PAPER N. 21
a.a. 2018/2019

Trento BioLaw Selected Student Papers

Cittadini, utenti o prodotti? Big data ed elezioni libere, dalla bubble democracy a una resilient democracy

WALTER BRUNO

Jean Monnet EUROPEAN CENTRE UNIVERSITY OF TRENTO
Co-funded by the Erasmus+ Programme of the European Union
UNIVERSITÀ DI TRENTO Facoltà di Giurisprudenza

I paper sono stati selezionati a conclusione del corso *BioLaw: Teaching European Law and Life Sciences (BioTell)* a.a. 2018-2019, organizzato all'interno del Modulo Jean Monnet "BioLaw: Teaching European Law and Life Sciences (BioTell)", coordinato presso l'Università di Trento dai docenti Carlo Casonato e Simone Penasa.

Cittadini, utenti o prodotti?

Big Data ed elezioni libere, dalla bubble democracy a una resilient democracy

*Walter Bruno**

ABSTRACT: In recent times the debate arised on consequences of spread of new media on democratic-constitutional systems all over the world, launched by the Cambridge Analytica scandal and boosted by the approval of the GDPR in the framework of the EU. Profiling and microtargeting techniques have considerably changed the information and political communication landscape. By analysing the effects on right to free elections, this work reflects on features of right-duty to information which can be able to challenge the evolutions imposed by new media. The control on data processing too, in a semi-duopoly market, assumes a fundamental relevance in privacy protection and in forming the opinion of the people in the choice of the legislature. Evaluating the current legal context and main proposals, this paper asks for an answer which has to call into question certain paradigms of our law, and which can leverage users' awareness in everyday use of digital platforms.

KEYWORDS: Bubble democracy; big data; profiling; information; AI

«Tutto quello che limita la libertà e la pienezza della comunicazione erige barriere che dividono gli esseri umani in gruppi e categorie, in sette e fazioni contrapposte, e di conseguenza indebolisce la democrazia»
John Dewey[1]

1. Introduzione: la democrazia dei big data: profilazione e social networks

Già da alcuni anni, un popolarissimo servizio di streaming di film e telefilm offre ai propri utenti suggerimenti sui prodotti più vicini ai propri gusti, in base a una serie di preferenze espresse e alla cronologia delle pellicole già viste, anche da altri utenti. In questo modo il fornitore riesce a dare a ciascuno un'indicazione personalizzata, consentendogli di risparmiare molto tempo nella scelta. Quello appena descritto è un chiaro esempio di un meccanismo, la profilazione, ormai già ampiamente diffuso in molti servizi commerciali in rete: dagli acquisti on-line alla comunicazione politica.

Secondo l'art. 4 c. 4 del Regolamento UE 2016/679, noto con l'acronimo inglese GDPR, per profilazione deve intendersi «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per

* *Studente dell'Università di Trento, Facoltà di Giurisprudenza*.

[1] Filosofo statunitense, citato in E. PARISER, *Il filtro*, trad. di B. Tortorella, 2011.

analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica». Tramite gli strumenti offerti dalle compagnie digitali, gli utenti rivelano ai *service provider*, fornitori di servizi, una serie di informazioni personali, sensibili e non, al fine di ricevere un servizio che è, spesso *inconsapevolmente*, personalizzato. La profilazione, d'altra parte, non è nient'altro che una forma particolare di un'attività realizzata da un'intelligenza artificiale, nota col nome di *machine learning* che a partire da un esteso archivio di dati, tramite una loro analisi, giunge a una previsione probabilistica su un fatto non conosciuto o non ancora avvenuto[2]. Queste tecniche permettono dunque, attraverso i dati raccolti, di affinare la loro rielaborazione fino anche a comprendere e apprendere modelli complessi costruiti, in questo caso, su dati personali e relazionali: è il c.d. deep learning. La profilazione si occupa dunque di analizzare il comportamento on line per ricostruire le caratteristiche e i comportamenti probabili degli utenti, o meglio, del singolo utente. Detto in altri termini, l'efficienza del meccanismo «è garantita dall'uso di algoritmi di ricerca e di *selection story* che selezionano quali informazioni, tra quelle contenute in rete, devono raggiungere il lettore»[3]. Ciò che quindi è di necessità primaria per alimentare questo procedimento è un archivio di dati il più vasto possibile da cui attingere: i c.d. *big data*.

Negli ultimi anni la quantità di dati circolanti in rete è aumentata in maniera esponenziale e la tendenza non si arresterà nel breve periodo: nel 2025 si giungerà a 163 ZettaBytes (ossia 163 miliardi di GigaBytes) prodotti ogni anno nel mondo da un numero di dispositivi in continuo aumento. Si passerà ben presto dagli 8.4 miliardi di *device* connessi nel 2017 ai 30 miliardi nel 2020[4]. Preferenze espresse, interazioni, immagini, video, messaggi vocali, testo, posizione GPS, attività motoria: questi ed altri dati contribuiscono a costruire una sorta di "identità digitale" di un cittadino connesso alla rete, cui i *service provider* avranno accesso, profilando un utente in maniera decisamente più dettagliata di oggi.

Allo stato attuale, l'impiego forse più evidente è nella pubblicità, ma lo stesso accade, per ciò che rileva in questa sede, nella gerarchia di presentazione dei contenuti sulle reti sociali e nei risultati dei motori di ricerca, anche questi ormai da tempo personalizzati[5]. In questo modo i risultati rifletteranno la condizione e i gusti del soggetto, da quelli musicali a quelli politici[6]. L'attività di restituire agli utenti ciò che il meccanismo di *machine learning* indica come più (probabilmente) gradito è definito *microtargeting*: una

[2] Una descrizione più estesa della definizione qui data è reperibile in INFORMATION COMMISSIONER'S OFFICE (UK), *Democracy disrupted?*, in https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf (ultima consultazione 31/03/2019).

[3] M. FASAN, *Intelligenza artificiale e pluralismo: uso delle tecniche di profilazione nello spazio pubblico democratico*, in *BioLaw Journal – Rivista di BioDiritto,* 1, 2019, 101-113.

[4] J. BARTLETT, J. SMITH, R. ACTON, *The Future of political campaigning*, DEMOS, July 2018, commissioned by ICO Information Commissioner's Office of the UK, 2.

[5] Una stessa ricerca operata da due utenti diversi sui propri dispositivi, tramite lo stesso servizio di ricerca di Google, offre risultati differenti, non senza influenzare la percezione di chi li visualizza.

[6] C. CASONATO, *Potenzialità e sfide dell'intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto,* 1, 2019, 177-182.

forma di marketing in cui il destinatario di un qualsiasi contenuto è definito individualmente in base al suo profilo.

Quando i prodotti di cui sopra rientrano nel dominio dell'informazione pubblica, in particolare politica, i suddetti meccanismi rischiano di offrire agli utenti contenuti che si rifanno a uno spettro molto ristretto di visioni culturali. Il rischio è quello di un individuo, cittadino-utente, vittima inconsapevole di una «sindrome del mondo amico», secondo una formula coniata da Eli Pariser[7]. Più comunemente, questo "mondo amico" è descritto come una "bolla" o "bolla dei filtri", con una definizione che ha avuto fortuna con l'autore pocanzi citato. Nel "ghetto", è proprio il caso di dirlo, in cui il lettore sarebbe limitato, i riferimenti culturali e politici finirebbero per essere ristretti e fissi, creando un ambiente autoreferenziale. Anche le notizie di cronaca e le conseguenti letture giornalistiche sarebbero speculari a quei riferimenti, impoverendole di una pluralità di punti di vista essenziale per evitare la circolazione delle *fake news* e dei c.d. *deep fake*[8]. Anche la comunicazione politica e l'informazione, soprattutto in periodi di campagna elettorale, sarebbero influenzate dal fenomeno, distorcendo la percezione della realtà. Questo avrebbe come conseguenza di influenzare negativamente il convincimento degli elettori, indebolendo il diritto a libere elezioni.

D'altra parte, la personalizzazione dei contenuti permette di indirizzare a un utente contenuti politici predeterminati, isolandolo non solo rispetto a messaggi politici dissonanti, ma anche rispetto alle parti di un programma politico che esulano dai temi "preferiti", specie se contrastanti con le affinità rivelate dalla profilazione. In questo modo anche un manifesto politico diventa personalizzato, e dai partiti di massa si passa ben presto ai "partiti dei singoli". Una democrazia "a macchie di leopardo"[9], estremamente frammentata, e dunque facilmente soggetta a fenomeni di esclusione e radicalizzazione.

