà di espressione[76]. Può essere utile ricordare che nel nostro Paese, come descritto da C. Bologna[77], la dottrina dominante sottolinea, alla luce dell'ampia formulazione dell'art. 21 e dell'ispirazione personalista che la permea, il carattere individualistico della libertà di manifestazione del pensiero, anziché un'impostazione funzionalistica. Questo approccio è confermato dall'assenza, nella nostra Costituzione, di disposizioni analoghe all'art. 18 della Legge fondamentale tedesca, che regola l'abuso del diritto orientando l'esercizio della libertà verso il perseguimento di specifici valori politici[78]. Al contrario, la Costituzione italiana adotta un modello pienamente pluralista in materia di libertà di espressione, come dimostrato anche dalla scelta di escludere il limite dell'ordine

73. Fabiano 2023.

74. Borrello 2021.

75. Consiglio Europeo 2024.

76. "Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione. […] La stampa non può essere soggetta ad autorizzazioni o censure".

77. Bologna 2021.

78. La legge fondamentale tedesca, come sottolineato da M. Manetti, ripropone a tal fine il concetto di "abuso del diritto" nell'ambito di un ordine ideale di rango costituzionale che non vada solamente a condizionare in maniera esplicita l'esercizio della libertà di pensiero ma che si proponga anche di rifondare il concetto stesso di tale libertà, inserendovi un vincolo che leghi l'individuo alla collettività.

pubblico dal testo dell'art. 21[79]. Si ricorda infatti che lo Stato liberale ha attribuito alla libertà di opinione e di stampa valore costitutivo della sua forma politica, sancendone però al contempo il divieto di "abuso"[80]. Durante il fascismo, pertanto, tale limite era stato interpretato in maniera estensiva, trasformandosi in una clausola suscettibile di essere riempita con i valori dominanti dell'epoca. Di fatto, il regime fascista si è distinto per la tendenza ad estendere il proprio controllo sulle condizioni di esercizio della libertà di stampa, tramite l'istituzione dell'Ordine e dell'Albo dei giornalisti, inteso come meccanismo di filtraggio e accesso "politico" di coloro che avessero voluto esercitare la professione giornalistica, con l'effetto di effettuare un'azione censoria sul contenuto degli stampati[81].

Oggi, la libertà di propaganda, come dichiarato chiaramente dalla Corte costituzionale nella sentenza n. 84 del 1969, è considerata come un'espressione della libertà di manifestazione del pensiero, garantita dall'art. 21 della Costituzione e definita come la pietra angolare dell'ordine democratico. In aggiunta a ciò, le esigenze di tutela del regime democratico, all'interno della Carta costituzionale italiana, possono operare soltanto come un "limite" esterno e non come fondamento di questa libertà, così come delle altre libertà inviolabili[82]. Secondo Spataro[83], sia l'art. 21 della Costituzione che gli artt. 48 e 49 hanno un contenuto difensivo nei confronti di possibili abusi del potere pubblico. Inoltre, questi articoli implicano che il potere pubblico debba compiere interventi positivi finalizzati all'integrazione dei cittadini nella comunità politica statale attraverso una partecipazione reale. Questo approccio mira a evitare "il divorzio tra la titolarità del diritto politico e il suo esercizio". Pertanto, spetta al legislatore garantire le condizioni necessarie per una rappresentanza politica democratica efficace. Risulta utile sottolineare che il ruolo fondamentale attribuito ai partiti dall'art. 49 della Costituzione in questo contesto è centrale: essi sono chiamati a garantire ai cittadini la possibilità di partecipare in maniera democratica alla definizione delle politiche nazionali. Rinunciare a tale funzione significherebbe compromettere il sistema democratico della Repubblica, così come previsto dalla Costituzione. È pertanto compito dei partiti stessi recuperare questo ruolo, che costituisce la loro ragion d'essere: in un contesto dominato dalle tecnologie dell'informazione e della comunicazione (ICT), risulta indispensabile adottare modelli organizzativi che sfruttino queste risorse, senza però trascurare i rischi che esse comportano. Non basta semplicemente impiegare gli strumenti tecnologici, ma è cruciale saperne gestire l'influenza, preservando la propria funzione costituzionale; i partiti devono dunque proporre politiche che non siano limitate alla contingenza del momento o alle emozioni e opinioni del web o delle piazze, ma che riflettano un orizzonte più ampio e lungimirante[84].

