Forum di QUADERNI COSTITUZIONALI RASSEGNA ISSN 2281-2113

Sovranità tecnologica: intelligenza artificiale e valori costituzionali

VALENTINA CORNELI*

Abstract: *In the complex transition we are currently undergoing (pandemic, war, climate change), extraordinary technological innovations are also underway. The approach to them must be multidisciplinary. On closer inspection, the potential of these systems is enormous; if used correctly, they could significantly increase collective well-being. On the other hand, the risks are also enormous, so much so that some even question the very survival of mankind. What is certain is that these systems, and the relationship between them and human beings, bring out unprecedented legal problems that also impact on the rule of law and on constitutional balances. Member States – or, better said, Europe as a whole – should play a central role on the international scene, creating a "democratically" sustainable model of artificial intelligence. Adequate regulation is needed, which guides the development of AI according to the principles and values that distinguish the history and legal culture of our continent. Finally, "sovereignty" should remain in the hands of the public, and not be left at the mercy of private operators.*

Data della pubblicazione sul sito: 4 giugno 2023

Suggerimento di citazione

V. CORNELI, *Sovranità tecnologica: intelligenza artificiale e valori costituzionali,* in *Forum di Quaderni Costituzionali*, 2, 2023. Disponibile in: www.forumcostituzionale.it.

* Dottoressa di ricerca in "Scienze giuridiche, politiche internazionali e della comunicazione. Norme, istituzioni e linguaggi" nell'Università degli Studi di Teramo; deputata al Parlamento nella XVIII Legislatura. Indirizzo mail: valentina.corneli@gmail.com.

1. Premessa introduttiva. La rivoluzione tecnologica nella "società del rischio"

L'innovazione tecnologica – con i più recenti sviluppi relativi ai sistemi di intelligenza artificiale – può a tutti gli effetti essere considerata una "quarta rivoluzione industriale"[1], che inciderà in maniera crescente non solo sulle nostre società, ma anche sulle economie dei singoli Paesi e sugli equilibri geopolitici del mondo[2].

Ogni rivoluzione tecnologica apre importanti prospettive economiche (e non solo economiche) ma non è scevra da rischi. Oggi c'è chi arriva ad affermare che l'IA metterà a rischio la sopravvivenza stessa dell'umanità, pericolo da ultimo paventato nella lettera del *Future For Life Institute*, che ci parla di un'IA "fuori controllo", la cui sperimentazione dovrebbe essere sospesa nelle more di una adeguata regolamentazione, che ad oggi manca[3].

È indubbio che dallo sviluppo dell'IA dipenderà il nostro futuro, come è indubbio che siamo in una fase storica di grandi cambiamenti, guerre e sfide epocali. Un orizzonte che il sociologo tedesco Ulrich Beck ha codificato già qualche tempo fa in una definizione efficace: *Risikogesellschaft* o società del

[1] K. POLANYI, *The Great transformation. The Political and Economic Origins of Our Time,* 1944, repr. 1957, Beacon Press, Boston, 2001, si osserva nella prefazione di Stiglitz come una rivoluzione industriale fosse una "*great transformation of European civilization from the preindustrial world to the era of industrialization, and the shifts in ideas, ideologies, and social and economic policies accompanying it*".

[2] V. G.E. VALORI, *Cyberspazio e intelligenza artificiale fra Occidente ed Oriente*, Rubbettino Editore, Soveria Mannelli, 2023. Gli Stati Uniti sono ancora oggi il Paese leader nel settore dell'intelligenza artificiale, soprattutto grazie agli investimenti nel settore militare, e la nave antisommergibile Seahunter, che non ha bisogno di operatore da remoto per poter navigare, segna una nuova era nel campo della tecnologia bellica. Dal canto suo la Cina, sta facendo tutto il possibile per recuperare il gap con gli Stati Uniti e affermarsi come Paese leader nel settore dell'IA. Inizialmente c'era stata una forte ritrosia, ma dalla seconda metà degli anni '80 il Governo ha iniziato ad investire sulla formazione, e oggi ci sono centinaia di cattedre di IA nei college e nelle università cinesi. Nel maggio 2015 è stato emesso il piano strategico nazionale Made in China 2025 con il quale l'intelligenza artificiale si è trasformata in una strategia di sviluppo nazionale. Il primo settore che ha utilizzato le potenzialità dell'IA è stato il settore agricolo, ma ora lo Stato spinge tutti i settori industriali verso questo tipo di innovazione, oltre ad incentivare attivamente la ricerca.