Detto in altri termini, il pericolo di un impiego indiscriminato di queste tecniche rischia di aprire le porte a una vera e propria manipolazione di orwelliana memoria. Non a caso il fenomeno è spesso descritto con l'espressione "*online manipulation*". Molteplici studi hanno già dimostrato come l'utilizzo dei social media influenzano i nostri acquisti, le nostre letture e i nostri desideri, reali e/o percepiti. Allo stesso modo questo accade, o per lo meno rischia di accadere, anche per le intenzioni di voto[10].

---

[7] E. PARISER, *Il filtro*, cit., 120.

[8] Rientrano nella categoria dei contenuti prodotti automaticamente da un sistema di intelligenza artificiale (nel linguaggio comune *autobot*), che sfrutta la combinazione di dati esistenti per generare contenuti realistici. I *deepfake* in particolare costituiscono un «Filmato che presenta immagini corporee e facciali catturate in Internet, rielaborate e adattate a un contesto diverso da quello originario tramite un sofisticato algoritmo.», definizione in Treccani.it, voce "Deepfake", ultima consultazione 03/08/2019.

[9] «[…] a shift in paradigm that could jeopardise democracy itself», in CONSIGLIO D'EUROPA, COMMITTEE OF EXPERTS ON INTERNET INTERMEDIARIES, *Algorithms and Human Rights Study on the human rights dimensions of automated data processing techniques and possible regulatory implications,* DGI(2017)12, 03/2018.

[10] Così è chiaramente descritto in S. ARAL, D. ECKLES, *Protecting elections from social media manipulation,* Science, 30/08/2019, in https://science.sciencemag.org/content/365/6456/858?utm_campaign=toc_sci-mag_2019-08-29&et_rid=335080406&et_cid=2966345 (ultima consultazione 02/09/2019), dove inoltre si propone una ricerca con la stessa metodologia delle indagini impiegate per misurare l'influenza dei social media sui consumi, ritenendo che intervenire sulle scelte di mercato sia più facile che sulle convinzioni politiche. Tuttavia, come gli stessi autori riconoscono, per realizzare un tale tipo di ricerca servirebbe un accesso molto capillare ad alcune categorie di dati, rischiando di entrare in rotta di collisione persino con la segretezza del voto, che rappresenterebbe il risultato della manipolazione da misurare.

Ecco dunque che intorno a questo nucleo centrale rappresentato dal diritto a libere elezioni, fondamentale è analizzare le implicazioni anche sul diritto all'informazione e sulla libertà di espressione da un lato; su gestione dei dati personali dall'altro. Serve concentrarsi sul modo in cui i cittadini utilizzano le risorse in rete e in cui il diritto regola o dovrebbe regolare la raccolta dei dati finalizzata al *microtargeting*, al fine di impedire che i cittadini-utenti non finiscano per diventare essi stessi il *prodotto* di una forma di marketing e di comunicazione di cui dovrebbero essere liberi fruitori.

Nel primo paragrafo le conseguenze sul diritto a elezioni libere verranno affrontate dal punto di vista dell'informazione, quale risultato della libertà di espressione e quale fonte del libero convincimento degli elettori. Nel secondo paragrafo la gestione dei dati da parte dei fornitori dei servizi sarà messa in relazione al potenziale ruolo di altri soggetti, pubblici o indipendenti, quale contrappeso a nuove forme di potere para-pubblicistico. Nel terzo e nel quarto paragrafo si andrà ad analizzare alcune proposte che nel dibattito sul tema sono state avanzate, inserendole nel panorama giuridico attuale, per formulare, nel quinto ed ultimo paragrafo auspici e prospettive per una *resilienza*[11] dello stato di diritto nei confronti della c.d. democrazia delle bolle: la bubble democracy.

2. Diritto-dovere a un'informazione consapevole?

In una consultazione della cittadinanza europea del 2015 ad opera della Commissione Europea è emerso chiaramente che Internet è ormai la prima fonte di informazione nell'Unione, utilizzato a questo scopo dal 72% degli intervistati. La carta stampata e la TV seguono ormai rispettivamente al 63% e al 62%[12]. Questo evidenzia come la formazione dell'opinione pubblica è veicolata sempre più dalla comunicazione in rete. Questo aspetto si somma a quella che da più parti viene considerata una crisi dei media tradizionali, caratterizzata da un calo drastico del giornalismo investigativo e un aumento di uno stile giornalistico povero nella rielaborazione delle notizie, che predilige l'accesso diretto al fatto oggetto di comunicazione al pubblico, spesso privo di una contestualizzazione necessaria a comprendere ciò che accade.[13] Si assiste dunque all'affermazione di un nuovo paradigma tanto per l'informazione quanto per le campagne su internet: l'istituzione di un canale di comunicazione diretto tra forze politiche ed elettori orientato a una forte personalizzazione, impiegando strumenti come il *microtargeting*. La pubblicità politica risulta così «adattata al singolo elettore, secondo contenuti, format e linguaggi»[14]. Certo, questi nuovi metodi di

[11] C. CASONATO, *Diritto e scienze della vita: complessità, tentazioni, resilienza*, in *Diritto Pubblico Comparato ed Europeo*, 2015.
[12] Commissione Europea, *EU Citizenship Consultation 2015, common values, rights and democratic participation*, 2015 in EUROPEAN DATA PROTECTION SUPERVISOR, Opinion 3/2018 on online manipulation and personal data, 19/03/2018.
[13] E. LEHNER, Fake news *e democrazia*, in *MediaLaws*, n.1/2019, pp. 93-122 e R. CAPLAN, D. BOYD, *Who Controls the Public Sphere in an Era of Algorithms?*, in https://datasociety.net/pubs/ap/MediationAutomationPower_2016.pdf (ultima consultazione 25/06/2019).
[14] F.J. ZUIDERVEEN BORGESIUS, J. MÖLLER, S. KRUIKEMEIER, R. Ó FATHAIGH, K. IRION, T. DOBBLER, B. BODO, C. DE VREESE, *Online Political Microtargeting: Promises and Threats for Democracy*, in *Utrecht Law Review*, 14, 1, 2018, 82-96.

comunicazione presentano indubbiamente dei vantaggi: la possibilità di poter coinvolgere più cittadini nella vita politica di una comunità, così come vi è l'opportunità per partiti piccoli o nuovi, privi di mezzi finanziari importanti, di poter raggiungere più facilmente i propri elettori potenziali, a patto che gli strumenti disponibili non siano economicamente proibitivi. Alla stessa maniera risulta più facile far emergere le istanze delle minoranze. Ma d'altra parte, laddove manca una regolamentazione delle campagne politiche ed elettorali on line, è difficile impedire che i soggetti con più risorse godano di un vantaggio, esattamente come accade offline. Evidentemente i rischi maggiori per la vita dei singoli cittadini sono quelli riguardanti la privacy e i propri dati, utilizzabili per una sottile attività di manipolazione[15], sotto una sorta di "microbombardamento mediatico", *ad personam*. In pratica, stiamo parlando di un ostacolo al libero convincimento dell'elettore.

La questione chiave è il modo in cui ai contenuti creati e caricati in rete viene "affidato" un destinatario. Tecnicamente, si tratta di accedere al funzionamento dell'algoritmo che è alla base dei sistemi di *microtargeting*. Come in tutti i meccanismi di *machine learning* e *deep learning*, emerge il problema della c.d. *black box*, ossia dell'impossibilità di accedere alle ragioni che hanno determinato il risultato di un processo ad opera dell'algoritmo, in questo caso la profilazione e l'abbinamento tra utenti e contenuti. A questo si aggiungono le misure applicate dai fornitori di servizi per garantire trasparenza, che si rivelano del tutto insufficienti allo scopo di tutelare i diritti in oggetto. La possibilità di accedere a una serie di informazioni e di impostazioni riguardanti la trasparenza e la privacy, e le impostazioni di default che spesso prevedono un consenso generalizzato al trattamento dei dati si scontrano con l'effettività della tutela di un uso corretto della rete come fonte di informazione e con la sostenibilità del sistema che ne emerge[16]. Ugualmente insufficienti sono le misure adottate in favore della tracciabilità dei contenuti, soprattutto in merito a quelli generati automaticamente, ad esempio per prevenire *fake news* e *deep fake*. La presenza di queste comunicazioni del provider ricorda da vicino i "libri degli ingredienti", di cui la legge prevede l'esposizione negli esercizi commerciali alimentari, che vengono effettivamente consultati solo in circostanze eccezionali. Allo stesso modo, le misure attuali, inducono negli utenti un livello di consapevolezza basso riguardo i meccanismi che permettono loro di crearsi un'opinione sugli avvenimenti del mondo. Questo spinge in ultima analisi a riconsiderare la posizione giuridica dei service provider. A lungo, infatti, la c.d. "*net neutrality*", ossia la neutralità nella gestione di ciò che circola in rete, ha fatto presumere che tutti gli aggregatori di notizie avessero un ruolo imparziale rispetto al pluralismo

[15] *Ivi*, 82-96.