Il nuovo regolamento si occupa dunque di distinguere quelli che sono i contenuti organici, ovvero quelli diffusi all'interno di una piattaforma online a titolo personale, senza il pagamento di un servizio di promozione, e quelli sponsorizzati, che vengono mostrati agli utenti a fronte di un compenso versato alla piattaforma. Il regolamento si concentra in particolare sulla pubblicità politica (e non sulla propaganda), definendola all'articolo 3 come "la preparazione, collocazione, promozione, pubblicazione, consegna o diffusione, con qualsiasi mezzo, di un messaggio fornito normalmente dietro retribuzione o tramite attività interne o nell'ambito di una campagna di pubblicità politica". Tuttavia, la distinzione tra contenuti sponsorizzati e organici può risultare ambigua. Alcuni contenuti, pur non essendo ufficialmente sponsorizzati, riescono a ottenere una vasta diffusione grazie alla viralità, all'uso strategico degli algoritmi e all'abilità di social media manager e *data analyst*

79. Pace–Manetti 2006.

80. Lo Statuto Albertino, all'art. 28 recitava: "La Stampa sarà libera, ma una legge ne reprime gli abusi. Tuttavia le bibbie, i catechismi, i libri liturgici e di preghiere non potranno essere stampati senza il preventivo permesso del Vescovo".

81. Caretti–Cardone 2019.

82. Barbera 1975.

83. Spataro 2022.

84. Morana 2021.

nel massimizzare la visibilità dei messaggi. Questo scenario solleva interrogativi sulla possibilità di aggirare le normative sfruttando meccanismi di amplificazione algoritmica, rendendo più complessa la regolamentazione della pubblicità politica online. Nell'ecosistema della comunicazione politica online, un ruolo significativo è svolto anche dagli influencer, inclusi i micro-influencer, e dagli attivisti, che possono contribuire alla diffusione di determinati messaggi senza che questi rientrino formalmente nella categoria della pubblicità sponsorizzata. Inoltre, le campagne di pubblicità politica possono talvolta fare ricorso a strategie opache o poco trasparenti, come l'uso di reti di social bot, l'attività coordinata di troll, il fenomeno dell'*astroturfing* (ovvero la creazione artificiale di consenso tramite account falsi o organizzazioni fittizie) e l'impiego di *potëmkin personas*, identità digitali costruite ad hoc per influenzare il dibattito pubblico. Questi meccanismi complicano ulteriormente la distinzione tra contenuti organici e sponsorizzati, rendendo più difficile il monitoraggio della trasparenza nella comunicazione politica online. Tale dinamica contribuisce a rendere particolarmente complessa la distinzione tra i messaggi veicolati, i soggetti che li diffondono e coloro che ne sono i reali promotori. Il considerando 30 del regolamento fornisce un segnale che dimostra la consapevolezza dei regolatori del possibile manifestarsi di determinate problematiche: "Un'opinione politica non dovrebbe essere considerata espressa a titolo personale se è prevista una remunerazione specifica da parte di terzi, comprese prestazioni in natura, a fronte dell'espressione di tale opinione o in relazione alla stessa".

Se la libertà di pensiero si compone di due aspetti fondamentali, la formulazione di un'idea e l'utilizzo di un mezzo per la sua diffusione e per la sua acquisizione, è indiscutibile che Internet, per sua stessa natura, offra agli individui enormi possibilità di esprimere e diffondere idee in uno spazio sociale teoricamente più libero e accessibile, in quanto privo di barriere. Tuttavia, è indispensabile sottolineare che la vastissima quantità di informazioni presenti online, prodotta in modo decentralizzato e spesso disorganizzato, richiede un certo ordine per poter essere realmente fruibile dagli utenti[85]. Per questo motivo, sono necessari strumenti che organizzino le notizie sulle pagine web e ne determinino il livello di visibilità, non limitatamente a ciò che concerne i contenuti sponsorizzati.

Il regolamento non estingue del tutto la problematica appena descritta, ma stabilisce in maniera esclusiva: "norme armonizzate sull'uso delle tecniche di targeting e consegna del messaggio pubblicitario che comportano il trattamento di dati personali nel contesto della fornitura di pubblicità politica online" con l'obbiettivo di "tutelare i diritti e le libertà fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, in particolare il diritto alla vita privata e la protezione dei dati personali". Viene ravvisata quindi la necessità di intervenire a livello europeo per assicurare una protezione settoriale aggiuntiva ai dati personali trattati per il targeting della pubblicità politica[86], andando oltre, per certi versi, quelle che sono le tutele stabilite dal GDPR. Quest'ultimo prevede già il principio di finalità (contenuto nell'art. 5), il quale comporta il divieto di raccolta e uso di dati personali a fini di targeting elettorale tramite processi di *web crawling*[87]. Su questo tema, il Garante per la protezione dei dati personali è intervenuto più volte, ribadendo gli obblighi normativi che partiti e candidati devono osservare durante le campagne elettorali. In particolare, l'Autorità ha imposto il divieto di utilizzare, per propaganda elettorale e comunicazione politica, dati liberamente accessibili online, inclusi quelli raccolti automaticamente attraverso software specifici o

