Introduzione

Negli ultimi decenni si sente sempre più spesso parlare di Intelligenza Artificiale, soprattutto per i recenti progressi nella robotica e nell'apprendimento automatico. Tali sistemi sono ormai in grado di competere con le capacità umane sotto moltissimi aspetti e sono attualmente utilizzati in altrettanti ambiti, come ad esempio l'intrattenimento, il trasporto, la sanità e la Pubblica Amministrazione.

Affinché tali meccanismi possano contribuire a migliorare la vita dei cittadini, è necessario che essi funzionino nel rispetto dei diritti fondamentali degli individui e che siano disciplinati in modo chiaro a livello normativo. Il loro progressivo e diffuso utilizzo, infatti, pone da un lato nuove opportunità per l'innovazione e lo sviluppo sociale, ma dall'altro molte sfide per il legislatore europeo e italiano laddove non vi sia un corretto e pronto adeguamento della regolamentazione in materia.

Obiettivo di questo elaborato è dunque quello di individuare come e se l'ordinamento vigente sia adatto ad una realtà tecnologica in evoluzione e quali possano essere le soluzioni per una disciplina dell'AI a servizio del cittadino. Si fornirà innanzitutto un quadro generale sui sistemi di apprendimento automatico e sull'impianto normativo europeo con particolare attenzione ai tre settori del diritto principalmente investiti dall'Intelligenza Artificiale: la tutela della privacy, la responsabilità civile e la protezione della proprietà intellettuale.

Lo scopo è infatti quello di valutare se le istituzioni abbiano adottato regolamentazioni adeguate alle possibili problematiche di tali meccanismi e di rispondere ad alcuni interrogativi fondamentali: la sfera privata degli individui è adeguatamente protetta in sistemi basati su enormi quantità di dati personali? Chi è il responsabile per le decisioni prese da una macchina? A chi fa capo il diritto d'autore per le opere generate autonomamente da algoritmi intelligenti?

Si analizzerà dunque l'approccio dai legislatori sui diversi temi, analizzando le decisioni adottate a tutela sia del cittadino sia dello sviluppo economico del settore dell'Intelligenza Artificiale. L'attenzione sarà posta anche alle prospettive europee, nel tentativo di definire il piano d'azione che le istituzioni perseguiranno nel prossimo futuro.

Capitolo I

Il tema della profilazione attraverso l'intelligenza artificiale

1. L'intelligenza artificiale e il *machine learning*

Il concetto di intelligenza artificiale è tuttora oggetto di dibattito, sebbene quest'ultima sia una tecnologia già ampiamente diffusa. I motivi della sua difficile determinazione sono probabilmente riconducibili alle sue innumerevoli quanto complesse funzionalità e alla varietà degli ambiti in cui viene applicata.

Una prima definizione di intelligenza artificiale (in seguito AI, dall'inglese *Artificial Intelligence*) è quella fornita da John McCarthy, l'informatico statunitense che ne coniò il termine nel 1955. Egli la definì come "la scienza e l'ingegneria legate alla creazione di macchine intelligenti"[1].

Nel 2018, la Commissione Europea ha fornito una definizione più articolata: "Intelligenza artificiale indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi"[2]. In questo caso, la Commissione ha riconosciuto a tali meccanismi anche un lato attivo e parzialmente autonomo nello svolgimento delle loro funzionalità. Ciò rende la concezione di intelligenza oggetto di diverse interpretazioni, che a loro volta portano alla necessaria distinzione tra sistemi artificiali forti e deboli.

Quando si parla di meccanismi di apprendimento automatico, ci si riferisce al cosiddetto *machine learning*, cioè a quell'insieme di algoritmi informatici che migliorano automaticamente attraverso l'esperienza e l'uso di dati[3]. Queste tecnologie andrebbero identificate, allora, come forme di AI deboli, perché puntano all'emulazione dell'ingegno umano. L'intelligenza, in questo caso, viene "simulata"[4] e si ricollega alla capacità delle macchine di estrarre schemi complessi apprendendo da grandi volumi di dati con