[16] Ad esempio, secondo l'Information Commissioner's Office del Regno Unito, Facebook ha un livello di trasparenza basso che non permette agli utenti di capire come saranno profilati e successivamente raggiunti da una campagna politica. È possibile bloccare determinate pubblicità, ma non è possibile bloccare preventivamente l'insieme delle pubblicità basate su determinati contenuti. *Ammesso che si giunga prima a un livello di consapevolezza tale da rendere desiderabile questa opzione (ndr).* INFORMATION COMMISSIONER'S OFFICE (UK), *Democracy disrupted?*, in https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf (ultima consultazione 31/03/2019).

informativo[17] nei confronti del quale erano i c.d. *content provider*, fornitori di contenuti, i veri responsabili: gli editori dei siti produttori di notizie o gli utenti nei contenuti direttamente pubblicati. Tuttavia, come evidenziato da Roberto Borrello, questo paradigma è da rivedere, laddove l'informazione, per essere «completa, obbiettiva, imparziale ed *equilibrata*»[18] abbisogna principalmente di contraddittorio nella molteplicità delle fonti[19]. Ed ecco dunque che il ruolo di "moderatore" assunto dagli aggregatori digitali diviene tutt'altro che ininfluente.

Offrendo un servizio personalizzato, inoltre, è anche difficile parlare di un'unica opinione pubblica. Laddove i media tradizionali avevano la capacità di dare alle comunità dei punti di riferimento attorno a cui aggregarsi[20], il rischio dei servizi automatizzati è quello di predeterminare i contenuti che saranno visualizzati da ciascuno, con la conseguenza di chiudere l'elettore all'interno di una camera di risonanza delle proprie convinzioni o peggio, realizzare una "democrazia dei singoli", in cui ogni uomo è un'isola, poiché l'inconsapevolezza dei meccanismi spinge ad affidarsi a ciò che ha l'apparenza di essere tecnico, automatico e non arbitrario.

Venendo agli aspetti più strettamente giuridico-costituzionali, il diritto a libere elezioni è affermato in particolare dalla Convenzione Europea per i Diritti dell'Uomo, nell'art. 3 del Protocollo addizionale n.1: «Le Alte Parti contraenti si impegnano a organizzare, a intervalli ragionevoli, *libere* elezioni a scrutinio segreto, *in condizioni tali da assicurare la libera espressione dell'opinione del popolo sulla scelta* del corpo legislativo.»[21] Presupposto delle libere elezioni, secondo la lettera della CEDU, è evidentemente il libero convincimento dei cittadini nella formazione della propria opinione, da esprimersi nelle urne a scrutinio segreto. Il diritto all'informazione emerge come presupposto per il corretto funzionamento di un sistema democratico elettivo. La Corte costituzionale italiana si è pronunciata in alcune sentenze a cavallo del nuovo millennio, in merito al ruolo che in questo panorama è chiamato a giocare il servizio pubblico radiotelevisivo. Secondo Eva Lehner, i suoi obblighi «rispetto "ad una informazione completa, obiettiva, imparziale ed equilibrata"» in merito non implicano, secondo la Corte, «che si possa pretendere da singoli soggetti "una comunicazione imparziale ed esauriente" la quale può derivare solo da una informazione equilibrata che si sviluppi nel contraddittorio tra i diversi soggetti interessati»[22]. Dunque, è il contraddittorio, ossia la pluralità di voci contrapposte a determinare la sostenibilità (e la costituzionalità) di un sistema informativo nel suo complesso. Ora, nella necessità di elaborare un diritto all'informazione che

[17] R. Borrello, *Alcune riflessioni preliminari (e provvisorie) sui rapporti tra motori di ricerca ed il pluralismo informativo*, in *MediaLaws*, 1, 2017, 68-78.
[18] Sentenza C. Cost. 49/1998, corsivo aggiunto.
[19] R. Borrello, *op.cit.*, 68-78.
[20] R. Caplan, D. Boyd, *op.cit.*
[21] Corsivo aggiunto.
[22] E. Lehner, *op.cit., 93-122.* Sentenze citate C. Cost. 49/1998 e 502/2000.

possa efficacemente adattarsi al nuovo contesto mediatico, mi sembra utile muovere dall'art. 21[23] della Costituzione italiana, che pone la libertà di manifestazione del pensiero come un necessario presupposto alla realizzazione del diritto all'informazione.

Una valida proposta in tal senso appare essere quella di Antonio Nicita[24], che prende le mosse da uno specifico testo di *soft law*: la Dichiarazione Universale dei Diritti Umani del 1948. All'art. 19, la libertà di espressione è così definita: «Ogni individuo ha diritto alla libertà di opinione e di espressione incluso il diritto di non essere molestato per la propria opinione e quello di *cercare, ricevere e diffondere informazioni e idee attraverso ogni mezzo* e senza riguardo a frontiere.»[25] Posto che la profilazione e il *microtargeting* non limitano la possibilità di cercare informazioni, considerazioni diverse possono forse svolgersi sugli altri due aspetti: ricevere e diffondere. Le piattaforme in oggetto, infatti, se da un lato permettono all'utente di ricevere dei contenuti, dall'altro gli impongono una limitazione nella scelta degli stessi, predeterminati dall'algoritmo. Allo stesso modo si potrebbe dire che "lanciare" un contenuto su tali piattaforme non equivale a renderlo davvero "*pubblico*", in considerazione del fatto che esso rischia di essere visualizzato solo da uno spettro ristretto di utenti, probabilmente già concordanti con il merito delle informazioni. Intrinseco è dunque l'aspetto relazionale del diritto di espressione: stando a questa visione, esso non è effettivamente tutelato se oltre a manifestare il pensiero non è garantito che esso pervenga al pubblico. «"Manifestare", qui, non significa solo esprimere, ma appunto, "rendere *noto*" al *pubblico.*»[26] in maniera generalizzata e non limitata. Un contributo in questa direzione è dato anche dall'art. 10 CEDU[27]. L'autore suddetto recupera anche una risalente *dissenting opinion* del giudice della Corte Suprema USA Thurgood Marshall in *Keindienst v. Mandel*, 408 U.S. del 1972, secondo la quale «la libertà di parlare e la libertà di ascoltare sono inseparabili, esse sono due facce della stessa medaglia». In ultima analisi, per dirla con le parole di Nicita, «questa natura "reciproca" (o pubblica o politica) della libertà di espressione finisce per esser *diluita*, se non compromessa del tutto, nel duplice combinato disposto della confirmation bias[28] da un lato e della profilazione algoritmica delle piattaforme digitali dall'altro, che assorbe, alimenta e potenzia proprio quella distorsione cognitiva»[29].

In conclusione, serve forse recuperare le caratteristiche del diritto all'informazione per dare loro effettività e tutela da questa distorsione cognitiva: un'informazione che oltre che «completa, plurale, obiettiva,

[23] Art. 21 c.1-2: «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».
[24] A. NICITA, *Libertà d'espressione e pluralismo 2.0: i nuovi dilemmi*, in *MediaLaws*, 1, 2019, 314-319.
[25] Corsivo aggiunto.
[26] A. NICITA, *op.cit.*, 316. Corsivo aggiunto.
[27] Art.10 (c.1, primi due periodi): «Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di *ricevere o di comunicare informazioni o idee* senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera». Corsivo aggiunto.
[28] Fenomeno per cui gli algoritmi, lungi da essere neutrali, confermano e amplificano i pregiudizi presenti già nei dati pregressi e nella loro impostazione. Cfr. §3, a proposito della *net neutrality*.
[29] A. NICITA, *op. cit.*, 316. Corsivo aggiunto.

imparziale ed equilibrata», recuperi anche il suo aspetto comunicativo e relazionale all'interno della comunità, diventando in fondo anche un'informazione *consapevole* da parte del cittadino. Laddove i contenuti visualizzati permettono ai singoli di accedere a punti di vista maggiormente divergenti rispetto al proprio *background*, è anche più facile raggiungere maggiore consapevolezza sulla molteplicità delle posizioni e delle proposte politiche, che altrimenti rischiano di restare in un angolo cieco, escluse dall'algoritmo di *microtargeting* e dunque fuori da un metaforico "campo visivo". Di conseguenza ciò ridurrebbe il rischio di chiudersi nella propria "bolla" e di innescare meccanismi di auto-esclusione e radicalizzazione. Questo si traduce in uno spazio da regolamentare da molteplici punti di vista, esattamente come prima di esso lo è stato il sistema mediatico tradizionale: per trasparenza, tracciabilità, riservatezza ma anche concentrazione.