85. Bazzoni 2019.

86. Il Regolamento offre definizioni per circoscrivere e stabilire il significato di "tecniche di targeting", indicate come "le tecniche usate per rivolgere un messaggio di pubblicità politica solo a una persona specifica o a un gruppo specifico di persone, o per escludere tale persona o gruppo di persone, sulla base del trattamento di dati personali" e le "tecniche di consegna del messaggio pubblicitario", definite come "tecniche di ottimizzazione utilizzate per aumentare la circolazione, la portata o la visibilità di un messaggio di pubblicità politica sulla base del trattamento automatizzato di dati personali e che possono servire a consegnare il messaggio di pubblicità politica a una persona specifica o a un gruppo specifico di persone".

87. Califano 2022.

provenienti da social network, forum o newsgroup, tra cui quelli pubblicati dagli interessati stessi sui social network[88]. La questione relativa al consenso risulta centrale anche nel nuovo regolamento[89]. Il titolare deve infatti ottenere il consenso esplicito e separato per le finalità di targeting e pubblicità politica e tener conto di una garanzia aggiuntiva offerta dal regolamento: "l'obbligo di ottenere il consenso al trattamento dei dati personali non può essere evitato affermando che l'interessato ha reso pubblici i dati personali in questione". A supporto di quanto dichiarato, il considerando 81 include al suo interno un rimando alla "sentenza della Corte di giustizia del 4 luglio 2023 nella causa C-252/21, *Meta Platforms e a.* (Condizioni generali di utilizzo di un social network)", con l'obbiettivo di ribadire la necessarietà di un consenso che sia prestato liberamente e che non vada ad influire sull'accesso ai servizi, e che sia dunque separato dal consenso richiesto per altre finalità al di fuori da quelle per marketing politico[90]. L'obbligo di fornire un'alternativa alla pubblicità politica viene ribadito anche dall'art. 18[91], al comma 4, in cui è stabilito che: "all'interessato che non presta il proprio consenso sia offerta un'alternativa equivalente per l'utilizzo del servizio online senza ricevere pubblicità politica". Un aspetto di particolare rilevanza su cui si è soffermata la Corte di giustizia riguarda la base giuridica utilizzabile per il trattamento dei dati personali ai fini di pubblicità mirate. Generalmente, le piattaforme digitali adottano la posizione secondo cui tale trattamento possa basarsi sull'art. 6, par. 1, lett. f) del Regolamento generale sulla protezione dei dati (GDPR), ossia sul legittimo interesse del titolare del trattamento o di terzi. Tale interpretazione trova un possibile appoggio nel considerando 47 del GDPR, dove si afferma che il trattamento dei dati personali per finalità di marketing diretto possa essere considerato un legittimo interesse[92]. Secondo l'interpretazione del GDPR, il modello "*pay-or-okay*" di Meta non garantisce che il consenso sia prestato liberamente, poiché viene richiesto in un contesto di squilibrio di potere, in modo condizionato, non specifico e dannoso, rendendo il consenso invalido ai sensi dell'articolo 6 del GDPR. Diverse Autorità garanti hanno però riconosciuto la legittimità di questi modelli andando a stabilire ulteriori condizioni specifiche, come la ragionevolezza del prezzo e l'equivalenza delle alternative. Di conseguenza, anche se il modello di Meta potrebbe, con alcune modifiche, essere conforme alle diverse condizioni dei Garanti, non si può sostenere che il consenso degli utenti sia prestato liberamente, il che renderebbe la pratica non conforme al GDPR[93].

Trattando dati personali, segnatamente categorie particolari di dati personali ai sensi dell'art. 9 del regolamento GDPR, è possibile segmentare diversi gruppi elettorali o di privati cittadini e sfruttarne le caratteristiche o vulnerabilità, ad esempio, diffondendo messaggi di pubblicità politica in momenti e luoghi ad hoc per trarre vantaggio da situazioni in cui potrebbe essere più acuta la sensibilità a un certo tipo di informazione/messaggio. Tale trattamento dei dati personali, come segnala il considerando 74 del Regolamento 900, va a generare un impatto negativo sui diritti e sulle libertà fondamentali delle persone, come il diritto di essere trattate in modo equo e paritario, non essere manipolate, ricevere informazioni obiettive, farsi

88. *Provvedimento in materia di propaganda elettorale e comunicazione politica* - 18 aprile 2019.

