

COVID-19, INTELLIGENZA ARTIFICIALE E DEMOCRAZIA: UN'INEVITABILE DIFFICOLTÀ

Jorge Castellanos-Claramunt¹

Abstract: La crisi del COVID-19 costituirà un *prima* ed un *dopo* nei sistemi democratici, così come li conosciamo oggi. Tutto ciò provocherà una sfiducia di massa sui pilastri su cui si fondano le organizzazioni umane. L'Intelligenza Artificiale irromperà in tutti i settori e sarà potenziata, anche, nello scenario democratico. Proprio per questo, nel presente saggio si tratteranno le questioni di maggior incidenza dell'Intelligenza Artificiale nelle democrazie, mettendo in evidenza i pericoli che possono derivare da una sua applicazione ed indicando anche le migliorie socio-politiche che possono prodursi, con particolare riguardo alla partecipazione politica dei cittadini.

Parole chiave: COVID-19, Intelligenza artificiale, Democrazia, Algoritmi, Personalizzazione, Partecipazione política.

Abstract: The COVID-19 crisis is going to produce a before and after in democratic systems as we know them. All this is going to provoke a massive distrust in the pillars on which human organizations are based. The emergence of Artificial Intelligence in all sectors will also be enhanced in the democratic scenario. For this reason, this article addresses the issues with the highest incidence of Artificial Intelligence in democracies, warning of the dangers that may arise and indicating the improvements that may occur, especially in relation to the political participation of citizens.

Keywords: COVID-19, Artificial intelligence, Democracy, Algorithms, Customization, Political participation.

1. INTRODUZIONE

A causa dell'enorme estensione, a livello planetario, della malattia possiamo sorvolare sulla contestualizzazione tipica dei saggi accademici: il COVID-19 è, senza alcun dubbio, l'indiscusso protagonista del 2020, e speriamo che non lo sia anche dei prossimi anni.

¹ Universitat de València (España). E-mail: jorge.castellanos@uv.es

Recebido em 04/06/2020
Aprovado em 11/07/2020

Come è noto, a fronte della dichiarazione di pandemia per il cosiddetto “coronavirus” dell’Organizzazione Mondiale della Salute (OMS), rilasciata lo scorso 11 marzo 2020 (DE LA SIERRA, 2020, p. 36), si sono sviluppate un’ingente quantità di misure per cercare di contenere e risolvere questo problema di salute globale. L’adozione di siffatte misure da parte dei diversi governi s’inseriscono, naturalmente, in una prospettiva sanitaria che non sarà oggetto di quest’indagine. Tuttavia, come magistralmente ci ricorda l’arcinoto brocardo latino “*ubi homo, ibi societas; ubi societas, ibi ius, ergo ubi homo ibi ius*”, in ciò che concerne gli esseri umani nulla è estraneo al Diritto e, pertanto, per un meccanismo di pura logica, su una decisione che – come l’appena citata – incida sul complesso della popolazione vi è sempre spazio per un’analisi giuridica.

Innanzi a situazioni di eccezionalità, come quella provocata dal coronavirus, si producono restrizioni ai diritti fondamentali con l’obiettivo di salvaguardare la salute della popolazione nel suo insieme. Tanto, comporta la presa di decisioni governamentali che, a causa delle restrizioni delle libertà fondamentali, sarebbero impossibili da sostenere in qualsiasi altro momento: la dichiarazione dello stato d’allarme o emergenza, così come il confinamento nei rispettivi domicili evocano notizie di altre epoche ed altri scenari, come la Seconda Guerra Mondiale.

Il problema sanitario che la malattia sta generando è considerevole. Sono centinaia di migliaia gli infettati e, disgraziatamente, il numero di decessi non smette di aumentare. Questo è, certamente, il problema principale. Peraltro, quando il problema di salute globale sarà finalmente superato, sarà necessario fare un bilancio – come a fronte di qualsiasi catastrofe naturale – dei retaggi che detto processo avrà lasciato. Tra questi, uno che sembra inevitabile è una profonda regressione democratica, a causa delle profonde crepe che, su aspetti fondamentali, si sono prodotte nella società o che già esistevano e si sono semplicemente allargate.

È necessario concentrare i nostri sforzi argomentativi in un concetto: la sfiducia.

La vita, in generale, si basa su parametri basilari di fiducia.

Tutto ciò che facciamo riposa nell’idea che esisterà un domani: confidiamo che domani ci sarà un’alba, confidiamo che, dopo la nostra, ci sarà un’altra generazione, confidiamo in noi stessi e ci fidiamo degli altri. La società, dunque, è fondata su piccole ramificazioni, che si sviluppano in successive embricature umane che consentono il funzionamento della società. Il venir meno di questa fiducia provoca il cedimento degli elementi che sostengono le relazioni

tra le persone: le piccole certezze della vita quotidiana lasciano il posto ad inquietudini condivise (RESTA, 2009).

Sfiducia verso le persone. Questo è l'elemento fondamentale. Gli esseri umani si sono convertiti, potenzialmente nella principale minaccia per i loro simili. Non ci riferiamo, in senso figurato, all'hobbesiano "*Homo homini lupus*", ma all'uomo come potenziale portatore del virus che provoca, inevitabilmente, il distanziamento delle persone dai propri simili. Il pericolo, infatti, consiste proprio nell'avvicinarsi all'altro: non parliamo, poi, della possibilità di intavolare una conversazione. Ci può essere una minaccia più grande, per una società, rispetto a quella in cui i cittadini corrono terrorizzati gli uni dagli altri? L'insolidarietà, la paura, o meglio il panico, prendono forme in comportamenti del tutto irrazionali come l'approvvigionamento massivo di beni di prima necessità.