[1] MCCARTHY J., MINSKY M.L., ROCHESTER N., & SHANNON C.E., *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, in *AI Magazine*, 2006, p. 12.
[2] COMMISSIONE EUROPEA, COM(2018) 237 final, *L'intelligenza artificiale per l'Europa*, Bruxelles, 25/04/2018, p. 1.
[3] Cfr. MITCHELL T., *Machine Learning*, New York, McGraw-Hill Education, 1997.
[4] Cfr. SEARLE J., *Minds, Brains and Programs*, in *The Behavioral and Brain Sciences*, vol. 3, 1980, p. 417.

impressionante precisione predittiva, ma basandosi comunque sulla statistica fornita dalle informazioni a cui attingono[5].

Abbiamo invece AI forti quando tali algoritmi permettono alla macchina di modificare autonomamente i propri risultati, adattandosi all'ambiente in modo spontaneo e risolvendo problemi attraverso l'attuazione di processi di pensiero propri[6]. Nonostante ad oggi nessuna macchina abbia ancora superato il test di Turing[7], l'intelligenza artificiale ha già cominciato ad applicare le proprie eccezionali funzionalità in ambiti legati all'arte e alla robotica cognitiva.

Entrambe queste forme di AI contengono intrinsecamente una serie di questioni etico-giuridiche di non poco conto, che da una parte toccano la sfera dei diritti fondamentali dell'uomo, e dall'altra dimostrano l'assoluta necessità di una normativa nazionale e comunitaria che tenga conto del contributo economico-sociale di queste nuove forme di intelligenza.

In quest'ottica, si può senz'altro parlare di quarta rivoluzione industriale, intendendo con essa la "crescente compenetrazione tra mondo fisico e digitale"[8]. Il motore su cui si fondano i sistemi intelligenti, protagonisti di questa trasformazione tecnologica, utilizza una risorsa tanto nuova quanto fondamentale: i dati. Secondo l'espressione generalmente attribuita al matematico britannico Clive Humby nel 2006, "*data is the new oil*"[9]; in tale prospettiva, il valore dei dati ha inevitabilmente posto nuove questioni relative alla loro regolamentazione e alla tutela dei soggetti coinvolti.

1.1 L'impatto dell'AI sui *Big Data*

Come accennato, per riuscire ad "apprendere", gli algoritmi hanno bisogno di essere alimentati attraverso informazioni. E grazie alle loro straordinarie capacità di calcolo, le

[5] Cfr. BASSOLI E., *Intelligenza artificiale, tutela della persona e dell'oblio*, Pacini Giuridica, 2021, pp. 3-4.
[6] Cfr. SANTUCCI U., *Intelligenza artificiale debole e forte*, in www.umbertosantucci.it.
[7] Il test di Turing si basa sul "gioco dell'imitazione": se una macchina riesce ad essere indistinguibile da un essere umano, allora può essere considerata intelligente. Per un approfondimento, si v. TURING A.M., *Computing machinery and intelligence*, in *Mind*, 59, 1950, pp. 433-460.
[8] SALESFORCE ITALIA, *Che cos'è la quarta rivoluzione industriale?*, in www.salesforce.com, 2019.
[9] Cfr. PALMER M., *Data is the new oil*, in *Ana Marketing Maestros* (https://ana.blogs.com), 2006; MARR B., *Here's Why Data Is Not The New Oil*, in www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil.

tecnologie intelligenti sono in grado di elaborare enormi quantità di dati con rapidità e precisione, ad un costo estremamente ridotto.

Per dare un'idea di quanti siano realmente i dati elaborati a livello mondiale, basti pensare che nel 2010 la loro massa raggiungeva la cifra denominata zettabyte, equivalente a 10^{21} bytes: in termini pratici, 180 milioni di volte le informazioni conservate nella biblioteca del Congresso di Washington[10]. Diversi studi prevedono nei prossimi anni una crescita che arriverà addirittura a sfiorare i 175 zettabyte nel 2025[11]. È per tale motivo che vengono denominati *Big Data* (grandi dati). Nello specifico, essi sono definiti come "*the information asset characterized by such a high volume, velocity and variety to require specific technology and analytical methods for its transformation into value*"[12].