89. Il consenso al trattamento dei dati personali è dato e revocato in conformità ai regolamenti (UE) 2016/679 e (UE) 2018/1725.

90. "Alla luce della sentenza della Corte di giustizia del 4 luglio 2023 nella causa C-252/21, *Meta Platforms e a.* (Condizioni generali di utilizzo di un social network), gli interessati dovrebbero disporre della libertà di rifiutare, nell'ambito della pubblicità politica, di prestare il loro consenso a operazioni particolari di trattamento di dati, senza essere per questo tenuti a rinunciare integralmente alla fruizione di un servizio online. Come dichiarato dalla Corte di giustizia, a tali utenti dovrebbe essere proposta un'alternativa equivalente non accompagnata da simili operazioni di trattamento di dati".

91. L'art. 18 si occupa di stabilire obblighi specifici in materia di tecniche di targeting e di consegna del messaggio pubblicitario in ambito di pubblicità politica online.

92. Battaglia 2023.

93. D'Amico–Pelekis–Santos–Duivenvoorde 2024.

un'opinione, prendere decisioni politiche ed esercitare il diritto di voto. Il considerando prosegue indicando inoltre come queste tecniche vadano ad incidere negativamente sul processo democratico, in quanto conducono a una frammentazione del dibattito pubblico su importanti questioni sociali, a una comunicazione selettiva e, in ultima analisi, alla manipolazione dell'elettorato.

Di particolare interesse è il considerando 79 del nuovo regolamento, perché amplia le garanzie a favore dell'utente rispetto a quanto stabilito dall'art. 9 del GDPR. In concreto, il Regolamento 900, sostiene che nei casi in cui un utente di un social network, nella sua attività di navigazione, visiti una pagina, utilizzi un'applicazione o qualsiasi funzione di un servizio online (per esempio, l'acquisto, per se stesso o terzi di libri a carattere politico, l'utilizzo di applicazioni di preghiera, etc.) a cui si possono riferire una o più categorie di cui all'articolo 9, paragrafo 1 del GDPR, il trattamento di tali dati da parte del gestore dovrebbe essere considerato un trattamento di categorie particolari di dati personali, che è, in linea di principio, vietato (qualora tale trattamento di dati consenta di rivelare informazioni che rientrino in una di tali categorie, anche se tali informazioni non sono necessariamente conformi con l'idea o il pensiero dell'interessato stesso).

Inoltre, si ricorda che l'art. 9 del GDPR prevede alcune eccezioni al divieto di trattare categorie particolari di dati, una delle quali riguarda i dati personali che sono stati resi manifestamente pubblici dall'interessato stesso. Ciò significa, se un interessato rende volontariamente e apertamente accessibili al pubblico alcuni dati sensibili, per esempio attraverso social media o altre piattaforme pubbliche, tali dati potrebbero essere trattati senza che il titolare del trattamento debba rispettare le severe restrizioni normalmente imposte per le categorie particolari di dati personali. Il considerando 80 del nuovo regolamento pone un limite a questa eccezione: "ai fini del presente regolamento, l'obbligo di ottenere il consenso al trattamento dei dati personali non può essere evitato affermando che l'interessato ha reso pubblici i dati personali in questione". Tale limite è in linea con quanto stabilito anche dal DSA e contribuisce alla coscienza di un divieto sempre più diffuso dell'utilizzo di tecniche di *web-crawling* per quanto concerne le categorie di dati particolari.

6. Conclusioni

Nonostante l'ulteriore tutela rispetto a quanto previsto dal GDPR, permangono dubbi sull'efficacia della nuova regolamentazione nel limitare il micro-targeting, poiché essa continua a permettere la profilazione politica e il targeting basati sul consenso dei cittadini (sebbene siano escluse categorie particolari di dati personali ai sensi dell'art.9 del GDPR). Spesso gli utenti non sono pienamente consapevoli dei trattamenti a cui acconsentono, né delle conseguenze che ne derivano. L'affidamento esclusivo al consenso rimane una questione che merita attenzione all'interno del dibattito sul quadro normativo europeo sulla protezione dei dati[94]. L'uso mirato dei dati personali per modellare la percezione politica, spesso senza piena consapevolezza degli utenti, può alterare le dinamiche del dibattito democratico, minando il principio di trasparenza. L'adozione del Regolamento europeo 2024/900 segna dunque un passo in avanti importante per la tutela della privacy e dei diritti fondamentali nell'ambito della pubblicità politica online, introducendo norme specifiche per il trattamento dei dati personali a fini di targeting. Tuttavia, la sua portata limitata ai contenuti di pubblicità a pagamento lascia aperta la questione più ampia dell'influenza algoritmica e della diffusione di contenuti manipolatori esenti dalle più tracciabili sponsorizzazioni tramite piattaforma, i quali non sono direttamente regolamentati. Ciò pone dei dubbi anche presso i cittadini più educati ai media che devono essere messi nelle condizioni di decidere se credere o non credere a quanto viene proposto loro dal sistema di raccomandazione dei contenuti. Questo apre interrogativi su come affrontare strategie di persuasione indiretta, che sfruttano dinamiche virali, reti di influencer e pratiche opache per orientare il dibattito pubblico senza essere direttamente soggette alla normativa. Resta dunque la necessità di un ulteriore approfondimento normativo per affrontare le dinamiche più sottili e pervasive della comunicazione politica digitale, garantendo maggiore trasparenza e protezione agli utenti. Questo vuoto normativo è particolarmente rilevante nel contesto delle campagne di guerra ibrida condotte