3. Big data: forza monopolistica privata o nuova forma di potere?

Nel mondo dell'intelligenza artificiale, in questa promessa "quarta rivoluzione industriale", di cui profilazione e *microtargeting* rappresentano solo alcune applicazioni, i dati assumono un'importanza prevalente, cui va certamente l'attribuzione di "bene", dal punto di vista giuridico, ma soprattutto economico. Le informazioni sono un bene con una caratteristica particolare: esse possono essere duplicate e diffuse senza limiti. All'opposto, cancellarne le tracce diventa un meccanismo a volte difficile e ben poco trasparente, senza considerare la pirateria informatica. A ragione possiamo ritenere che sono stati definiti la "valuta del XXI secolo". Già ad oggi, le società più redditizie che operano nel panorama digitale non sono più valutate soltanto in base al loro fatturato, ma anche in base alle quantità di dati che ricevono e sono in grado di veicolare[30]. I "giganti di internet" iniziano dunque ad essere *gestori* di un potere economico basato su informazioni anche personali, con le quali si è visto che può essere influenzata l'opinione pubblica[31]. Come già nella fornitura di servizi nell'informazione pubblica, così nel trattamento dei dati personali degli utenti, i service provider si trovano nella posizione di poter condurre alcuni poteri para-pubblicistici che esulano dagli schemi tradizionali del costituzionalismo. Queste nuove forme di potere iniziano ad avere un peso negli equilibri di *check and balance* delle costituzioni occidentali.

Questo potere si è concentrato nelle mani di pochi, pochissimi, soggetti. Anzi, è ormai pacifico definire questa concentrazione nelle forme di un quasi-duopolio, dominato dai due giganti privati Google e Facebook. Le convention periodicamente organizzate per il loro sviluppo, gli incontri sempre più frequenti con autorità nazionali e internazionali, li collocano su un piano che rasenta la parità con queste ultime, in trattative su politiche pubbliche e tassazione. Le audizioni di Mark Zuckerberg al Congresso americano e al

[30] Y.N. HARARI, *21 lezioni per il XXI secolo*, 2018.

[31] Lo scandalo Cambridge Analytica in occasione del referendum britannico sulla partecipazione all'U.E. ne è una chiara dimostrazione.

Parlamento Europeo in seguito allo scandalo *Cambridge Analytica* rappresentano un esempio della forza "contrattuale" guadagnata dai colossi della rete. Anche l'assenza di una serrata concorrenza certo favorisce un comportamento più blando da parte di questi operatori, che offrono servizi al momento unici o percepiti da gran parte del mercato come tali[32]. In questo modo, il bilanciamento tra beni e diritti che si incrociano nell'utilizzo delle piattaforme è interamente nelle mani di un privato (ad esempio tra libertà di espressione da un lato e discriminazione, offensività o diritto all'oblio dall'altro, o ancora, in merito alle misure *anti-fake news*) con ben poche vie di fuga. Anche in merito alla riservatezza dei dati raccolti, sebbene ogni trattamento si basi su un consenso dato dall'utente, molto si potrebbe dire sulle misure attuate dalle piattaforme per rendere consapevole tale consenso, e sulle reali possibilità di poter usufruire della piattaforma anche limitando il consenso. La dimensione globale di tali organizzazioni rende spesso difficile la loro regolazione a livello statale, potendo influire più efficacemente soltanto a livello sovranazionale. Un esempio è il recentissimo e ancora vivo dibattito internazionale sulla c.d. web tax, giunta sul tavolo non solo dell'Unione Europea, ma anche del G20 del giugno 2019. Proprio il caso *Cambridge Analytica*, già più volte richiamato, testimonia che i rischi per la democrazia nascosti nei servizi delle piattaforme digitali vanno ben al di là di ogni confine nazionale. Per questo è fondamentale che le istituzioni internazionali abbiano un ruolo primario nell'elaborazione delle proposte che dovranno tutelare i sistemi costituzionali e sub-costituzionali dai potenziali rischi analizzati. Per quanto ci riguarda, servirà anche che gli organismi deputati alla giurisdizione dei diritti si armino di strumenti interpretativi idonei a far fronte a queste nuove forme di potere. Su questo tanto la Corte di Giustizia dell'UE quanto la Corte EDU ci danno segnali incoraggianti, come si vedrà nel paragrafo successivo.

Ma ancora più importanti del livello istituzionale sono le caratteristiche che devono avere gli organismi che dovranno occuparsi del controllo sulla gestione dei dati, sia personali che aggregati. È chiaro che la proprietà dei dati in capo agli utenti non è sufficiente a garantirne un'efficace tutela, a partire dal momento in cui il consenso viene concesso al fornitore di servizi. Utili sono le riflessioni di Yuval Noah Harari e di Eli Pariser[33] sul ruolo degli enti pubblici e privati. Se da un lato, infatti, una gestione interamente privata corre il rischio di soccombere di fronte agli scopi economico-finanziari delle società, dall'altro anche un eccessivo controllo da parte degli apparati pubblici non sarebbe una forma di tutela molto lungimirante nei confronti di potenziali tendenze autoritarie. Ecco che allora una soluzione migliore potrebbe essere quella intermedia: ossia una forma di controllo che insista su sostanziali misure di trasparenza, per un'accessibilità non solo potenziale ma effettiva. Una forma di controllo che non può che essere partecipativa.

[32] Anche C. Cadwallard in un articolo sul Guardian mette in luce come un'assenza di concorrenza e la concentrazione massima di utenti su poche piattaforme favorisce anche l'operato di chi vuole influire sui risultati elettorali. In C. CADWALLARD, *Google, Democracy and the truth about internet search,* The Guardian, 04/12/2016, https://www.theguardian.com/technology/2016/dec/04/google-democracy-truth-internet-search-facebook (ultima consultazione 01/09/2019).

[33] Y.N. HARARI, *op.cit.*, p. 129 e E. PARISER, *op. cit.*, 114.

Inoltre, non è da sottovalutare nemmeno il ruolo che può essere ricoperto dalle agenzie e dalle autorità indipendenti, come in Italia l'AGCOM, Autorità per le Garanzie nelle Comunicazioni, che ha già poteri di controllo su alcune posizioni di mercato, sulla tutela dei principi costituzionali espressi nell'art. 21, nonché sulla riservatezza delle comunicazioni, in un'epoca in cui esse avvengono quasi esclusivamente attraverso internet. Un ulteriore esempio è l'EDPS, Garante Europeo della Protezione dei Dati (*European Data Protection Supervisor*), ad oggi responsabile di monitorare il trattamento dei dati all'interno delle istituzioni UE, ma che si occupa anche delle evoluzioni delle stesse questioni nel settore dei privati, tramite pareri, in collaborazione con il nuovo Comitato Europeo per la Protezione dei Dati, nato con il GDPR, di cui fa parte pure il Garante italiano della Protezione dei Dati Personali. Non a caso, anche il Parlamento Europeo, in una sua Risoluzione[34] del 2017 ha proposto alla Commissione l'istituzione di una nuova Agenzia Europea per la Robotica e l'Intelligenza Artificiale. Evidentemente, dunque, le misure che saranno elaborate e proposte dovranno coinvolgere un panorama variegato di attori, puntando anche a una collaborazione tra soggetti pubblici e privati.

4. Il contesto giuridico e il "nuovo corso" nella giurisprudenza in Europa

L'evoluzione dell'intelligenza artificiale, nei vari campi di applicazione che comportano conseguenze sui meccanismi di funzionamento del diritto e delle democrazie, potrebbe presto avvicinare il rischio di una nuova forma di "funzionalismo", una sorta di governo tecnico-amministrativo, in cui l'analisi dei dati predetermina gran parte del dibattito pubblico e delle decisioni politico-legislative[35]. Il diritto, nelle sue varie specializzazioni, è chiamato dunque a prevenire questi rischi, permettendo all'intelligenza artificiale di dare un contributo positivo alle nostre società.

Ma qual è il contesto normativo attuale? Della normativa europea di riferimento in merito a libere elezioni (Prot. 1, art. 3 CEDU[36]), informazione e libertà di espressione (Art. 10 CEDU[37]) i primi riferimenti sono già stati illustrati nei paragrafi precedenti, tuttavia il quadro va completato. Com'è noto, nessuna riflessione riguardo le norme della Convenzione Europea dei Diritti dell'Uomo può dirsi esaustiva senza prendere in considerazione il formante giurisprudenziale. Così, la Corte di Strasburgo mette in guardia sul fatto che gli articoli menzionati possono confliggere tra di loro, specie in prossimità delle elezioni. Infatti, se da un lato, «la pubblicazione di informazioni mirate a influenzare gli elettori rappresenta un esercizio della libertà di

[34] PARLAMENTO EUROPEO, *Risoluzione del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)).*

[35] R. CALO, *Artificial Intelligence Policy: A Primer and Roadmap,* in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015350. Riflessione simile anche in Y.N. HARARI, *op. cit.*, 114.