Sfiducia verso le istituzioni. C'è un sentimento di sfiducia nei confronti del *know-how* dei governanti. Questo non rappresenta di certo una novità: infatti, Innerarity sul punto evidenzia come il fatto che i politici e le politiche siano del tutto insoddisfacenti è tanto palese, che non merita neppure di essere approfondito (INNERARITY, 2015, p. 33). La situazione generata dalla pandemia provocherà la caduta di molti governi nelle prossime tornate elettorali: i cittadini, con ragionevole certezza, riterranno i diversi governi – a prescindere dal loro *colore* – responsabili della gestione sanitaria e sociale.

Sfiducia verso i mezzi di comunicazione. Il proliferare di *fake news*² ha aggravato, negli ultimi anni, il senso di sfiducia della popolazione nei confronti dei mezzi di comunicazione. A tanto pare doveroso legare anche un processo di progressiva *spettacolarizzazione* dell'informazione politica che ha contribuito a minare il prestigio tanto dei politici quanto della categoria giornalistica. Tuttavia, nel caso che ci occupa, l'informazione permanente sui progressi della malattia è senza precedenti. La contabilizzazione, sistematica e quasi burocratica, dei morti e dei contagiati non corrisponde ad un trattamento degno del problema innanzi al quale ci troviamo.

Sfiducia verso la scienza. La scienza evoca un sapere oggettivo, quasi divino, nella misura in cui si elimina la discussione. Il sapere scientifico tende manifestarsi come un complesso di teorie che si compiono, e soltanto nel momento in cui una teoria spodesta una di queste si mette in dubbio la consocenza scientifica anteriore³.

² Secondo il Dizionario Oxford, è stata la parola dell'anno 2017 (MUÑOZ-MACHADO, 2020, p. 122).

³ Siffatto meccanismo di funzionamento della scienza pare essere assai lontano dal più noto dei principi della struttura normativa della scienza, delineata da Robert K. Merton. Il riferimento è al cosiddetto scetticismo

Peraltro, questa *cieca fiducia* nella scienza, da qualche anno, è ormai in caduta libera nel sentire comune della popolazione, come dimostra lo sviluppo di un fronte *anti-vax* che, in Italia, ha portato il Governo a prendere una polemica decisione, poi confermata, con alcune significative modificazioni, in Parlamento (INSANGUINE MINGARRO, 2019).

Siffatto sentimento di sfiducia nei confronti del sapere scientifico porta a questionare, naturalmente, anche le direttive della scienza sulla pandemia che, come è noto, sono state la base fondamentale che ha determinato l'azione dei diversi governi e che ha prodotto un patente malcontento nella popolazione.

Sfiducia verso la democrazia. Pare del tutto paradossale che si sia prodotto, nell'opinione pubblica, il convincimento che la gestione della crisi sanitaria in Cina sia stata ottimale. Risulta curioso perché, di fatto, l'origine di questo problema di estensione globale affonda le proprie radici proprio nel paese asiatico, e concretamente nella città di Wuhan⁴. In ogni caso, si tessono le lodi sul modo in cui i lavori governamentali (autoritari) sono stati sviluppati per contenere il problema. Ciò che s'intende evidenziare con questa considerazione è che, sacrificando i diritti dei cittadini, per la preservazione di un bene superiore, si è riusciti, almeno apparentemente, a frenare il problema sanitario. Trascende, dunque, una sorta di apologia dell'infantilismo democratico, a cui è sottesa la considerazione che la "mano dura" contro la popolazione è la medicina più efficace per combattere i problemi di quest'indole.

D'altronde, da paesi democratici come Italia, Spagna, Regno Unito o Canada, governi di diverse ideologie politiche hanno approvato misure che concentrano poteri e funzioni nell'esecutivo e un rafforzamento delle misure di controllo sui cittadini⁵.

In autocratie o paesi con democrazie fragili, i leader stanno strumentalizzando la pandemia come scusa per debilitare le istituzioni democratiche e le opposizioni, nonché per rafforzare la vigilanza e la censura. Non a caso, la possibilità che alcune di queste misure possano rimanere in vigore dopo il dissolvimento dell'emergenza, preoccupano teorici ed attivisti dei diritti umani e delle libertà civili.

organizzato, in forza del quale ciascuno scienziato è tenuto a sottoporre le sue opinioni alla critica, anche propria, e a confrontarsi criticamente con le opinioni altrui (MERTON, 1973, pp. 273 e ss.).

⁴ La prima comunicazione ufficiale sul COVID-19 si è realizzata il 31 dicembre 2019 dalle autorità cinesi, concretamente dalla Commissione municipale di Salute e Sanità di Wuhan (provincia di Hubei) (DE LA SIERRA, 2020, p. 32).

⁵ Peraltro, come è stato brillantemente affermato, "frente a los efectos de la excepcionalidad necesariamente ha de haber contrapesos y límites" [contro gli effetti dell'eccezionalità devono necessariamente esserci contrappesi e limiti] (COTINO, 2020, p. 90).

Tutto ciò ci conduce a temere che questa tendenza possa convertirsi in una nuova corrente che minacci la democrazia, ed in questo senso l'irruzione dell'Intelligenza Artificiale (d'ora in avanti, IA) e la sua applicazione all'ambito politico può assumere un certo protagonismo⁶.

2. IL MOMENTO DELL'INTELLIGENZA ARTIFICIALE

Da qualche anno, la società si trova in un processo di evoluzione permanente dovuto al successo di Internet e dei nuovi prodotti tecnologici.