Vista la quantità di informazioni che strumenti sempre più potenti riescono a raccogliere ed elaborare, si intuisce facilmente quanto possa risultare sottile la linea tra rispetto e violazione della sfera privata degli individui. È quindi sempre più rilevante trovare il modo di tutelare il diritto alla riservatezza, o nello specifico il diritto alla privacy.

2. La protezione dei dati personali: la normativa europea

Il Regolamento europeo per la protezione dei dati personali 2016/679 (GDPR) è la principale normativa comunitaria in materia di tutela dei dati personali dei cittadini. Pubblicato sulla Gazzetta ufficiale dell'Unione il 4 maggio 2016, è entrato in attuazione in tutti gli Stati membri due anni dopo, il 25 maggio 2018.

Non si tratta, però, della prima regolamentazione europea riguardo il trattamento di dati personali. Già il 24 ottobre 1995, la Direttiva n. 95/46 del Parlamento europeo impegnava gli Stati dell'Unione a mettere in campo, tramite interventi nazionali di recepimento, una normativa che garantisse la tutela delle persone fisiche in materia di trattamento dei loro dati. In Italia, infatti, la Direttiva venne recepita con la l. 31 dicembre 1996, n. 675, in seguito sostituita dal Codice in materia di protezione dei dati personali (D. Lgs. 30 giugno 2003, n. 196), comunemente noto come "codice della privacy", che per anni ha

[10] Cfr. CASONATO C., *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Dir. pubbl. comp. ed eur.*, 2019, Speciale (maggio), p. 106.
[11] Cfr. REINSEL D., RYDNING J. e GANTZ J.F., *Worldwide Global DataSphere Forecast, 2021–2025: The World Keeps Creating More Data*, in IDC (www.idc.com), 2021.
[12] DE MAURO A., GRECO M. & GRIMALDI M., *A Formal definition of Big Data based on its essential features*, in *Library Review*, vol. 65, n. 3, 2016, p. 124.

rappresentato la fonte primaria della disciplina italiana in termini di tutela della riservatezza.

Tuttavia, a causa delle divergenze tra le varie leggi nazionali di recepimento, l'obiettivo della Direttiva 95/46 di armonizzare le norme e garantire la libera circolazione dei dati personali all'interno dell'Unione mostrò alcune lacune, preso atto delle quali il Parlamento europeo decise di sostituirla con il GDPR. Quest'ultimo, in quanto Regolamento UE, costituisce un atto comunitario dotato di maggiore forza rispetto alla direttiva: non necessita, infatti, di leggi di recepimento, ma è direttamente applicabile in tutti gli Stati membri. Nell'ottica del legislatore sovranazionale, la sua adozione assicurerebbe un livello coerente di protezione dei dati in tutto il territorio dell'Unione e preverrebbe eventuali ostacoli alla loro libera circolazione[13]. L'Italia, dunque, con il D. Lgs. 18 agosto 2018, n. 101, ha modificato ampiamente il codice della privacy nazionale, al fine di armonizzarlo alla disciplina europea.

Il GDPR rappresenta una vera rivoluzione nell'ambito della tutela della privacy. Esso, infatti, porta ad un importante cambio di prospettiva: si passa da un modello formale e prescrittivo che prevedeva controlli *ex post* da parte delle autorità garanti, ad un impianto di tutela basato sui doveri del titolare del trattamento. Con il GDPR, infatti, è il titolare a diventare il protagonista dell'intero processo e, in quanto tale, assume un ruolo centrale di "responsabilizzazione" (principio dell'*accountability*): è ora suo compito garantire un trattamento "lecito, corretto e trasparente nei confronti dell'interessato" (art. 5, par. 1)[14].

Inoltre, l'esponenziale sviluppo delle tecnologie dell'informazione nel primo decennio del nuovo secolo ha provocato una inevitabile modificazione dei concetti stessi di privacy e di dati personali, a cui si è ritenuto di dare una nuova definizione uniforme e più approfondita in tutti gli Stati membri. Anche prima del GDPR, infatti, il codice della privacy dava una definizione di dato personale, intendendo "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale" [art. 4, co. 1, lett. b)].