[36] CEDU, Prot. 1 art. 3: «Le Alte Parti contraenti si impegnano a organizzare, a intervalli ragionevoli, libere elezioni a scrutinio segreto, in condizioni tali da assicurare la libera espressione dell'opinione del popolo sulla scelta del corpo legislativo».

[37] V. nota n. 23.

espressione»[38], e ogni restrizione va «strettamente interpretata»[39], d'altra parte tali restrizioni potrebbero divenire necessarie per «assicurare la libera espressione dell'opinione del popolo nella scelta del corpo legislativo»[40]. Come la Corte ha poi ulteriormente affermato[41], «un controllo legislativo del dibattito pubblico è necessario per proteggere il processo elettorale». Infine, in merito alle *fake news*[42], la Corte ha deciso che le piattaforme in rete non hanno nessun obbligo di sorveglianza sui contenuti degli utenti che non sono sottoposti ad alcuna preventiva moderazione. Diverso è invece stato l'atteggiamento nei confronti dei contenuti e persino dei commenti ritenuti diffamatori. Nel caso *Delfi AS c. Estonia*[43] la Corte ha infatti ritenuto di confermare la sanzione a carico di un service provider per i commenti diffamatori pubblicati anonimamente da un utente, di cui il provider stesso era stato reso edotto. Un approccio molto simile a quello della Direttiva UE c.d. "E-commerce", che esclude l'estraneità del service provider solo nel momento in cui lo stesso venga effettivamente a conoscenza delle attività potenzialmente illecite (in questo caso diffamatorie) svolte sulla piattaforma. In conclusione, va detto che fino a un recente passato negli orientamenti generali di entrambe le Corti europee si registrava un atteggiamento più morbido nei confronti degli Internet Service Provider, a maggior tutela dei fornitori di servizi che operano in maniera passiva e automatica, della libertà di iniziativa economica e in ultima analisi in ragione della ritenuta difficoltà di controllo dei contenuti in forme diverse da quelle della segnalazione. Di recente va invece messo in luce quello che potremmo definire un "nuovo corso", evidente soprattutto nella giurisprudenza eurounitaria, più attento ai diritti degli utenti e meno prudente nei confronti degli operatori della rete. D'altra parte, infatti, non mancano indicazioni verso un'estensione della responsabilità dei prestatori di servizio laddove essi operino o siano in grado di operare facilmente un controllo sui contenuti, sia che ciò accada nel caso specifico emergente di volta in volta grazie a segnalazioni, sia in maniera più generalizzata, similmente agli editori[44].

Anche nella tutela da parte dell'Unione europea, la Carta dei Diritti Fondamentali dell'U.E. si occupa a sua volta di informazione e di media, tutelando all'art. 11, non solo la libertà, ma anche il loro *pluralismo*.

Sul lato invece della profilazione e il trattamento dei dati personali, la produzione giuridica è ben più florida. La stessa CEDU tutela all'art. 8 il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza, tutelando i cittadini dalle limitazioni ad esso poste dalle autorità pubbliche. La stessa

[38] CEDU (Grande Camera), *Bowman c. Regno Unito*, 2000, 24839/94 in Information Commissioner's Office (UK), *op. cit.*
[39] CEDU (Sezione), *Andrushko c. Russia*, 2010, 4260/04 in Information Commissioner's Office (UK), *op. cit.*
[40] V. nota n. 35.
[41] CEDU (Grande Camera), *Animal Defenders International c. Regno Unito*, 2013, 48876/08 in Information Commissioner's Office (UK), *op. cit.*
[42] CEDU (Sezione), *Magyar Tartalomszolgáltatók Egueslete and Index.hu Zrt c. Ungheria*, 2016, 22947/13, in G. De Gregorio, The market place of ideas *nell'era della post-verità: quali responsabilità per gli attori pubblici e privati* online*?*, in *MediaLaws*, 1, 2017, 91-105.
[43] CEDU (Grande Camera), *Delfi AS c. Romania*, 2015, 64569/09 in G. De Gregorio, *op. cit.*, 91-105.
[44] M. Bassini, *La rilettura giurisprudenziale della disciplina sulla responsabilità degli Internet service provider. Verso un modello di responsabilità "complessa"?*, in *Federalismi.it*, https://bit.ly/2lxVihi (ultima consultazione 02/09/2019).

protezione è richiamata dall'art. 7 della Carta dei Diritti Fondamentali UE, cui va aggiunto il suo art. 8 che tutela la protezione dei dati personali[45]. In merito ai rapporti tra CEDU e protezione dei dati, la Corte ha avuto modo di intervenire solo marginalmente[46]. Ma rimanendo nell'ambito del Consiglio d'Europa, una Convenzione importante a riguardo è la n. 108[47], riguardo la protezione e il trattamento automatizzato dei dati, aperta ad adesione nel 1981 ed entrata in vigore nel 1985. Si tratta dunque di uno dei testi più risalenti a riguardo, rivisto tuttavia nel 1999 e nel 2018 per raccordarlo al GDPR. Ciò che qui è importante rilevare di questo trattato è l'attenzione che viene posta a speciali categorie di dati: all'art. 6, infatti, si afferma che «i dati a carattere personale che rivelano l'origine razziale, le opinioni politiche, le convinzioni religiose o altre convinzioni, nonché i dati a carattere personale relativi alla salute o alla vita sessuale, non possono essere elaborati automaticamente a meno che il diritto interno preveda delle garanzie appropriate. Lo stesso vale per i dati a carattere personale relativi a condanne penali», abbinandoci diritti riguardo la conoscenza e la correzione dei dati detenuti, e infine protezione dalla pirateria. Questa norma, al quale pure l'Unione Europea ha aderito, va oggi correlata per lo meno all'art. 22 del GDPR, che pone una regola generale e tre eccezioni: «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. Il Paragrafo 1 non si applica nel caso in cui la decisione: 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.» E sebbene l'art. 9 par. 1 vieti il trattamento di dati sensibili, allo stesso modo il par. 2 lett. a lo autorizza dietro esplicito e specifico consenso. Ora, è evidente che specialmente le lett. a) e c) dell'art. 22 abbiano l'effetto di indebolire sensibilmente l'efficacia delle disposizioni di cui al par. 1[48]. Per le considerazioni già fatte sulla natura del consenso e il modo in cui viene prestato, siamo davanti a una tutela ridotta a poco più di una formalità, specie quando esso è necessario per usufruire della piattaforma. Sempre in collegamento con la disposizione della Convenzione n. 108, gli artt. 5 e 6 del GDPR pongono in capo al responsabile del

[45] Art. 8: «1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

[46] Riguardo i database creati dalle autorità, spesso dichiarandone l'illegittimità oltre ciò che è strettamente necessario alle funzioni pubbliche. In (Grande Camera) *Amann v. Switzerland*, 2000, 27798/95 e (Grande Camera) *Rotaru v. Romania* 2000, 28341/95, citate in V. FERRARIS, F. BOSCO, E. D'ANGELO, *The impact of profiling on fundamental rights*, in http://www.unicri.it/special_topics/citizen_profiling/PROFILINGproject_WS1_Fundamental_1110.pdf (ultima consultazione 31/03/2019).

[47] Consiglio d'Europa, *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*, n. 108, 28/01/1981.

[48] C. CASONATO, *op. cit*, 7.

trattamento degli obblighi molto simili a quelli previsti dal testo internazionale sui tempi nei quali i dati vanno trattati (ossia nei limiti del necessario), sulla rettificabilità delle informazioni raccolte, l'obbligo di garantire adeguate misure di sicurezza da trattamenti non autorizzati, distruzione e danni accidentali. L'art. 6 poi, impone al responsabile di individuare una base giuridica adeguata al trattamento dei dati. Infine, per chiudere con una nota positiva, una menzione merita l'art. 80 che permette che il singolo sia affiancato e supportato da «un organismo, un'organizzazione o un'associazione senza scopo di lucro» debitamente costituiti, fino alla possibilità di dar loro mandato di esperire i mezzi approntati dal Regolamento. È da ritenersi una misura di grande importanza per la giustizia in concreto, trattandosi di casi in cui le violazioni da parte di grandi piattaforme spesso colpiscono un numero notevolmente esteso di utenti (si pensi che nel solo caso *Cambridge Analytica* sono stati coinvolti ben 87 milioni di utenti *Facebook*[49]) ed è difficile per gli stessi avere contezza tanto della violazione, quanto delle sue dimensioni generalizzate. Dunque, la presenza di organismi "collettivi" potrebbe ricoprire un importante ruolo di osservazione e sostegno agli utenti nella loro quotidianità "digitale".