La democrazia pare aver mutato il proprio DNA, e la fonte di questa mutazione è la rivoluzione digitale. La politica ormai si fa sugli *smartphone*, a colpi di *post* allarmistici, *tweet* mattutini e *selfie* con gli elettori (BARBERIS, 2020, p. 10). A ciò va sommato che l'irruzione nella vita quotidiana delle cosiddette macchine intelligenti ha determinato un cambiamento non solo sociale, ma anche legale (RAMÓN FERNÁNDEZ, 2019, p. 1). Questi cambiamenti implicano delle necessarie e profonde trasformazioni nei meccanismi di funzionamento del Diritto, le cui strutture – concettuale ed applicative – sono messe duramente in discussione (BOIX PALOP, 2020, p. 225).

A questo processo verrà impressa una forte accelerazione dovuta all'impatto mondiale della pandemia provocata dal COVID-19, sebbene sin dalla scoperta dell'Internet delle cose

⁶ Al fine di superare la pandemia, alcuni paesi si sono affidati alla tecnologia autoritaria. Ad esempio, a Mosca, si stanno utilizzando le migliaia di camera di sicurezza con un moderno sistema di riconoscimento facciale per individuare chi non rispetta le norme di isolamento domiciliare, oltre a tracciare dati sul registro di automobili. A fronte della straordinaria situazione, anche la Commissione Europea ha chiesto a diverse compagnie telefoniche di proporzionare dati anonimizzati per valutare il movimento ed elaborare modelli sull'evoluzione del contagio. In Slovacchia si è optato per localizzare, in via temporanea, i cellulari di chi è affetto dal virus per assicurarsi che la quarantena venga rispettata. In Polonia, il Governo ha adottato una politica di controllo di chi arriva dall'estero e devono necessariamente accedere ad un'applicazione sul cellulare che dimostri che stiano in casa, mediante l'invio di una foto e la risposta ad un messaggio. In Belgio, in virtù di una legge finalizzata ad evitare e comprimere le minacce alla vita umana a causa di problemi sanitari, le principali compagnie telefoniche possono divulgare conversazioni se le autorità lo considerano necessario al fine di controllare i contatti con gli infettati. Negli stati a natura democratica più fragile, dove non vi è la nostra *cultura della privacy*, tali misure sono state adottate senza alcun clamore: pare appena il caso di evidenziare che il rischio aggiunto in detti casi riposa sulla possibilità che dette misure vengano utilizzate per la repressione di attivisti ed oppositori, nonché costituire un pericoloso precedente. Va però segnalato che l'uso di queste tecniche di vigilanza intrusiva è stata la chiave del successo in Corea del Sud. Il paese, che sta superando in maniera ottimale il contagio epidemico, ha applicato un uso massiccio della tecnologia di geolocalizzazione per tracciare i movimenti delle persone sospette di contagio. Sul punto, una solida normativa sull'uso dei dati ed una grande trasparenza da parte del governo ha fatto sì che la popolazione abbia accettato l'uso di dette tecniche senza particolari discussioni (cfr. <https://elpais.com/internacional/2020-03-30/democracia-en-cuarentena-por-coronavirus.html>) (Ultimo accesso, 31/03/2020).

(BARRIO ANDRÉS, 2018) siamo sommersi da incognite che dobbiamo necessariamente risolvere il prima possibile (SALARDI, 2017, pp. 19-38), e che si sono complicate con l'evoluzione della robotica e dell'IA.

Sulla stessa lunghezza d'onda, la Commissione Europea nel suo Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia⁷ indica che:

“l'intelligenza artificiale si sta sviluppando rapidamente. Cambierà le nostre vite migliorando l'assistenza sanitaria (ad esempio rendendo le diagnosi più precise e consentendo una migliore prevenzione delle malattie), aumentando l'efficienza dell'agricoltura, contribuendo alla mitigazione dei cambiamenti climatici e all'adattamento ai medesimi, migliorando l'efficienza dei sistemi di produzione mediante la manutenzione predittiva, aumentando la sicurezza dei cittadini europei e in molti altri modi che possiamo solo iniziare a immaginare. Al tempo stesso, l'intelligenza artificiale comporta una serie di rischi potenziali, quali meccanismi decisionali opachi, discriminazioni basate sul genere o di altro tipo, intrusioni nelle nostre vite private o utilizzi per scopi criminali” (COMMISSIONE EUROPEA, 2020, p. 1).

Pertanto, siamo di fronte ad una graduale sostituzione di una forma di operare determinata dalla progressiva capacità dell'intelligenza artificiale che è destinata a superare l'intelligenza umana in sempre più ambiti (TEGMARK, 2018, pp. 49-55). Come sostiene Pasquale, le decisioni che erano fondate sulla riflessione umana adesso si prendono in maniera automatica con l'impiego di algoritmi, i cui software codificano migliaia di regole ed istruzioni calcolate in una frazione di secondo (PASQUALE, 2015).

Così, in nome di una maggiore efficienza, il ricorso ad algoritmi sta progressivamente sostituendo le decisioni umane –*augmentation systems* (VEALE y BRASS, 2019, pp. 125-127) – in virtù dello sviluppo dell'automazione cognitiva o, direttamente, dell'intelligenza artificiale nella sua massima espressione⁸ (VALERO TORRIJOS, 2019, p. 85).

⁷ Disponibile in: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_it.pdf

⁸ Occorre precisare che questa realtà è giuridicamente presidiata solo dal punto di vista dei dati personali. Si riporta in particolare il Considerando 71 del Regolamento Generale sulla Protezione dei Dati (in inglese General Data Protection Regulation), ufficialmente regolamento (UE) n. 2016/679 in sigla RGPD (più noto con la sigla inglese GDPR), regolamento dell'Unione europea in materia di trattamento dei dati personali e di privacy, adottato il 27 aprile 2016:

In proposito, sono stati enucleati una serie di principi per mezzo dei quali governare quest'evoluzione⁹. In ogni caso, pare innegabile che questo processo di automazione pervaderà ogni ambito della società: economico, sociale, politico e, pertanto, democratico.