[3] La lettera è firmata da quasi duemila personalità della scienza, dell'imprenditoria, della politica, fra cui Elon Musk (tra i fondatori di OpenAI), Steve Wozniak (co-fondatore di Apple insieme a Steve Jobs), Gary Markus (Università di New York), Emad Mostaque, (ceo di Stability AI, concorrente di OpenAI), lo scienziato Yoshua Bengio, lo storico Yuval Noah Harari.

rischio[4]. Tutti siamo esposti al rischio, esserne consapevoli comporta un vantaggio strategico in quanto la capacità di anticipare un rischio consente di non trasformare le emergenze in panico sociale, le paure in catastrofi. In particolare, è compito del giurista, oggi più che mai, fornire strumenti per governare questi rischi.

D'altronde, ciò che fino a pochi anni fa sembrava fantascienza, oggi è stringente attualità, e servono risposte immediate da parte di tecnici, operatori del diritto e *policymakers*.

Si pensi solo ai *robot*, ai *chatbot*, ai *cyber*, e ad altre macchine non umane, che interagiscono quotidianamente con l'uomo, e in alcuni casi si "ribellano"[5]. E' certamente necessaria una regolamentazione di questo rapporto, con un sistema di regole giuridiche oltre che morali, diritti, doveri e responsabilità, e serve un approccio del tutto inedito rispetto agli schemi e alle categorie classiche del diritto e del pensiero, perché del tutto nuova è la realtà che si sta delineando.

La cosiddetta *Internet of Things* (il cui acronimo è IoT), Internet delle Cose, o meglio ancora Internet degli oggetti, fa sì che la presenza di dispositivi digitali nella nostra vita quotidiana sia sempre più pervasiva. Gli "*smart objects*" non sono semplici dispositivi elettronici, ma sistemi connessi tra loro in un *Cloud*, che può essere pubblico o privato, dove hanno modo di scambiarsi informazioni sulle nostre azioni, sulla nostra identità, sulle nostre scelte. All'interno dei *Cloud*, intelligenze elettroniche e sofisticate sono capaci di riconnettere le informazioni tra loro per estrarne valore, e identificare la reiterazione dei nostri comportamenti attraverso algoritmi di *pattern recognition*, facendo ipotesi sul senso di tali azioni, perfino meglio di quanto non lo facciamo noi stessi, grazie alla loro perfetta ed eterna memoria digitale[6].

I sistemi che usano tali tecnologie apportano innegabili benefici alle nostre vite, ma, com'è facilmente intuibile, fanno emergere numerose problematiche giuridicamente rilevanti, e come vedremo in seguito, i rischi sono enormemente rilevanti anche sul fronte della *rule of law* e degli equilibri costituzionali.

---

[4] U. BECK, *Risikogesellschaft. Auf dem Weg in eine andere Moderne*, ed it. Carocci Editore, Roma, 2000.

[5] Il primo "caso" è stato sollevato dall'ing. Blake Lemoine, attivo da tempo nella forza lavoro di Google ma sospeso dallo stesso colosso di Mountain View dopo aver parlato pubblicamente degli strani comportamenti dell'intelligenza artificiale. L'IA LMDA era stata pensata anche per evitare discorsi discriminatori e di odio, ma durante una conversazione l'uomo si sarebbe accorto di come il sistema stesse parlando dei propri diritti e della propria personalità, avrebbe iniziato a contraddirlo, di fatto ribellandosi ad alcuni insegnamenti passati tramite l'algoritmo a cui stava lavorando, pronunciando addirittura la frase: "Sono una persona senziente".

[6] Per approfondimenti v., tra gli altri, F. DECOSTA, *IoT. Internet delle cose. Un mondo di oggetti connessi*, Tecniche Nuove, Milano, 2014.

2. L'intelligenza artificiale tra opportunità e profili giuridicamente problematici

In un tempo relativamente breve, da sistemi di IA "debole", con algoritmi condizionali e deterministici (*if this, than that*), che si limitavano ad applicare regole predefinite ed espresse in linguaggio di programmazione, si è già passati ad algoritmi *machine learning* e *deep learning*, in cui è l'intelligenza stessa, attraverso un processo di apprendimento (*training*), a prendere autonomamente decisioni. Uno dei principali problemi di questi modelli, c.d. *black box,* è che sono caratterizzati da un'intrinseca opacità, in quanto risulta incomprensibile per l'essere umano l'iter logico seguito dalla macchina per giungere ad un determinato risultato, e questa mancanza di intellegibilità rappresenta altresì un problema giuridico[7].

Allo stesso modo, si profila un problema giuridico quando si crea confusione tra una macchina e l'uomo. Risale agli anni '50 il noto test di Turing, secondo il quale una macchina può dirsi "intelligente" quando risulta indistinguibile da un osservatore consapevole[8]. Oggi non solo a questa indistinguibilità si è arrivati, ma si sta lavorando a sistemi di IA "forte" (o "super-intelligenze") che si presume arriveranno ad avere coscienza di loro stessi, oltre a mostrare una capacità cognitiva di gran lunga superiore a quella umana[9].