Restando in materia di diritto dell'Unione Europea, però, un tassello davvero fondamentale è rappresentato da una teoria interpretativa dei diritti fondamentali nata in Germania, e che alla luce delle considerazioni fatte nel paragrafo 2 rivela il suo valore aggiunto nell'applicazione di molte tutele costituzionali. Si tratta della teoria dell'effetto orizzontale dei diritti, detta anche *drittwirkung*. Come messo in luce da Oreste Pollicino[50], in base a questa teoria, il rispetto dei diritti fondamentali non è solo richiesto da parte della pubblica autorità a protezione dei singoli, ma anche *tra* privati, come mezzo per rendere davvero effettiva tale tutela, soprattutto nel contesto degli ordinamenti liberal-democratici. Applicazione paradigmatica di questa teoria da parte della Corte di Giustizia dell'UE si ha nel caso Defrenne II[51], per garantire il principio della parità retributiva tra uomo e donna anche nella condotta di un privato. D'altra parte, lo stesso principio, in nuce, era già stato affermato dalla Corte UE a fini molto più ampi in *Van Gend & Loos*, con ricadute sull'intera architettura giuridica delle Comunità Europee.

Tornando alla protezione dei dati, possiamo constatare un'applicazione del principio in parola nel caso *Google Spain*[52], nel quale i Giudici di Lussemburgo hanno imposto al motore di ricerca di rimuovere, su espressa richiesta dell'interessato, link relativi a pagine contenenti dati lesivi del diritto all'oblio. Anche qui, infatti, è data efficacia diretta all'art. 8 della Carta dei Diritti e delle Libertà Fondamentali dell'Unione Europea, che mira a proteggere i dati di carattere personale. Questo principio può dunque rivelarsi una

[49] C. KANG, A. FRENKEL, *Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users*, New York Times, 04/04/2018 in https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html (ultima consultazione 02/09/2019).
[50] O. POLLICINO, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta La giurisprudenza della Corte di giustizia in materia di* digital privacy *come osservatorio privilegiato*, in *MediaLaws*, 3, 2018, 138-163.
[51] CGUE, *G. Defrenne c. Société anonyme belge de navigation aérienne Sabena* ("Defrenne II"), 1976, C-43/75.
[52] CGUE (Grande Camera), *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, 2014, C-131/12.

chiave fondamentale per ricondurre anche nuove forme di potere al necessario rispetto dello stato di diritto. Le più recenti pronunce della Corte di Giustizia, a partire da *Google Spain*, possono sempre più rientrare, a pieno titolo in quello che è stato definito poco sopra come "nuovo corso" nelle questioni riguardanti il trattamento dei dati sulla rete, che vede l'individuo-utente al centro di una protezione sempre più esigente nei confronti dei prestatori di servizi.

Il 1° ottobre 2019 la Corte del Lussemburgo ha infatti emesso quella che appare subito come un'importante pronuncia riguardante i c.d. *cookies*[53]. Interpretando alcune direttive in materia[54], i giudici hanno stabilito che per acconsentire alla loro installazione e al loro funzionamento non può più essere ritenuto compatibile con il diritto UE il consenso dato tramite una casella precompilata sulle classiche finestre automatiche che compaiono all'apertura di un sito, ma il consenso è definito non solo «*specifico*» ma persino «*attivo*», con un'affermazione che potrebbe segnare un notevole passo avanti nelle riflessioni riguardanti, appunto, il ruolo futuro del consenso e la consapevolezza di quest'ultimo da parte degli utenti. Ai navigatori quindi, dovrebbe essere richiesto di validare una casella prima di inviare il consenso all'archiviazione e al trattamento di informazioni sulla propria attività sul sito a fini profilativi e/o pubblicitari[55].

La seconda pronuncia che si richiama qui all'attenzione segue di sole quarantotto ore la precedente, e riguarda in particolare i commenti illeciti sui social network, nella fattispecie, Facebook. Qui la Corte ha stabilito che «il diritto UE non osta a che venga ingiunto a un prestatore di servizi, di rimuovere commenti identici, e a certe condizioni» persino «equivalenti a quelli precedentemente dichiarati illeciti.»[56] Anche in questo caso si tratta, ad avviso di chi scrive, di un notevole passo in avanti[57], in quanto tali operatori vedranno accrescere la propria responsabilità non solo in casi in cui il singolo contenuto viene segnalato, ma anche per quei contenuti identici o equivalenti. Il che implica, si direbbe per forza di cose, che il prestatore dovrà impiegare strumenti di intelligenza artificiale in grado di rilevare le "copie" del contenuto illecito e ogni altro che sia «equivalente a quello di un'informazione precedentemente dichiarata illecita o di bloccare l'accesso alle medesime, purché la sorveglianza e la ricerca delle informazioni oggetto di tale ingiunzione siano limitate a informazioni che veicolano un messaggio *il cui contenuto rimane*

[53] I cookies sono «file che il fornitore di un sito Internet installa nel computer dell'utente di tale sito e ai quali il fornitore può nuovamente accedere durante una nuova visita del sito da parte dell'utente, per facilitare la navigazione in Internet o transazioni oppure al fine di ottenere informazioni sul comportamento dell'utente.» in Corte di Giustizia dell'Unione Europea, *Comunicato Stampa n.125/19*.

[54] Nello specifico: Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche; Direttiva 95/46/CE del Parlamento europeo e del Consiglio, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati; Regolamento UE 2016/679 del Parlamento europeo e del Consiglio (c.d. GDPR).

[55] CGUE, *Bundesverband der Verbraucherzentralen und Verbraucherverbände c. Planet49 GmbH,* 2019, C-673/17.

[56] Corte di Giustizia dell'Unione Europea, *Comunicato Stampa n.128/19.*

[57] Va tuttavia considerata anche una riserva da porre a questo giudizio positivo, riguardanti i pericoli di una (seppure in questo caso lieve) discrezione collocati nelle mani dei service provider privati, come è stato messo in luce nel §2 e come si dirà a proposito delle misure *anti fake-news*.

sostanzialmente invariato rispetto a quello che ha dato luogo alla dichiarazione d'illeceità e che *contengono gli elementi specificati nell'ingiunzione* e *purché le differenze* nella formulazione di tale contenuto equivalente rispetto a quella che caratterizza l'informazione precedentemente dichiarata illecita *non siano tali da costringere il prestatore di servizi di hosting ad effettuare una valutazione autonoma di tale contenuto*»[58]. Infine, un elemento "rassicurante" non trascurabile è che requisito per tale eventualità, e dunque responsabilità, è un accertamento giudiziale sull'illiceità del contenuto sotteso a un'ingiunzione.

5. Nuove prospettive e alcune proposte

Sulla scia di questo nuovo corso giurisprudenziale, è ora il momento di analizzare alcuni dei numerosi provvedimenti che, nel vasto dibattito *de jure condendo* suscitato su varie categorie scientifiche, sono stati promossi, sia di ampio respiro, sia di massima specificità su alcuni aspetti particolari.

Per quanto riguarda la disciplina delle campagne politiche, innanzitutto risulta opportuno integrare quelle norme già esistenti sulle campagne elettorali, che mal si adattano a condotte poste in essere ormai indipendentemente dalle elezioni. Si tratta piuttosto di ipotizzare un modo per esportare il principio della *par condicio* in situazioni parallele, non tanto nell'offerta di contenuti politici in rete da parte dei *content provider*, quanto nella loro aggregazione sulle piattaforme. Per far questo bisognerebbe anche approntare meccanismi idonei a identificare i contenuti pubblicati, quando questi fanno parte di una campagna, senza d'altra parte né limitare la libertà di stampa (e di espressione più in generale), né comprimere la libertà di poter scegliere i contenuti da leggere[59]. Anche nell'obbligo di pubblicazione della spesa online di ogni soggetto politico, al fine di poter eventualmente porre un tetto massimo, vi sono limiti riguardanti le campagne di terze parti[60], difficilmente inquadrabili, e ostacolanti la trasparenza e la tracciabilità.