---

[13] Cfr. MIRANDA C., *Il DPO simbolo della "rivoluzione" europea nel mondo della privacy*, in *Cyberlaws* (https://www.cyberlaws.it/), 08/01/2018.

[14] Cfr. CERRINA FERRONI G., *Il Garante per la protezione dei dati personali di fronte alle sfide dell'intelligenza artificiale* [30/04/2021], *Ciclo di Incontri: I diritti e l'intelligenza artificiale* organizzato dall'Università di Foggia, (video consultabile su CEA Centro E-learning di Ateneo https://www.youtube.com/channel/UCjjkrclFGszX0ClGX8NpZOw).

Con il Regolamento europeo si pone specifica attenzione ai metodi con cui una persona può essere identificabile online tramite meccanismi di intelligenza artificiale e di geolocalizzazione: "si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale" (art. 4, par. 1). Si può, quindi, far rientrare in questo insieme tutto ciò che concerne la vita privata o pubblica di un individuo, come il suo nome, le sue foto, il suo indirizzo, il suo numero di telefono o gli estremi del suo conto corrente. Ma non solo: grazie alle nuove tecnologie, è possibile ottenere informazioni anche su propensioni e atteggiamenti delle persone, che, attraverso i sopracitati algoritmi intelligenti, permettono di stilare un profilo dettagliato del singolo, definendone preferenze e prevedendone comportamenti[15].

È quindi evidente l'estrema importanza che ha avuto il rafforzamento della normativa a tutela dei dati personali dei soggetti per renderla in linea con un contesto innovativo e in continuo mutamento come quello di Internet e delle ICT (*Information and Communication Technologies*).

2.1 L'identità digitale e il consenso al trattamento

Il concetto di identità personale non è di facile definizione, in quanto si presta ad essere utilizzato in diverse dimensioni. In ottica giuridica, la Corte cost. ha ormai da tempo ricondotto l'identità personale nell'alveo delle tutele di cui all'art 2 Cost., intesa come il diritto di essere sé stessi, che include l'insieme di convinzioni ideologiche, morali e religiose dell'individuo[16]. Si tratta pertanto del modo in cui un soggetto viene rappresentato e percepito dagli altri tramite le informazioni che lo riguardano.

In questo contesto si inserisce l'attuale evoluzione tecnologica, che ha provocato un ulteriore ampliamento dell'ambito di definizione dell'identità individuale, che in rete diventa identità digitale.

[15] Cfr. BASSOLI E., *Intelligenza artificiale*, cit., p. 9.
[16] Cfr. BONAMORE D., *Il diritto al nome, patrimonio irretrattabile della persona umana e segno distintivo della personalità – nota a C. cost. 3 febbraio 1994 n. 13*, in *Riv. giur. scuola*, 1994, I, pp. 2435-2439.

Si ha una prima definizione di identità digitale nel DPCM 24 ottobre 2014 [art. 1, co. 1, lett. o)], che la riconosce come "la rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale". In altre parole, tutti i dati presenti online relativi ad una persona concorrono alla creazione della sua identità in rete. Essi vengono raccolti e processati continuamente per mezzo di algoritmi intelligenti ed è proprio tramite la loro aggregazione che i singoli dati acquisiscono significato.

Tuttavia, il soggetto interessato non è l'unico a condividere informazioni sulla propria persona. Ad esse si sommano tutte quelle attribuitegli da altri (è il meccanismo alla base dei *social network*), che contribuiscono in egual misura a costruire la sua identità online. Si è dunque in presenza di due diverse forme di identità digitale, che Roger Clarke distingue in "progettata" e "imposta", intendendo con la prima l'identità creata dall'individuo attraverso informazioni che egli stesso condivide, e con la seconda quella proiettata sulla persona per mezzo di dati pubblicati da terzi[17].

Se, dunque, in rete "siamo i nostri dati"[18], è indispensabile poter esercitare un controllo sul proprio essere. Il GDPR cerca, infatti, di attribuire all'interessato un ruolo attivo nel trattamento dei propri dati attraverso lo strumento del consenso, che definisce come "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento" (art. 4, co. 11). La normativa comunitaria in materia di privacy tutela inoltre i suoi diritti di verifica, rettifica e cancellazione. In tal senso, gli articoli 18 e 21 del GDPR consentono all'interessato di opporsi al trattamento o di limitarlo.