[71] “L'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani. Tale trattamento comprende la «profilazione», che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona. Tuttavia, è opportuno che sia consentito adottare decisioni sulla base di tale trattamento, compresa la profilazione, se ciò è espressamente previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento, o se è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, o se l'interessato ha espresso il proprio consenso esplicito. In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura non dovrebbe riguardare un minore.

Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti. Il processo decisionale automatizzato e la profilazione basati su categorie particolari di dati personali dovrebbero essere consentiti solo a determinate condizioni”.

⁹ Il pericolo di una deriva scivolosa nello sviluppo dell'IA ha portato all'emanazione di principi etici in una conferenza tenutasi ad Asilomar (2018, pp. 40-42) dalla comunità scientifica:

1) Research Goal: The goal of AI research should be to create not undirected intelligence, but beneficial intelligence.

2) Research Funding: Investments in AI should be accompanied by funding for research on ensuring its beneficial use, including thorny questions in computer science, economics, law, ethics, and social studies, such as:

- How can we make future AI systems highly robust, so that they do what we want without malfunctioning or getting hacked?
- How can we grow our prosperity through automation while maintaining people's resources and purpose?
- How can we update our legal systems to be more fair and efficient, to keep pace with AI, and to manage the risks associated with AI?
- What set of values should AI be aligned with, and what legal and ethical status should it have?

3) Science-Policy Link: There should be constructive and healthy exchange between AI researchers and policy-makers.

4) Research Culture: A culture of cooperation, trust, and transparency should be fostered among researchers and developers of AI.

5) Race Avoidance: Teams developing AI systems should actively cooperate to avoid corner-cutting on safety standards.

Ethics and Values

3. CONCETTI PRECEDENTI

Nel 1950, Alan Turing descrive la possibilità di un'intelligenza simulata da un computer, mentre il termine intelligenza artificiale venne utilizzato per la prima volta nel 1956 dallo scienziato della computazione nordamericano John McCarthy.

Attualmente, quando parliamo di IA ci riferiamo ad una branca empirica dell'informatica che si occupa dei metodi che consentono ad un computer di risolvere compiti che, se risolti dall'essere umano, necessitano dell'uso dell'intelligenza. L'intelligenza artificiale

6) Safety: AI systems should be safe and secure throughout their operational lifetime, and verifiably so where applicable and feasible.

7) Failure Transparency: If an AI system causes harm, it should be possible to ascertain why.

8) Judicial Transparency: Any involvement by an autonomous system in judicial decision-making should provide a satisfactory explanation auditable by a competent human authority.

9) Responsibility: Designers and builders of advanced AI systems are stakeholders in the moral implications of their use, misuse, and actions, with a responsibility and opportunity to shape those implications.

10) Value Alignment: Highly autonomous AI systems should be designed so that their goals and behaviors can be assured to align with human values throughout their operation.

32

Policy Paper on the Asilomar Principles on Artificial Intelligence

11) Human Values: AI systems should be designed and operated so as to be compatible with ideals of human dignity, rights, freedoms, and cultural diversity.

12) Personal Privacy: People should have the right to access, manage and control the data they generate, given AI systems' power to analyze and utilize that data.

13) Liberty and Privacy: The application of AI to personal data must not unreasonably curtail people's real or perceived liberty.

14) Shared Benefit: AI technologies should benefit and empower as many people as possible.

15) Shared Prosperity: The economic prosperity created by AI should be shared broadly, to benefit all of humanity.

16) Human Control: Humans should choose how and whether to delegate decisions to AI systems, to accomplish human-chosen objectives.

17) Non-subversion: The power conferred by control of highly advanced AI systems should respect and improve, rather than subvert, the social and civic processes on which the health of society depends.

18) AI Arms Race: An arms race in lethal autonomous weapons should be avoided.

Longer-term Issues

19) Capability Caution: There being no consensus, we should avoid strong assumptions regarding upper limits on future AI capabilities.

20) Importance: Advanced AI could represent a profound change in the history of life on Earth and should be planned for and managed with commensurate care and resources.

21) Risks: Risks posed by AI systems, especially catastrophic or existential risks, must be subject to planning and mitigation efforts commensurate with their expected impact.

22) Recursive Self-Improvement: AI systems designed to recursively self-improve or self-replicate in a manner that could lead to rapidly increasing quality or quantity must be subject to strict safety and control measures.

23) Common Good: Superintelligence should only be developed in the service of widely shared ethical ideals, and for the benefit of all humanity rather than one state or organization.

può anche essere definita come la capacità dei programmi per computer di produrre risultati di ragionamento equivalenti a quelli ottenuti dall'intelligenza naturale umana attraverso sistemi di apprendimento artificiale simili a quelli naturali (AGOTE EGUIZÁBAL, 2018, p. 40).

La Commissione Europea nella sua Comunicazione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni: L'intelligenza artificiale per l'Europa¹⁰ segnala che:

“L'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” (COMMISSIONE EUROPEA, 2018, p. 1)¹¹.

In termini generali, l'IA consiste nell'elaborazione di sistemi capaci di risolvere problemi e disimpegnarsi in compiti mediante la simulazione di processi intellettuali. Si può insegnare all'IA a risolvere un problema, ma anche lei stessa può studiare un problema ed imparare a risolverlo senza l'intervento umano. I diversi sistemi possono raggiungere livelli di autonomia ed arrivare ad agire in maniera indipendente. Ciò è quanto meglio conosciuto come *deep learning*, ossia un apprendimento automatico che gestisce grandi insiemi di dati in virtù di livelli addizionali di lavorazione, simili alle strutture neuronali del cervello. Come risultato, si rinvengono modelli astratti di alto livello e riconosce schemi in complessi dati estremamente complessi (PETIT, 2018, p. 5).