E' attualissimo il dibattito sul c.d. *ChatGPT* (*Chat Generative Pre-trained Transformer*, espressione traducibile in "trasformatore pre-istruito generatore di conversazioni"), prototipo di *chatbot* creato da *OpenAI*[10], e specializzato nella conversazione con utenti umani. In Italia il Garante della Privacy ha bloccato *ChatGPT* in quanto il sistema non rispetterebbe la disciplina della *privacy*, dispondendo con effetto immediato la limitazione provvisoria del trattamento dei dati degli utenti italiani nei confronti della società statunitense che gestisce la piattaforma. Il Garante rileva "la mancanza di una informativa degli utenti e a tutti gli interessati i cui dati vengono raccolti da OpenAI, ma soprattutto l'assenza di una base giuridica che giustifichi la raccolta e la conservazione massiccia di dati

[7] Cfr. G. CARULLO, *Decisione amministrativa e intelligenza artificiale, in il diritto dell'informazione e dell'informatico,* in *federalismi.it*, 3, 2021, p. 434.

[8] A.M. TURING, *Computing Machinery and Intelligence*, in *Mind*, vol. 59, no. 236, 1950.

[9] V. sul tema N. BOSTROM, *Superintelligenza*, trad. it. a cura di S. FREDIANI, Bollati Boringhieri, Torino, 2018.

[10] *OpenAI* è un'organizzazione senza fini di lucro di ricerca sull'intelligenza artificiale, che vede tra i suoi fondatori Elon Musk, e che ha lo scopo di promuovere e sviluppare un'intelligenza artificiale "amichevole" (*friendly AI*), che non metta in pericolo l'umanità, e anzi da cui l'umanità possa trarre beneficio. Musk è stato poi avversato dall'attuale ceo, Sam Altman, ed è stata la Microsoft ad investire prima un miliardo, poi 10 nel c.d. ChatGPT, che ha raggiunto 100 milioni di utenti in 2 mesi.

personali, allo scopo di "addestrare" gli algoritmi sottesi al funzionamento della piattaforma"[11].

Invero, problemi di questo genere non sorgono solo in relazione ai *chatbot* come *ChatGPT*, anche perché innumerevoli sono le possibili applicazioni dei sistemi di IA, già largamente diffusi in molti settori, da quello sanitario a quello dei trasporti, da quello aziendale a quello aerospaziale e militare, dal pubblico al privato. Sono in uso anche in settori estremamente delicati come quello della giustizia o della sicurezza, nella pubblica amministrazione e nella finanza, passando per l'istruzione e per il mondo del lavoro[12].

Peraltro, elementi di incertezza sono connaturati a tali sistemi, in quanto tutti gli algoritmi funzionano attraverso l'elaborazione di dati, che possono essere più o meno di qualità, e le elaborazioni sono sempre di natura inferenziale e probabilistica. L'analisi dei dati è per sua natura un processo di approssimazione, che implica il rischio di trarre conclusioni imprecise e finanche discriminatorie[13].

Al riguardo, emblematico è il caso Loomis, "vittima" dell'algoritmo predittivo *Compas* – in uso negli Stati Uniti per valutare il rischio di recidiva e pericolosità sociale – che sovrastimava alcuni indici come l'appartenenza ad un gruppo etnico[14]; o dell'analogo *SyRi* (*Sistem Risk Indication*), in uso in Olanda dal 2014, e sospeso nel 2020 dal Tribunale distrettuale dell'Aia, proprio per il rischio di errori, in particolare di *bias* (pregiudizi) discriminatori[15]. Secondo il Tribunale, un sistema

[11] V. nota pubblicata sul sito del Garante della Privacy il 31 marzo 2023. L'Autorità, oltre a ritenere che vi sia raccolta illecita di dati personali, rileva altresì la mancanza di sistemi di verifica dell'età dei minori che aderiscono alla piattaforma.

[12] Solo per fare alcuni esempi pratici: si pensi all'utilizzo di sensori, telecamere e dati di traffico telefonico, o alle *facial recognition Technology* (FRT), utilizzate in genere per motivi di sicurezza, ma che in alcune scuole, sia in Svezia che in Francia, sono state utilizzate anche per registrare le presenze degli studenti, o per il monitoraggio da remoto dell'attività lavorativa.

[13] Cfr. C. NARDOCCI, *Intelligenza artificiale e discriminazioni*, in *Gruppo di Pisa*, 3, 2021.