Tuttavia, tale disciplina appare non del tutto soddisfacente, in quanto non tiene conto dell'effettiva natura della rete, in cui l'individuo è oggetto di continue richieste di fornire i propri dati personali per poter usufruire di un servizio online. Ciò comporta il quasi "automatico" consenso dei termini e delle condizioni d'uso da parte degli interessati, anche senza la dovuta consultazione degli stessi. Sarebbe dunque più corretto parlare di

[17] Cfr. CLARKE R., *The Digital Persona and its Application to Data Surveillance*, in *The Information Society*, vol. 10, 1994, pp. 77-92.
[18] RODOTÀ S., *Il diritto di avere diritti*, Roma, Laterza, 2013, p. 395.

"consenso consapevolmente disinformato"[19]. Inoltre, il consenso dell'interessato costituisce solo una delle condizioni di liceità del trattamento dei dati personali previste dall'articolo 6 del Regolamento europeo, per cui il trattamento è consentito anche senza il suo esplicito consenso nei casi in cui esso sia necessario per l'esecuzione di un contratto, per adempiere un obbligo legale, per la salvaguardia di interessi vitali, per l'esecuzione di un compito di interesse pubblico o per il perseguimento dell'interesse del titolare del trattamento o di terzi.

Tale analisi mostra quella che sembra essere una contraddizione del Regolamento europeo: mentre da un lato esso si propone di tutelare il diritto alla privacy quale diritto fondamentale dell'uomo, dall'altro il GDPR dimostra di dare maggiore rilevanza alla libera circolazione dei dati personali, la quale non può essere "limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali" (art. 1, co. 13)[20].

3. Il processo decisionale automatizzato: la profilazione

È in questo quadro giuridico che si inseriscono gli algoritmi intelligenti. Con l'enorme mole di dati da cui possono attingere, essi riescono a catalogare le persone in *cluster*, cioè in gruppi omogenei al loro interno, attraverso un continuo meccanismo di profilazione.

La profilazione nasce come strumento di marketing mirato, attraverso cui le aziende possono conoscere gusti e preferenze dei consumatori per adattare di conseguenza le proprie campagne pubblicitarie. Tuttavia, il GDPR supera la finalità economica originaria e ricomprende al suo interno tutti i comportamenti che possano riguardare aspetti personali della vita degli individui. Esso identifica la profilazione come "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica" (art. 4, co. 4).

La disciplina normativa è costituita principalmente dall'articolo 22, il quale sancisce il diritto dell'individuo a 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". Sono però

[19] CASONATO C., *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Dir. pubbl. comp. ed eur.*, 2019, Speciale (maggio), p. 107.
[20] Cfr. BIANCA M.*, La filter bubble e il problema dell'identità digitale*, in *MediaLaws*, 2019, 2, pp. 42-43.

previste delle deroghe nei casi in cui tale decisione "sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, 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, o si basi sul consenso esplicito dell'interessato" (art. 22, par. 2). In ogni caso, tale trattamento deve essere subordinato a delle garanzie adeguate, come la specifica informazione all'interessato circa l'esistenza di tale processo automatizzato (Cons. 71) e il diritto di ottenere in qualsiasi momento l'intervento umano da parte del titolare del trattamento (art. 22, par. 3).

Tuttavia, come già affermato in precedenza, il Regolamento europeo si scontra con una realtà online in cui il consenso è di fatto "obbligatorio" e viene sistematicamente concesso dagli individui senza la dovuta attenzione. Il risultato è una profilazione che, seppur regolata giuridicamente, viene generata a prescindere dall'intervento dell'uomo e dal suo reale consenso informato. Ci si trova, dunque, in una situazione che si può definire di "dittatura dell'algoritmo"[21], in cui si inverte il rapporto di potere tra uomo e macchina, affidando a quest'ultima decisioni con conseguenze importanti sulla formazione delle identità singole e collettive.