Dal suo canto, un algoritmo è una sequenza di passi per risolvere un problema, comandi finalizzati alla trasformazione di un *input* in *output*. La combinazione di questi e la loro integrazione sono alla base di programmi informatici da decenni (COTINO HUESO, 2019, p. 917).

¹⁰ Disponibile in: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52018DC0237&from=ES>

¹¹ Siffatta definizione è stata poi ulteriormente perfezionata dal gruppo di esperti ad alto livello: “I sistemi di intelligenza artificiale (IA) sono sistemi *software* (ed eventualmente *hardware*) progettati dall'uomo che, dato un obiettivo complesso, agiscono nella dimensione fisica o digitale percependo il proprio ambiente attraverso l'acquisizione di dati, interpretando i dati strutturati o non strutturati raccolti, ragionando sulle conoscenze, o elaborando le informazioni derivate da questi dati e decidendo le migliori azioni da intraprendere per raggiungere l'obiettivo dato. I sistemi di IA possono usare regole simboliche o apprendere un modello numerico, e possono anche adattare il loro comportamento analizzando come l'ambiente è influenzato dalle loro azioni precedenti” (COMMISSIONE EUROPEA, 2020, p. 18).

Tutte queste tecnologie convergenti si basano sul *big data*, o macrodati, che integrano automaticamente il trattamento massivo dei dati. L'IA non può esistere senza i dati.

“Il funzionamento di numerosi sistemi di IA, nonché le azioni e le decisioni che ne possono derivare, dipendono in larga misura dai set di dati utilizzati per addestrarli. Occorre dunque adottare le misure necessarie per garantire che, nell'individuare i dati di addestramento dei sistemi di IA, siano rispettati i valori e le norme dell'UE, in particolare per quanto riguarda la sicurezza e le norme vigenti in materia di tutela dei diritti fondamentali” COMMISSIONE EUROPEA, 2020, p. 21).

Nella Risoluzione del Parlamento europeo del 14 marzo 2017 sulle implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto (2016/2225(INI))¹² si afferma che:

“[...] i Big Data si riferiscono alla raccolta, all'analisi e all'accumulo ricorrente di ingenti quantità di dati, compresi i dati personali, provenienti da una serie di fonti diverse, che sono oggetto di un trattamento automatizzato mediante algoritmi informatici e tecniche avanzate di trattamento dei dati, che usano sia informazioni memorizzate sia in streaming, al fine di individuare determinate correlazioni, tendenze e modelli” (PARLAMENTO EUROPEO, 2018, p. 2).

4. INFLUENZA DEGLI ALGORITMI

Per mezzo degli algoritmi si processa una grande quantità di informazione e, nell'organizzarla e dotarla di senso, si trasforma in un'arma con infinite possibilità¹³.

¹² Disponibile in: <https://op.europa.eu/es/publication-detail/-/publication/bba9b363-8fdf-11e8-8bc1-01aa75ed71a1/language-it/format-xhtml>

¹³ Ai fini di eventuali future discussioni su iniziative strategiche, sembra importante chiarire gli elementi principali da cui è composta l'IA, vale a dire i "dati" e gli "algoritmi". L'IA può essere integrata nell'hardware. Nel caso delle tecniche di apprendimento automatico, che costituiscono un sottoinsieme dell'IA, gli algoritmi vengono addestrati per dedurre determinati modelli partendo da un set di dati al fine di stabilire le azioni necessarie al conseguimento di un determinato obiettivo. Gli algoritmi possono continuare a imparare mentre vengono utilizzati. Sebbene i prodotti basati sull'IA possano agire in modo autonomo percependo il proprio ambiente senza seguire un insieme

Tuttavia, esistono precedenti in cui il Diritto sta riuscendo a ridurre ed indirizzare questo potenziale. Così, il *Rechtbank Den Haag* con la sentenza C-09-550982-HA ZA 18-388 dello scorso 5 febbraio¹⁴ ha stabilito che un sistema algoritmico utilizzato dal Governo dei Paesi Bassi per valutare il rischio di frode fiscale, non risponde alle esigenze di proporzionalità e trasparenza necessaria e, pertanto, si pone in contrasto con l'art. 8 della Convenzione Europea dei Diritti dell'Uomo che tutela la vita privata¹⁵. La normativa in questione, impugnata da diverse organizzazioni olandesi in difesa dei diritti umani e civili, è stata dichiarata non conforme a diritto per un elemento riferibile direttamente alla cittadinanza: la necessità di salvaguardare la vita privata così come tutelata dall'art. 8 della Cedu. Si tratta della prima sentenza europea che dichiara illegale un algoritmo sulla base di queste argomentazioni, sancendo così un precedente sulla necessità di stabilire limiti sull'influenza degli algoritmi sulla vita dei cittadini. Difatti, la consocenza di dati personali può portare ad inferire gusti, hobbies e orientamenti politici dei cittadini, ricostruibili attraverso le nostre interazioni con Internet, con le nostre mail, con i nostri likes, con le nostre ricerche.