Passando al funzionamento dei social networks, anche qui le proposte sono varie. L'ICO[61] britannico promuove il ruolo delle autorità indipendenti, tramite dei codici di buone pratiche, che possano intercettare la collaborazione dei providers, specialmente in merito alla tutela dei dati. Sempre in merito a questi ultimi, si potrebbe pensare di intervenire anche sulle impostazioni di default delle piattaforme, stabilendo le opzioni di base in maniera tale che siano più limitative rispetto ai consensi generalizzati di solito richiesti al momento dell'iscrizione, e che consentano di utilizzare determinati servizi in seguito, conoscendo meglio i necessari permessi correlati. Una variante prevede anche la possibilità per l'utente di modulare le preferenze sui contenuti visualizzati lungo una linea continua che va da "100% personalizzato", in base alla profilazione, a un 0% in cui i contenuti vengono mostrati in base a criteri standardizzati[62], che

[58] CGUE, *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, 2019, C-18/18.
[59] Riflessione in parte simile in European Data Protection Supervisor, Opinion 3/2018 on online manipulation and personal data, 19/03/2018.
[60] Information Commissioner's Office (UK), *op. cit.*
[61] Information Commissioner's Office (UK), *op.cit.*
[62] E. PARISER, *op.cit.*, p. 188.

permetterebbe di raggiungere contenuti fuori dalla bolla.[63] D'altra parte, si potrebbe pensare a un ruolo attivo della stessa intelligenza artificiale che già muove gli algoritmi, per esempio vietando di processare informazioni sensibili. Certo, in questo caso si rischiano possibili margini di errore, specie laddove l'IA non ha ancora raggiunto elevati livelli di precisione, e un affiancamento umano sarebbe opportuno, in un'ottica che lo stesso GDPR promuove. Ma il rilievo più importante in merito è forse un altro. I dati in qualche modo "*generici*" sono davvero scindibili dai dati *sensibili*? Ammesso anche il divieto di utilizzo da parte di un algoritmo di alcune categorie di dati, il suo giudizio probabilistico potrebbe portare a identificare certe preferenze personali pur non utilizzando dati che esplicitamente richiamano tali preferenze. Ad esempio, un algoritmo potrebbe giungere a una previsione sull'orientamento sessuale di un soggetto in base alla musica che ascolta, o le preferenze politiche in base ai film visualizzati in streaming, e questo a prescindere dalle interazioni sociali. La domanda da porsi è allora se rendere tabù alcuni dati agli occhi dell'intelligenza artificiale possa essere sufficiente a salvaguardare l'utente da una profilazione ugualmente "intima".

In uno sguardo più generale sul web, la stessa IA potrebbe avere un ruolo attivo nell'identificazione di contenuti prodotti automaticamente da un "collega" algoritmo (c.d. "*autobot*"). In vista delle elezioni, invece, sarebbe utile puntare alla diffusione di siti di informazione e orientamento al voto che siano plurali e presentino i programmi elettorali nel loro complesso, consentendo confronti e richiami tra temi diversi. In questo certamente le istituzioni pubbliche e le autorità indipendenti possono avere un ruolo determinante.

Infine, un capitolo a parte rappresentano le misure *antibufale*. Negli ultimi anni vi è stata nel mondo una proliferazione di misure legislative o paralegislative di contrasto alle *fake news*. Una per tutte, in Italia, il disegno di legge n. 2688/2017 di introduzione dell'art. 656-bis c.p., che prevede un'ammenda fino a €5000 per «chiunque pubblichi o diffonda notizie false, esagerate o tendenziose che riguardino dati o fatti manifestamente infondati o non veritieri, attraverso social media o altri siti che non siano espressione di giornalismo online», aggiungendo anche la responsabilità delle piattaforme in caso di ritardo nell'eliminazione dei contenuti. Tuttavia, questa ed altre proposte simili, oltre ad essere contrarie alla direttiva UE 2000/31/CE che vieta una forma di responsabilità automatica dei provider per i contenuti pubblicati dagli utenti, come spiega Filippo Donati[64], c'è il rischio che si trasformino in forme di censura *in concreto*. Allo stato attuale, la veridicità di una notizia non è condizione di per sé necessaria alla circolazione di un contenuto, non esistendo un giudizio dirimente che possa stabilire ontologicamente "cosa è falso", oltre al rischio di limitare "al contrario" il pluralismo, censurando «notizie e idee critiche nei confronti dei detentori di potere politico o economico, in contrasto con i principi desumibili dalla nostra

[63] Un'opzione simile è disponibile su Twitter, dove esistono due possibili visualizzazioni della home page: si può scegliere se visualizzare i tweet "più recenti" oppure quelli "più rilevanti", formula, quest'ultima, che evidentemente risente di un criterio di personalizzazione.

[64] F. DONATI, Fake news *e libertà di informazione*, in *MediaLaws*, 2, 2018, 440-446.

Costituzione»[65]. A conferma di ciò, in un rapporto del 2018[66] l'Unesco ha indicato le misure *anti-fake news* come uno dei più gravi pericoli per la libertà di stampa nel mondo negli ultimi anni. Evidentemente, molta strada ancora c'è da fare per trovare una soluzione ordinamentale a un problema che va affrontato. Una soluzione provvisoria, tuttavia, è indicata da Giovanni De Gregorio[67], in una possibile collaborazione tra le piattaforme e autorità pubbliche o indipendenti per poter indicare contenuti e notizie "non attendibili" come "*Disputed*", un compromesso tra libertà di espressione e diritto a un'informazione completa, oggettiva e, de iure condendo, consapevole.

6. Dalla "bubble democracy" alla "resilient democracy"

Cercando di individuare alcune linee direttrici verso le quali il dibattito si evolve e presentando anche alcuni auspici e proposte, è utile prendere brevemente le mosse da tre testi che pur non richiamandosi a vicenda si intrecciano nella visione che offrono per le future politiche sui media e sui dati. Si tratta, in ordine cronologico, di un Parere del novembre 2016 del Comitato Nazionale per la Bioetica su informazione, comunicazione e big data[68], di un'Opinione del marzo 2018 del Garante Europeo della Protezione dei Dati sulla manipolazione online[69], e infine delle Conclusioni formulate a valle della Conferenza di Helsinki del Consiglio d'Europa sull'intelligenza artificiale, nel febbraio 2019[70]. Il filo rosso che lega questi documenti tanto nelle proposte quanto nella visione di fondo gira intorno ad alcune parole chiave. Per tutti la *trasparenza* è una necessaria premessa, per consentire la *conoscibilità* di qualunque procedimento e trattamento, ancora di più lo è per provare ad avere una tracciabilità dei contenuti, in una rete in cui l'anonimato è da sempre un aspetto che ne ha garantito fino ad oggi la libertà e il successo. Ma la trasparenza in sé, almeno nelle forme attuali, è del tutto *insufficiente*. Il legislatore dovrà necessariamente intervenire e adottare delle misure attive che perseguano una tutela in concreto dei diritti fondamentali e dello stato di diritto. Dovrà farlo con una *multi-settorialità* che coinvolga vari settori del sapere, compresa la società civile (cfr. art. 80.2 del GDPR), giungendo fino a promuovere e monitorare l'auto-regolamentazione delle piattaforme, nella loro singolarità che certo rende difficile una norma generale e astratta.

---

[65] F. Donati, *op. cit.*

[66] Unesco, World Trends in Freedom of Expression and Media Development, Global Report 2017/2018, 38-9 e 112, in E. Lehner, *op. cit.*, 95.

[67] Ispirandosi a una collaborazione nata in Francia tra Facebook e l'International Fact-Checking Network, in G. De Gregorio, *op. cit.*

[68] Comitato Nazionale per la Bioetica, *Tecnologie dell'informazione e della comunicazione e* big data*: profili bioetici*, 25/11/2016, in http://bioetica.governo.it/it/documenti/pareri-e-risposte/tecnologie-dell-informazione-e-della-comunicazione-e-big-data-profili-bioetici/ (ultima consultazione 11/08/2019).

[69] European Data Protection Supervisor, *op. cit.*

[70] Consiglio d'Europa, *Conclusions from Helsinki Conference "Governing the Game Changer – Impacts of Artificial Intelligence development on human rights, democracy and the rule of law",* 26-27 febbraio 2019, in https://www.coe.int/en/web/portal/-/artificial-intelligence-helsinki-conference-conclusions (ultima consultazione 07/06/2019).