L'utilizzo dell'AI per la profilazione degli individui, quindi, lancia al legislatore sfide importanti su diversi fronti, dall'aspetto sociale del fenomeno alla cosiddetta giustizia predittiva. Il *clustering* online rischia, infatti, di rappresentare da un lato una limitazione al libero confronto di idee (principio base della democrazia), con la conseguente propagazione di pregiudizi e *fake news*[22], e dall'altro un fattore di discriminazione e influenza nelle decisioni giudiziarie.

3.1 La profilazione sui social network: la *filter bubble*

L'applicazione degli algoritmi al trattamento dei dati personali tocca gli ambiti più diversi e permette di offrire all'utente un'esperienza personalizzata nella sua interazione con l'intelligenza artificiale: dai motori di ricerca, ai servizi di traduzione, fino ad arrivare alle piattaforme di *social networking*.

[21] Cfr. MURZIO A. e SPALLINO C., *La dittatura degli algoritmi. Il dominio della matematica nella vita quotidiana*, Diarkos, 2019.
[22] Cfr. BIANCA M.*, La filter bubble*, cit., pp. 39-53.

Coniato già nel 2011 dall'attivista Eli Pariser, il termine *filter bubble* (in italiano "bolla di filtraggio") fa riferimento ai contenuti mirati mostrati online dagli algoritmi, sulla base di dati relativi a gusti e preferenze del singolo raccolti in precedenza. Nella sua opera, Pariser metteva in evidenza gli effetti che sarebbero derivati dall'introduzione da parte di *Google* della personalizzazione delle ricerche, meccanismo utilizzato in modo simile anche dalla piattaforma di *Facebook*. Secondo l'autore, nel presentare i contenuti agli utenti gli algoritmi creerebbero "*a unique universe of information for each of us, which fundamentally alters the way we encounter ideas and information*"[23].

Quasi tutti i siti, e nello specifico i *social network*, utilizzano un sistema di *machine learning* che, attraverso cronologia e dati socio-demografici, crea un profilo dell'utente basato sulle sue preferenze e gli fornisce contenuti che ritiene compatibili con esse[24]. Si tratta di una personalizzazione informativa che dà forma, attraverso gli algoritmi online, ad un'identità digitale "imposta" su cui il soggetto non ha quasi alcun controllo e, spesso, nessuna consapevolezza. È così che il profilo creato dalla macchina costringe e vincola l'individuo in una *echo chamber* (o "camera dell'eco") coerente con le informazioni raccolte dal sistema di intelligenza artificiale[25]. La navigazione diventa, in tal modo, un susseguirsi di articoli e post coerenti con le proprie idee, che alimentano un circolo vizioso in cui una persona entra in contatto esclusivamente con pensieri simili ai suoi e li rafforza.

Questa distorsione di accesso alle informazioni priva il soggetto della possibilità di esporsi ad una pluralità di fonti e costituisce un ostacolo al dibattito libero delle società pluraliste. I sistemi politici democratici, infatti, si fondano sul principio di *government by discussion*, secondo cui deve essere garantito un confronto pubblico e aperto tra idee diverse e confliggenti, che permetta a ogni cittadino di scegliere la propria verità[26]. In assenza di tali condizioni, vengono a crearsi conseguentemente polarizzazioni ed estremizzazioni ideologiche: persone che hanno le medesime opinioni tendono ad esaltarsi a vicenda e a perdere l'inclinazione a discutere le proprie idee con gruppi dalle visioni opposte. Da qui l'importanza della tutela del dissenso[27], in quanto parte del diritto di manifestazione del pensiero protetto dall'art. 21 Cost., il quale riconosce un interesse

[23] PARISER E., *The Filter Bubble: What the Internet Is Hiding from You*, Penguin Books Ltd, 2011, p. 9.
[24] Cfr. MONTALDO R., *La tutela del pluralismo informativo nelle piattaforme online*, in *Medialaws*, 2020, 1, pp. 225-226.
[25] Cfr. BIANCA M., *La filter bubble*, cit., p. 50.
[26] Cfr. PITRUZZELLA G., *La libertà di informazione nell'era di Internet*, in *Medialaws*, 2018, 1, p. 10.
[27] Cfr. PITRUZZELLA G., *ibidem*.