Inoltre, in tempo reale si possono analizzare le reazioni dei potenziali votanti su determinati fatti. La capacità di manipolare la cittadinanza, così, aumenta in via esponenziale attraverso la ricostruzione delle reazioni a determinati elementi emozionali, che possono essere strumentalizzati da un'ideologia o da una corrente politica: infatti, è possibile creare tendenze, polarizzare le posizioni generando scontri, ma anche fomentare adesioni. In definitiva, la tecnologia risultante dalla combinazione di *big data*, *algoritmi* e *IA* sembra una minaccia molto seria per la libertà dei cittadini (CASTELLANOS CLARAMUNT, 2019, p. 4).

Una deriva negativa di questo processo ci potrebbe condurre verso un'autoritarismo digitale. Gli autori che esprimono questa preoccupazione affermano che il costo d'implementazione di queste forme di controllo sarà molto basso, ed assai appetibile per la loro efficacia.

di istruzioni predeterminate, il loro comportamento è in larga misura definito e limitato dai loro sviluppatori. Gli esseri umani determinano e programmano gli obiettivi che un sistema di IA dovrebbe raggiungere nel modo più efficace (COMMISSIONE EUROPEA, 2020, p. 18).

¹⁴ Liberamente consultabile al seguente link:
<https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878>

¹⁵ Diritto al rispetto della vita privata e familiare: 1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

Siffatto autoritarismo, basato sull'IA e sull'impiego di algoritmi per controllare l'attività cittadina, produrrebbe una società basata sulla censura e la restrizione di libertà. Questo controllo esaustivo ed estenuante della cittadinanza ridurrebbe ai minimi il dibattito politico e provocherebbe un regresso democratico notevole, o addirittura la demolizione degli scenari democratici (WRIGHT, 2018, p. 41).

Come è noto, gli algoritmi possono classificare i cittadini. Mediante la generazione di categorie possono dirigersi campagne politiche specifiche su uno specifico nucleo della popolazione in modo tale da orientare, quanto meno indirettamente, l'azione politica della cittadinanza. Un altro modo di giungere allo stesso risultato sarebbe isolare il cittadino in termini politici, dando così vita a quello definito da Parisier come “*filter bubble*”:

«I filtri di nuova generazione stabiliscono le cose che ci piacciono – in base a quello che facciamo o che interesse a persone simili a noi – e poi estrapolano le informazioni. Sono in grado di fare previsioni, di creare e raffinare continuamente una teoria su chi siamo, che cosa faremo e cosa vorremo. Nell'insieme, creano un universo di informazioni specifico per ciascuno di noi, una “bolla dei filtri”, che altera il modo in cui entriamo in contatto con le idee e le informazioni» (PARISER, 2012, pp. 14-15).

In proposito, non può non citarsi il caso di *Cambridge Analytica*. Si tratta di una compagnia privata che combinava la raccolta analisi dei dati con la comunicazione strategica per il processo elettorale (CASTELLANOS CLARAMUNT, 2019, pp. 11-12). Detta compagnia ha prestato il suo servizio nella corsa presidenziale di Donald Trump e nella campagna sul Brexit nel Regno Unito. Lo scandalo è sorto quando un ex dipendente della compagnia ha dichiarato pubblicamente che si realizzavano pratiche per influire nei risultati elettorali. In particolare, venne generata un'applicazione con il precipuo fine di monitorare il comportamento di persone. Tale sistema veniva poi combinato con un'applicazione di *Facebook* mediante cui è possibile recopilarne informazione degli utenti e dei loro contatti e che, tuttavia, era utilizzabile solo per finalità accademiche. L'applicazione risultante venne poi lanciata sulla piattaforma *Amazon Mechanical Turk*, pensata per il reclutamento di lavoratori su richiesta, da cui venne scaricata da oltre 270.000 cittadini. Per mezzo dei dati di questi, poi, si è potuto arrivare ad analizzare il profilo di 87 milioni di persone, sebbene si è riconosciuto che si è giunti solo a 50 milioni. Cosa si studiava di quelle persone? Gusti, preferenze e

comportamenti di cittadini che vennero venduti a *Strategic Communication Laboratories*, collegata di *Cambridge Analytica*.

Posteriormente, venne utilizzata per generare modelli astratti di potenziali votanti ed usare i loro timori al fine di ottenere voti con messaggi pubblicitari personalizzati lanciati in particolare su *Facebook*, che giocò un ruolo indispensabile in tutto il processo per il suo potente sistema pubblicitario che consente di inviare messaggi in maniera precisa e segmentata. Tanto, combinato con i modelli dei votanti generò la creazione di un canale pubblicitario incontrollabile che permise la manipolazione dei cittadini, che vennero indotti a credere in determinate notizie e, soprattutto, fu canalizzata ed orientata la loro volontà politica (SUÁREZ-GONZALO, 2018, pp. 27-36).

L'obiettivo di tutto questo processo è che un potenziale votante ascolti o legga ciò che può indurlo a votare un determinato partito, a non votare un altro o – semplicemente – andare a votare. E per fare ciò ci si serve dell'ingente quantità di dati generata dai social networks, dalle applicazioni e dall'invio di posta elettronica da cui si può ricavare una vera e propria strategia elettorale (CASTELLANOS CLARAMUNT, 2019, p. 25). Anche Barberis denuncia questa situazione, affermando che:

«Rinchiusi nelle rispettive bolle mediatiche, governi e loro follower si dedicano a tempo pieno all'intrattenimento. I governi sfornano leggi-manifesto per vincere le elezioni. I follower abboccano sempre più distrattamente a news feed selezionati da algoritmi su misura» (BARBERIS, 2020, p. 12).

5. DIFFICOLTÀ DEMOCRATICHE

Se diamo ormai per assodato che un elemento esterno ed artificiale possiede una quantità tale di dati, su di noi e sul mondo, da fornirci la miglior decisione possibile in altri ambiti come quello imprenditoriale, del lavoro o dell'ozio (basti pensare alla gestione degli itinerari, la selezione dei viaggi, l'acquisto di prodotti in base ai nostri gusti, di polizze assicurative in funzione delle nostre condizioni naturali), perché non chiederli consiglio anche sulla madre di tutte le decisioni? Perché non delegare la nostra partecipazione politica a chi ha in mano molte più alternative?