94. Ruohonen 2023.

da attori esteri, in primo luogo la Russia, che sfruttano disinformazione e manipolazione algoritmica per polarizzare il dibattito politico, minare la fiducia nelle istituzioni e alterare l'esito dei processi elettorali. La capacità di tali strategie di agire al di fuori dei confini della regolamentazione evidenzia la necessità di un approccio più ampio e coordinato a livello europeo, volto a contrastare le minacce ibride alla democrazia e a garantire un'informazione trasparente e pluralista. Per far fronte a tali minacce, alcune nazioni europee hanno istituito delle agenzie nazionali volte alla salvaguardia psicologica dei cittadini, come in Svezia l'Agenzia per la difesa psicologica, attiva dal 2022 e operante sotto il Ministero della Difesa, costituita da un team specializzato nella lotta alla disinformazione e nell'analisi digitale. Anche la Francia ha attivato il Servizio di vigilanza e protezione contro le ingerenze digitali estere (Viginum), istituito nel 2021 sotto il Segretariato generale della difesa e della sicurezza nazionale del Primo Ministro la cui *mission* principale è individuare e analizzare le ingerenze digitali straniere che influenzano il dibattito pubblico online in Francia. Attualmente, in Italia, il DDL 1090 del 2024 per "l'istituzione dell'Agenzia sulla disinformazione e la sicurezza cognitiva" (ADISC) rimane solamente una proposta.

A partire dalla fine del 2025, con l'applicazione del nuovo regolamento, sarà possibile valutarne l'impatto sull'ecosistema digitale. Google ha già annunciato l'eliminazione *in toto* della pubblicità politica, mentre Meta non ha ancora definito una posizione. Se anche altre piattaforme seguissero questa linea, si rischierebbe di ridurre ulteriormente lo spazio per il dibattito politico online, con effetti potenzialmente contrari a quelli auspicati dalla normativa. Se da un lato la regolamentazione limita la pubblicità politica, dall'altro emergono nuove modalità di infiltrazione nel dibattito pubblico, come l'uso di troll, bot e strategie coordinate per influenzare l'opinione pubblica senza ricorrere alla pubblicità tramite adv e sponsorizzazioni. La campagna elettorale è un momento fondamentale per le democrazie, poiché consente di proporre idee e candidati, alimentando il confronto politico. Tuttavia, le nuove restrizioni e i cambiamenti nel panorama digitale pongono interrogativi su quali strumenti rimarranno disponibili per la comunicazione politica e in che misura questi cambiamenti influenzeranno la trasparenza e il pluralismo del dibattito pubblico.

Riferimenti bibliografici

M.R. Allegri (2018), *Diritto all'oblio, tutela della* web reputation *individuale e "eccezione giornalistica". Spunti giurisprudenziali*, in "Forum di Quaderni Costituzionali - Rassegna", 11 giugno 2018

A.C. Amato Mangiameli (2022), *Intelligenza artificiale, big data e nuovi diritti*, in "Rivista italiana di informatica e diritto", 2022, n. 1

F. Banterle (2018), *Pubblicità comportamentale, GDPR e rischi di discriminazione*, in S. Bonavita (ed.), "Società delle tecnologie esponenziali e General Data Protection Regulation", Ledizioni, 2018

A. Barbera (1975), *Art. 2*, in G. Branca (ed.), "Commentario della Costituzione", Zanichelli, 1975

F. Battaglia (2023), *La sentenza Meta platforms. Riflessioni in materia di valore dei dati e libera espressione del consenso*, in "Ordine internazionale e diritti umani – Osservatorio sulla Corte di Giustizia dell'Unione europea", 2023, n. 3