Un'informazione personalizzata è all'opposto di un modello di dibattito pubblico costruito sul contraddittorio, in un contesto che tende anzi a elidere ogni forma di dissonanza rispetto ai propri *probabili* gusti. Questo procedimento, al quale tutti gli utenti si affidano, è gestito da un meccanismo vestito di una neutralità tecnica che, come si è visto, dovrebbe forse essere messa in dubbio, posto che non esiste conoscenza neutrale, senza giudizio, o peggio, pregiudizio. Dunque, non esiste nemmeno decisione neutrale. Ciò su cui bisogna investire dunque, oltre che sull'intelligenza artificiale, è la *coscienza* umana. Il Comitato dei Ministri del Consiglio d'Europa promuove una «critical digital literacy»[71], un'alfabetizzazione digitale *critica*. Sarà certamente dirimente puntare molto sulla *consapevolezza* da parte della cittadinanza degli strumenti che quotidianamente sono impiegati per comunicare, conoscere, esprimersi e del loro funzionamento. Una discussione ampia è necessaria anche sul concetto di *consenso*, sull'anonimato e sui loro limiti[72]. Una delle chiavi del futuro sarà l'atteggiamento del singolo e della società di fronte al potere dei dati. Riusciremo ad "emanciparci" dai dati quando fornirli sarà necessario per usufruire di servizi essenziali, o fortemente richiesti? Il modo in cui i nostri ordinamenti affronteranno questa questione sarà dirimente per la riservatezza nel web. Per questo serve spingere verso ciò che il Comitato Nazionale per la Bioetica definisce un «uso socialmente e psicologicamente sostenibile ed eticamente consapevole»[73] della rete. I nuovi media hanno aperto a grandi potenzialità per poter coinvolgere e far avvicinare alla cittadinanza attiva molte parti sociali che normalmente rischiano l'esclusione, si pensi ai giovani. Non si tratta dunque di tornare indietro nel tempo, ma di dare un indirizzo *sostenibile*, appunto, ai nuovi mezzi. Lo stato di diritto, la democrazia e il diritto nel suo insieme dovranno adattarsi a nuovi paradigmi, "sgonfiare la bolla" e dar prova di resilienza[74]. Pena, trasformare il web in una spider web.

Per questo l'alternativa alla c.d. "*bubble democracy*" non può che essere costituita da un'ampia convergenza di azioni di tutti gli attori sul campo per intraprendere un percorso segnato dalle questioni poco sopra evidenziate. Di fronte alle sfide che i nostri sistemi sono chiamati ad affrontare serviranno una serie di adattamenti, cambi di paradigmi, evoluzioni, in grado spingere questi cambiamenti verso una direzione sostenibile. All'interno di questo modello che potremmo definire di "*resilient democracy*"[75], non

[71] Consiglio d'Europa, Comitato dei Ministri, *Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes*, Decl(13/02/2019)1, adottata il 13 febbraio 2019.

[72] Il CNB parla di «consapevolezza critica dell'impossibilità dell'anonimato», in Comitato Nazionale per la Bioetica, *op. cit.*, 11.

[73] *Ivi.*

[74] «Therefore, we should not only try and shape the development of technology so that it benefits our society, but also prepare our institutions, policies, people and society at large to become more flexible, adaptable and ready to transform. Basically, we need to become more resilient» In European Commission, Joint Research Centre, *Artificial Intelligence, A European Perspective*, 2018.

[75] "Resilienza" e "democrazia" vengono già spesso abbinati tra loro nel linguaggio scientifico corrente, in un gran numero di dibattiti riguardanti le sfide cui la democrazia è sottoposta negli ultimi tempi in vari settori. Il termine "resilienza" infatti, la cui definizione è richiamata nella nota 82, si presta perfettamente a definire una reazione degli equilibri democratici a qualsiasi questione potenzialmente pericolosa. Si ricorda qui a titolo di esempio, per affinità al tema affrontato, un evento tenutosi il 12 febbraio 2019 a Washington dal Carnegie Endowment dal nome "Resilient Democracy in a Digital World". Tuttavia, non è ancora rinvenibile una vera e propria nozione di *resilient democracy*, dovendosi osservare ad oggi un collegamento a questa espressione di

solo le questioni da affrontare, ma anche i meccanismi dello stato di diritto e del diritto in generale svolgono, dal nostro punto di vista giuridico, un ruolo da protagonista. Prendendo le mosse dalle teorie sviluppate da F. Ost e M. van der Kerchove[76], il diritto del XXI secolo dovrà innanzitutto e necessariamente mettere da parte la visione piramidale che ha determinato la sua storia fino a metà '900, lasciando spazio a una visione reticolare: il diritto come frutto del contributo e del confronto dei vari soggetti dell'ordinamento chiamati in causa.[77] Questa "rete" dovrà necessariamente non solo estendersi nei rapporti tra legislatore e giudice e tra giudici[78], ma dovrà anche coinvolgere rapporti inter-ordinamentali. Dovranno emergere, o forse già emergono oggi, forme di regolamentazione diverse da quelle puramente legislative. L'importanza della giurisprudenza è sempre più evidente ormai anche nei sistemi di civil law, soprattutto per quanto riguarda la tutela dei diritti fondamentali nel dialogo tra le corti di tutta Europa[79]. D'altra parte, proprio la concatenazione di atti che partono dal legislatore per giungere all'applicazione del caso concreto da parte del giudice, mette in luce, come già ricordato da numerosi autori, tra cui A. Ruggeri, la sua duttilità a adattarsi alla continua evoluzione del mondo digitale. I recentissimi passi avanti della giurisprudenza eurounitaria richiamati nei paragrafi precedenti ne sono una dimostrazione.

Servirebbe poi elaborare tecniche e forme di regolazione anche al di fuori del diritto "classico". Dovranno collaborare tra loro diverse branche del diritto, in una multi-settorialità, già richiamata, evidentemente necessaria. Ma anche un diritto che esca dai propri schemi e finisca per affiancarsi alle c.d. "politiche". Ad esempio, sarà necessario investire su autorità ed enti indipendenti in grado di monitorare, anche con il supporto della società civile, le dinamiche in corso. Si pensi già su questo a numerosi testi di soft law elaborati da questo tipo di organismi, e non solo, al fine di indirizzare la risposta delle nostre comunità alle sfide dell'intelligenza artificiale. Sulla stessa riga non si dovrebbe dimenticare anche il potenziale ruolo delle istituzioni internazionali, su cui ci si è già soffermati, nell'indirizzo comune della ricerca e della regolamentazione di fronte a giganti tecnologici che già oggi mettono in ombra alcuni poteri pubblici.

Potrebbe poi rappresentare un'opportunità per il diritto di chiamare in causa anche altre branche del sapere in questo sforzo "regolativo". È il caso della teoria dei *nudge*[80], in grado di stimolare, forse più di ogni altro mezzo, comportamenti virtuosi. Ma è il caso soprattutto anche dell'etica e dell'istruzione: nuove

numerose analisi, descrizioni e proposte riguardanti temi molto diversi tra loro, dalla radicalizzazione politica ai conflitti in paesi di recente impronta democratica.

[76] F. OST, M. VAN DE KERCHOVE, *De la pyramide au réseau ? Pour une théorie dialectique du droit*, Bruxelles, 2002.

[77] A. RUGGERI, *La "federalizzazione" dei diritti fondamentali, all'incrocio tra etica, scienza e diritto,* in *MediaLaws*, 2, 2018, 14-31.

[78] V. nota 37.

[79] Si pensi, ad esempio, alle tradizioni costituzionali comuni come base della protezione dei diritti fondamentali nell'Unione Europea, tanto nella giurisprudenza CGUE quanto nella protezione offerta dal diritto primario UE, e d'altra parte nella formazione del c.d. "European consensus" nella giurisprudenza CEDU.

[80] Nudging: "Ogni aspetto nell'architettura delle scelte che altera il comportamento delle persone in modo prevedibile senza proibire la scelta di altre opzioni e senza cambiare in maniera significativa i loro incentivi economici", in R. THALER, C. SUSTEIN, *Nudge: La spinta gentile*, 2009.

forme di educazione dei cittadini a delle competenze trasversali[81] e a quelli che certamente saranno i nuovi mezzi con i quali vivranno le comunità nei prossimi decenni. Questi sono sicuramente i mezzi più efficaci per promuovere quella "critical digital literacy" che riassume magistralmente la proposta del Consiglio d'Europa. Insomma, una democrazia della post-modernità, o della realtà liquida, per dirla alla Baumann, che possa arginare una serie di pericoli tipici, se vogliamo, della post-modernità. Una democrazia chiamata a mettere in gioco e in discussione alcuni dei suoi meccanismi per continuare a garantire la sua funzione nonostante le alterazioni e le perturbazioni provocate dalle questioni messe in luce[82].

[81] Una riflessione in merito al ruolo delle capacità di empatia, creatività e pensiero critico nell'istruzione del futuro è reperibile L. LOBLE, *Apprendre à viver à l'ère de l'IA,* in Unesco, *Courrier Intelligence Artificielle: promesses et menaces*, 2018.

[82] Dalla definizione Treccani di "resilienza" in ecologia: «La velocità con cui una comunità (o un sistema ecologico) ritorna al suo stato iniziale, dopo essere stata sottoposta a una perturbazione che l'ha allontanata da quello stato». E in psicologia: «La capacità di reagire a traumi e difficoltà, recuperando l'equilibrio psicologico attraverso la mobilitazione delle risorse interiori e la riorganizzazione in chiave positiva della struttura della personalità». Disponibile in http://www.treccani.it/enciclopedia/resilienza/ (ultima consultazione 25/10/2019).