Così facendo, l'intelligenza artificiale eliminerebbe la partecipazione politica dei cittadini. E tutto fondato su un algoritmo, che potrebbe determinare qual è il miglior governo possibile, o quali sono le migliori leggi per una determinata popolazione. Può, dunque, l'intelligenza artificiale stroncare definitivamente la democrazia? Se gli algoritmi possono determinare la decisione ottima in qualsivoglia scenario perché non potrebbero farlo per l'organizzazione politica di una società?

Bene, la risposta a questa sorta di delega democratica ad enti artificiali è semplice: no. Non possiamo cedere ad altri la nostra condizione di persone. Così come la dignità non si può mettere all'asta, in quanto elemento inalienabile degli esseri umani che dota gli stessi di umanità, allo stesso modo la condizione di cittadino non consente la delega di competenze politiche, per molto intelligente che possa essere quell'ente artificiale e per molti dati che esso possa maneggiare (CASTELLANOS CLARAMUNT, 2019, p. 15)¹⁶.

Come ci ricorda Barberis, la democrazia non è mai stata il governo del popolo, semmai è il controllo del popolo sul governo (BARBERIS, 2020). L'introduzione dell'IA nelle realtà democratiche, dunque, deve implicare controlli sulla sua proliferazione e sul suo sviluppo al fine di non intaccare la struttura democratica delle società.

6. CONCLUSIONE

L'IA è una tecnologia strategica che offre molti benefici ai cittadini, alle imprese e alla società nel suo insieme, a condizione che segua un approccio antropocentrico, etico, sostenibile e rispettoso dei valori e dei diritti fondamentali. Essa offre importanti vantaggi in termini di efficienza e produttività, che possono rafforzare la competitività dell'industria europea e migliorare il benessere dei cittadini. Può inoltre contribuire a individuare soluzioni ad alcune delle sfide sociali più urgenti, tra cui la lotta ai cambiamenti climatici e al degrado ambientale, le sfide legate alla sostenibilità e ai cambiamenti demografici, la protezione delle nostre democrazie e, ove tale uso sia necessario e proporzionato, la lotta alla criminalità (COMMISSIONE EUROPEA, 2020, p. 28).

¹⁶ La Commissione Europea nella sua Comunicazione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Una strategia europea per i dati* (Bruxelles, 19.2.2020. COM (2020) 66 finale), si mostra sulla stessa linea nel momento in cui manifesta che la visione della Commissione si basa su valori e diritti fondamentali europei, e nella convinzione che l'essere umano è e deve continuare ad essere al centro. (<https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0066&from=ES>)

Purtroppo, il cosiddetto COVID-19 ha dato origine a nuove situazioni a livello mondiale. Le ripercussioni economiche, politiche e sociali potranno essere analizzati solo con il passare del tempo. In ogni caso, una delle possibili letture di questo catastrofico avvenimento è che la definisca come “era digitale” deve farsi avanti, e deve farlo tenendo in seria considerazione la partecipazione dei cittadini. La possibilità che i cittadini partecipino attivamente nelle loro democrazie per mezzo di formati che consentano la distanza fisica e geografica è diventata, purtroppo, fondamentale.

Tutto ciò provocherà non poche difficoltà nell’ordine democratico, e dunque sarà necessario porre attenzione affinché i principi democratici non vengano alterati¹⁷.

L’estrema facilità che rende possibile l’implementazione dell’IA può condurre ad una progressiva delega delle decisioni dei cittadini verso enti autonomi prodotti dall’IA. Il mutamento di paradigma democratico che imporrà il COVID-19 non deve intaccare pilastri democratici delle società. Pertanto, il miglioramento che questi elementi informatici possono produrre deve essere sempre ricondotto al potenziamento sociale e produttivo, e per poter accedere allo scenario necessita di una profonda revisione umana ed etica.

In definitiva, il nuovo paradigma politico sarà accompagnato da una profonda evoluzione dell’IA. Per mantenere il sistema democratico sarà necessario mettere al centro l’essere umano, che non deve essere relegato ad una posizione secondaria a fronte delle decisioni automatizzate determinate dagli algoritmi. Sarà difficile, ma non possiamo farne a meno.

BIBLIOGRAFIA

AGOTE EGUIZÁBAL, Rubén. “Inteligencia Artificial, Ser humano y Derecho”, *Revista Claves de Razón Práctica*, 257, 2018, pp. 40-45.

ASILOMAR. *Informe sobre los principios Asilomar en Inteligencia Artificial*, Grupo de Estudio Evaluación de la tecnología de la digitalización de la Federación de Científicos Alemanes (VDW), Alemania, 2018, pp. 1-47.

¹⁷ “La strategia europea per l’IA e il piano coordinato sull’IA indicano chiaramente che la fiducia è una condizione indispensabile per assicurare un approccio antropocentrico all’IA: l’intelligenza artificiale non è fine a se stessa, ma è uno strumento a servizio delle persone che ha come fine ultimo quello di migliorare il benessere degli esseri umani” (COMMISSIONE EUROPEA, 2019, p. 2).

BARBERIS, Mauro. *Come internet sta uccidendo la democrazia: Populismo digitale*, Chiarelettere, Milano, 2020.

BARRIO ANDRÉS, Moisés. *Internet de las cosas*, Editorial Reus, Madrid, 2018.