G. Bazzoni (2019), *La libertà di informazione e di espressione del pensiero nell'era della democrazia virtuale e dei* global social media, in "Diritto di Internet", 2019, n. 4

M.R. Bianca (2019), *La* filter bubble *e il problema dell'identità digitale*, in "MediaLaws", 2019, n. 2

N. Bobbio (1990), *L'età dei diritti,* Einaudi, 1990

C. Bologna (2021), *Libertà di espressione e riservatezza «nella rete»? Alcune osservazioni sul mercato delle idee nell'*agorà *digitale*, in "Gruppo di Pisa", Quaderno n° 3, fascicolo speciale monografico abbinato al n. 2/2021

P. Bonini (2020), *L'autoregolamentazione dei principali Social Network. Una prima ricognizione delle regole sui contenuti politici*, in "federalismi.it", 2020, n. 11

R. Borrello (2021), *Le forme di raccordo tra le autorità indipendenti nazionali e la realizzazione di un modello comune europeo di disciplina della comunicazione politica: recenti sviluppi*, in "DPCE Online", vol. 47, 2021, n. 2

F. Bosco, N. Creemers, V. Ferraris et al. (2015), *Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities*, in S. Gutwirth, R. Leenes, P. de Hert (eds.), "Reforming European Data Protection Law", Springer, 2015

G. Caggiano (2021), *La proposta di Digital Service Act per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, in "Annali AISDUE", 2021, n. 1

L. Califano (2022), *Comunicazione politica e social network*, in "Cultura giuridica e diritto vivente", vol. 10, 2022

L. Califano (2021), *Come si governa la tecnologia digitale?*, in "Cultura giuridica e diritto vivente", vol. 8, 2021

E. Calzolaio (2023), *Beni digitali e proprietà tra* civil law *e* common law, in "Rivista critica del diritto privato", 2023, n. 3

S. Calzolaio (2024-a), *Isolamento e relazioni sociali. Il Connection-in-All-Policies approach. Nota a: U.S. Surgeon General, Our epidemic of loneliness and isolation: The U.S. Surgeon General's advisory on the healing effects of social connection and community, 2023*, in "Rivista italiana di informatica e diritto", 2023, n. 2

S. Calzolaio (2024-b), *Vulnerabilità della società digitale e ordinamento costituzionale dei dati*, in "Rivista italiana di informatica e diritto", 2023, n. 2

S. Calzolaio (2018), *Recensione di N. Richards, Intellectual privacy. Rethinking civil liberties in the digital age. New York, NY: Oxford University Press, 2017, pp. 220*, in "Giornale di storia costituzionale", 2018, n. 36

S. Calzolaio (2017), *Protezione dei dati personali*, in R. Bifulco, A. Celotto, M. Olivetti (a cura di), "Digesto delle Discipline Pubblicistiche", Aggiornamento, 2017

P. Caretti, A. Cardone (2019), *Diritto dell'informazione e della comunicazione nell'era della convergenza tecnologica*, il Mulino, 2019

C. Caruso (2023), *Il tempo delle istituzioni di libertà. Piattaforme digitali, disinformazione e discorso pubblico europeo*, in "Quaderni costituzionali", 2023, n. 3

R. Caso (2021), *La società della mercificazione e della sorveglianza: dalla persona ai dati. Casi e problemi di diritto civile*, Ledizioni, 2021

G. Cassano, V. Colarocco, G.B. Gallus, F.P. Micozzi (a cura di) (2018), *Il processo di adeguamento al GDPR*, Giuffrè, 2018

M. Castells (2009), *Comunicazione e potere*, Università Bocconi Editore, 2009

C. Cauffman, C. Goanta (2021), *A new order: The Digital Services Act and consumer protection*, in "European Journal of Risk Regulation", vol. 12, 2021, n. 4

J. Chester, K.C. Montgomery (2019), *The digital commercialisation of US politics – 2020 and beyond*, in "Internet Policy Review", December 2019

Commissione europea (2022), *Codice di buone pratiche sulla disinformazione 2022*

Consiglio Europeo (2024), *L'UE introduce nuove norme in materia di trasparenza e targeting della pubblicità politica*, comunicato stampa, 11 marzo 2024

V. Cuffaro (2019), *Il diritto europeo sul trattamento dei dati e la sua applicazione in Italia: elementi per un bilancio ventennale*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

A.S. D'Amico, D. Pelekis, C. Santos, B. Duivenvoorde (2024), *Meta's pay-or-okay model: An analysis under EU data protection, consumer, and competition law*, Utrecht University School of Law Research Paper 1-2024

A. Di Cerbo (2024), *La tutela dell'identità nell'ambiente digitale alla luce delle norme europee*, in "European Journal of Privacy Law & Technologies", 2022, n. 2