BOIX PALOP, Andrés. “Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la Administración para la adopción de decisiones”, *Revista de Derecho Público: Teoría y Método (Marcial Pons Ediciones Jurídicas y Sociales)*, vol. 1, pp. 223-270. https://doi.org/10.37417/RPD/vol_1_2020_33

CASTELLANOS CLARAMUNT, Jorge. “La democracia algorítmica: inteligencia artificial, democracia y participación política”, *Revista General de Derecho Administrativo*, 50, 2019, pp. 1-32.

COMMISSIONE EUROPEA, *Comunicazione della al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni: L'intelligenza artificiale per l'Europa* {SWD (2018) 137 final, 25.4. 2018, COM (2018) 237 final}. Disponible in: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52018DC0237&from=ES>

COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni: Creare fiducia nell'intelligenza artificiale antropocentrica*, Bruxelles, 8.4.2019, COM (2019) 168 final. Disponible in: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52019DC0168&from=es>

COMMISSIONE EUROPEA, *Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia*, Bruxelles, 19.2.2020, COM (2020) 65 final. Disponible in: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_it.pdf

COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, Una strategia europea per i dati*, Bruxelles, 19.2.2020. COM (2020) 66 final. Disponible in: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0066&from=ES>

COTINO HUESO, Lorenzo. “Derecho y garantías ante el uso público y privado de inteligencia artificial, robótica y big data”, in M. Bauza Reilly (dir.), *El derecho de las TIC en Iberoamérica*, La Ley Uruguay, Uruguay, 2019, pp. 917-952.

COTINO HUESO, Lorenzo. “Los derechos fundamentales en tiempos del coronavirus. Régimen general y garantías y especial atención a las restricciones de excepcionalidad ordinaria”, *El Cronista del Estado Social y Democrático de Derecho*, 86-87, 2020 (Ejemplar dedicado a: Coronavirus), pp. 88-101.

DE LA SIERRA, Susana. “Lectura de urgencia de las reacciones frente al COVID-19 desde una óptica jurídica internacional y comparada”, *El Cronista del Estado Social y Democrático de Derecho*, 86-87, 2020 (Ejemplar dedicado a: Coronavirus), pp. 32-41.

INNERARITY, Daniel. *La política en tiempos de indignación*, Galaxia Gutenberg, Barcelona, 2015.

INSANGUINE MINGARRO, Ferdinando Achille. “Vaccinazioni obbligatorie e diritti fondamentali: la paradossale condizione del minore alla luce del DL n. 73/2017”, *Sociologia del diritto*, 1, 2019, pp. 165-179.

MERTON, Robert K. *The Sociology of Science: Theoretical and Empirical Investigations*, The University of Chicago Press, Chicago, 1973.

MUÑOZ-MACHADO, Julia. “Noticias falsas. Confianza y configuración de la opinión pública en los tiempos de internet”, *El Cronista del Estado Social y Democrático de Derecho*, 86-87, 2020 (Ejemplar dedicado a: Coronavirus), pp. 122-137.

PARISER, Eli. *Il filtro. Quello che internet ci nasconde* (B. Tortorella, Trad.), Il Saggiatore, Milano, 2012

PARLAMENTO EUROPEO, *Risoluzione del Parlamento europeo del 14 marzo 2017 sulle implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto* (2016/2225(INI)), 2018/C 236/10, Gazzetta ufficiale dell'Unione europea, 25.7.2018. Disponible in: <https://op.europa.eu/es/publication-detail/-/publication/bba9b363-8fdf-11e8-8bc1-01aa75ed71a1/language-it/format-xhtml>

PASQUALE, Frank. *The black box society: the secret algorithms that control money and information*, Harvard University Press, Cambridge, 2015.

PETIT, Martí, “Por una crítica de la razón algorítmica. Estado de la cuestión sobre la inteligencia artificial, su influencia en la política y su regulación”, en *Quaderns del CAC*, vol. XXI, 44, 2018, pp. 5-15.

RAMÓN FERNÁNDEZ, Francisca. “Robótica, inteligencia artificial y seguridad: ¿Cómo encajar la responsabilidad civil?”, *Diario La Ley*, núm. 9365, Sección Doctrina, 25 de Febrero de 2019, Editorial Wolters Kluwer, 2019, pp. 1-13.

RESTA, Eligio. *Le regole della fiducia*, Laterza, Bari-Roma, 2009.

SALARDI, Silvia. “Fundamental rights and ‘moral’ Technologies: the legal status of Moral claims to ‘moral enhancement’ by Means of cognitive enhancement in the European legal system”, *Humanidades & Tecnologia em revista faculdade do noroeste de Minas – FINOM*, Ano XI, vol. 11 - Jan/Dez 2017, pp. 19-38.

SUÁREZ-GONZALO, Sara. “Tus likes, ¿tu voto? Explotación masiva de datos personales y manipulación informativa en la campaña electoral de Donald Trump a la presidencia de EEUU 2016”, *Quaderns del CAC*, vol. XXI, 44, 2018, pp. 27-36.

TEGMARK, Max. *Vita 3.0. Essere umani nell’era dell’intelligenza artificiale* (V. B. Sala, Trad.), Raffaello Cortina Editore, Milano, 2018.

VALERO TORRIJOS, Julián. “Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración”, *Revista catalana de dret públic*, 58, 2019.

VEALE, Michael e BRASS, Irina. “Administration by Algorithm? Public Management meets Public Sector Machine Learning”, en Karen YEUNG y Martin LODGE, *Algorithmic Regulation*, Oxford University Press, Oxford, 2019, pp. 121-149.

WRIGHT, Nicholas. “Inteligencia Artificial y orden global”, *Política Exterior*, vol. 32, 185, 2018, pp. 40-48.