A. Di Cerbo (2022), *L'inquadramento giuridico dei dati personali ceduti per la fruizione dei servizi digitali*, in "European Journal of Privacy Law & Technologies", 2022, n. 2

F. Donati (2021), *Verso una nuova regolazione delle piattaforme digitali*, in "Rivista di regolazione dei mercati", 2021, n. 2

F. Donati (2018), *L'art. 21 della Costituzione settanta anni dopo*, in "MediaLaws", 2018, n. 1

G. Donna (2018), *Modello di business, patrimonio strategico e creazione di valore*, in "Impresa Progetto. Electronic Journal of Management", 2018, n. 2

European Commission (2018), *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 22 August 2018

L. Fabiano (2023), *Le potenzialità manipolative della democrazia digitale fra interessi pubblici e poteri privati*, in "Il Diritto dell'informazione e dell'informatica", 2023, n. 4-5

C. Faralli (2019), *La privacy dalle origini ad oggi. Profili storico-filosofici*, in N. Zorzi Galgano (a cura di), "Persona e mercato dei dati. Riflessioni sul GDPR", Cedam 2019

S. Flaminio (2022), *Lotta alle fake news: Dallo stato dell'arte a una prospettiva di regolamentazione per il "vivere digitale" a margine del Digital Services Act*, in "Rivista italiana di informatica e diritto", 2022, n. 2

V. Frosini (1981), *La protezione della riservatezza nella società informatica*, in N. Matteucci (a cura di), "Privacy e banche dati", il Mulino, 1981

Garante per la protezione dei dati personali (2019), *Provvedimento in materia di propaganda elettorale e comunicazione politica - 18 aprile 2019*

E. Garzonio (2021), *L'algoritmo trasparente: obiettivi ed implicazioni della riforma dello Spazio digitale europeo*, in "Rivista italiana di informatica e diritto", 2021, n. 2

A. Genus, A. Stirling (2018), *Collingridge and the dilemma of control: Towards responsible and accountable innovation*, in "Research Policy", vol. 47, 2018, n. 1

G. Giacomini (2023), *Il GDPR e la regolamentazione della sfera digitale. Orientamenti degli italiani circa la disinformazione su Internet*, in "Comunicazione politica", 2023, n. 3

S. Gobbato (2019), *Big data e "tutele convergenti" tra concorrenza, GDPR e Codice del consumo*, in "MediaLaws", 2019, n. 3

G. Gulotta, M. Caponi Beltramo (2021), *Neurodiritti: tra tutela e responsabilità*, in "Sistema Penale", 1 ottobre 2021

W. Hartzog, N.M. Richards (2022), *The Surprising Virtues of Data Loyalty*, in "Emory Law Journal", vol. 71, 2022, n. 5

D. Kerpen (2011), *Likeable Social Media: How to Delight Your Customers, Create an Irresistible Brand, and Be Generally Amazing on Facebook (And Other Social Networks)*, McGraw-Hill, 2011

D. Imbruglia (2022), *Diritti fondamentali e ambienti digitali: prime note di una ricerca sul diritto a non essere sottoposto a una decisione interamente automatizzata*, in S. Orlando, G. Capaldo (a cura di), "Annuario 2022. Osservatorio Giuridico sulla Innovazione Digitale", Sapienza Università editrice, 2022

N. Irti (2019), *Il tessitore di Goethe (per la decisione robotica)*, in A. Carleo (a cura di), "Decisione robotica", il Mulino, 2019

M. Ladu, N. Maccabiani (2023), *L'autodeterminazione popolare nell'era digitale: tra opportunità normative e tecnologiche*, in "Consulta Online", 2023, n. 2

F. Lagioia, G. Sartor (2020), *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in "federalismi.it", 2020, n. 11

N. Liv, D. Greenbaum (2024), *Integrating Mental Privacy within Data Protection Laws: Addressing the Complexities of Neurotechnology and the Interdependence of Human Rights*, in "AJOB Neuroscience", vol. 15, 2024, n. 2

E. Longo (2021), *Rivoluzione digitale e sviluppi della partecipazione democratica nell'Unione europea*, in "Osservatorio sulle fonti", 2021, n. 3

M. Mancarella (2022), *Social media e comunicazione politica: quali rischi per il sistema democratico?*, in "Rivista elettronica di Diritto, Economia, Management", 2022, n. 3

M. Margolis, G. Moreno-Riaño (2009), *The Prospect of Internet Democracy*, Routledge, 2009

U.A. Mejias, N. Couldry (2019), *Datafication*, in "Internet Policy Review", vol. 8, 2019, n. 4

A. Morace Pinelli (2024), *Introduzione*, in Id. (a cura di), "Dalla *Data Protection* alla *Data Governance*: il regolamento (UE) 2022/868. Commentario al *Data Governance Act*", Pacini Giuridica, 2024

D. Morana (2021), *Partiti e partecipazione politica nell'era digitale: la prospettiva costituzionale*, in "Rivista trimestrale di diritto pubblico", 2021, n. 2

T.T. Nguyen, P.M. Hui, F.M. Harper et al. (2014), *Exploring the filter bubble: The effect of using recommender systems on content diversity*, in "WWW '14: Proceedings of the 23rd International Conference on World Wide Web", Association for Computing Machinery, 2014

C. O'Neill (2017), *Armi di distruzione matematica: come i big data aumentano la disuguaglianza e minacciano la democrazia*, Bompiani, 2017

G. Origgi (2018), *La democrazia può sopravvivere a Facebook? Egualitarismo epistemico, vulnerabilità cognitiva e nuove tecnologie*, in "Ragion pratica", 2018, n. 51

S. Orlando (2022-a), *Data vs capta: intorno alla definizione di dati*, in "Nuovo diritto civile", 2022, n. 4

S. Orlando (2022-b), *Per un sindacato di liceità del consenso privacy*, in "Persona e Mercato", 2022, n. 4

A. Pace, M. Manetti (2006), *Rapporti civili. Art. 21. La libertà di manifestazione del proprio pensiero*, Zanichelli, 2006

E. Pariser (2012), *The Filter Bubble: What the Internet is Hiding from You*, Penguin, 2012

F. Paruzzo (2022), *I sovrani della rete. Piattaforme digitali e limiti costituzionali al potere privato*, Edizioni Scientifiche Italiane, 2022

F. Pizzetti, S. Calzolaio, A. Iannuzzi et al. (2024), *La regolazione europea della società digitale*, Giappichelli, 2024

N.M. Richards (2015), *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*, Oxford University Press, 2015

S. Rodotà (2012), *Il diritto di avere diritti*, Laterza, 2012

J. Ruohonen (2023), *A Note on the Proposed Law for Improving the Transparency of Political Advertising in the European Union*, 2023

D. Sborlini (2022), *Profilazione elettorale e protezione dei dati personali: prospettive di soluzione in ambito europeo*, in "Il Diritto dell'informazione e dell'informatica", 2022, n. 6

O. Spataro (2022), *Diritti di partecipazione politica e piattaforme digitali, alcune riflessioni*, in "Dirittifondamentali.it", 2022, n. 2

E. Spiller (2021), *Il diritto di comprendere, il dovere di spiegare.* Explainability *e intelligenza artificiale costituzionalmente orientata*, in "BioLaw Journal - Rivista di BioDiritto", 2021, n. 2

S. Stalla-Bourdillon, A. Knight (2017), *Anonymous Data v. Personal Data – A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data*, in "Wisconsin International Law Journal", vol. 34, 2017

S. Stalla-Bourdillon, G. Thuermer, J. Walker et al. (2020), *Data protection by design: Building the foundations of trustworthy data sharing*, in "Data & Policy", 2020, n. 2

G. Stegher (2023), *Da cittadini elettori a cittadini consumatori: osservazioni sull'importanza di regolare le campagne elettorali sui social media*, in "Nomos", 2023, n. 1

I. Stepanov (2019), *Introducing a property right over data in the EU: the data producer's right – an evaluation*, in "International Review of Law, Computers & Technology", vol. 34, 2019, n. 1

C.R. Sunstein (2006), *Infotopia: How Many Minds Produce Knowledge*, Oxford University Press, 2006

S. Thobani (2019), *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in "MediaLaws", 2019, n. 3

R. Yuste, S. Goering, B. Agüera y Arcas et al. (2017), *Four ethical priorities for neurotechnologies and AI*, in "Nature", vol. 551, 2017

H. Zech (2016), *Data as a tradeable commodity*, in A. De Franceschi (ed.), "European contract law and the digital single market: Implications of the digital revolution", Intersentia, 2016

G. Ziccardi (2020), L'*uso dei social network in politica tra alterazione degli equilibri democratici, disinformazione, propaganda e dittatura dell'algoritmo: alcune considerazioni informatico-giuridiche*, in "Ragion pratica", 2020, n. 54

S. Zuboff (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Profile Books, 2019

F. Zuiderveen Borgesius, D. Trilling, J. Möller et al. (2016), *Should we worry about filter bubbles?*, in "Internet Policy Review", vol. 5, 2016, n. 1