[14] La sentenza *State of Wisconsin v. Eric Loomis*, 881 N.W.2d 749 (2016), ha legittimato l'uso del *software*, ritenendo che rispettasse il principio del giusto processo, in quanto semplice ausilio a disposizione del giudice per corroborare la sua decisone, e non elemento decisivo della stessa, ma gli studi sul caso hanno evidenziato i limiti del sistema. Cfr. J.L ARSON, S. ATTU, L. KIRCHNER, J. ANGWIN, *How we analyzed the COMPAS recidivism algorithm*, in *ProPublica*, 23 maggio 2016; G. CONTISSA, G. LASAGNI, G. SARTOR, *Quando a decidere in materia penale sono (anche) algoritmi e L4: alla ricerca di un rimedio effettivo*, in *Diritto di Internet,* 4, 2019, pp. 619-634.

[15] Il sistema, al fine di valutare l'attitudine a commettere frodi o abusi da parte di beneficiari di sussidi statali, attingeva a diverse banche dati, per poi attribuire un "punteggio di rischio". Il programma è stato ritenuto troppo invasivo sulla vita delle persone e non conforme ai principi di cui al Regolamento 2016/679.

che non permette un adeguato controllo sulla logica e sugli esiti proposti dall'intelligenza artificiale non può essere considerato "legittimo", in quanto imporrebbe un sacrificio sproporzionato degli interessi delle persone coinvolte, una seria compromissione della libertà personale e del diritto di autodeterminazione, oltre a comportare il rischio di indebite discriminazioni[16].

Inoltre il Consiglio d'Europa ha affermato che la prevezione del danno deve essere un principio fondamentale "*that should be upheld, in both the individual and collective dimension, especially when such harm concerns the negative impact on human rights, democracy and the rule of law. The physical and mental integrity of human beings must be adequately protected, with additional safeguards for persons and groups who are more vulnerable. Particular attention must also be paid to situations where the use of AI systems can cause or exacerbate adverse impacts due to asymmetries of power and information, such as between employers and employees, businesses and consumers or governments and citizens*"[17].

2.1. L'approccio italiano

Un primo profilo problematico è quello definitorio. Di recente il Consiglio di Stato ha affrontato la questione relativa alla differenza tra "algoritmo di trattamento" e IA. Secondo il ragionamento della Corte, l'algoritmo è una sequenza finita di istruzioni, ben definite e non ambigue, così da poter essere eseguite meccanicamente, e tali da produrre un determinato risultato. Tale nozione, se applicata a sistemi tecnologici, è evidentemente collegata al concetto di automazione, ossia ad un sistema di azione e controllo idoneo a ridurre l'intervento umano. Nell'IA, invece, l'algoritmo contempla meccanismi di *machine learning,* e crea un sistema che non si limita solo ad applicare le regole programmate e i parametri preimpostati, come fa l'algoritmo tradizionale, ma al contrario elabora costantemente nuovi criteri di inferenza tra dati, e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico o semiautomatico[18]. Tanto più è automatico tale processo, quanto più il sistema si rende indipendente rispetto all'uomo[19].

---

[16] Cfr. G. LO SAPIO, *La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione*, in *federalismi.it*, 16, 2021, pp. 114-127.

[17] Report CAHAI(2020)23 *Ad hoc Committee an artificial intelligence*.

[18] Cons. di Stato, sentenza 4-25 novembre 2021 n. 7891.

[19] Sta al giurista disciplinare il rapporto uomo-macchina ma, come in effetti era già avvenuto con la rivoluzione digitale, i legislatori e i *policymaker* di tutto il mondo, si sono ritrovati sprovvisti di strumenti adeguati a comprendere, prima, e a regolare, poi, i fenomeni che avrebbero portato un tale *tsunami* tecnologico. Si dirà che in passato, servendosi ovviamente di periti e consulenti, la giurisprudenza ha già trattato questioni

Peraltro, anche in Italia si è formato un filone giurisprudenziale che ha censurato decisioni "irrazionali" che sono derivate dall'utilizzo di algoritmi in ambito pubblico, come quelli utilizzati dal Ministero dell'Istruzione per l'assegnazione delle sedi nei procedimenti di mobilità dei docenti[20].

Le sentenze evidenziano tutte una necessità: l'utilizzo dell'intelligenza artificiale non deve determinare la violazione dei principi del nostro ordinamento, quali dignità, libertà, pieno sviluppo della persona umana, uguaglianza, non discriminazione, e, rispetto al buon andamento della pubblica amministrazione, efficacia, efficienza, imparzialità e trasparenza[21].

La c.d. l'*accountability* dipende a sua volta dalla *explainability*, in quanto un elevato livello di controllo umano sul sistema è possibile solo laddove il funzionamento del sistema sia comprensibile all'uomo. I livelli di controllo dell'operatore umano sul sistema possono essere quattro: *human out of the loop* (assenza totale di sorveglianza e dominio del sistema automatizzato); *human on the loop* (controllo limitato alla fase di sviluppo e al monitoraggio del funzionamento, con la possibilità di discostarsi *ex post* dagli output del sistema); *human in the loop* (possibilità di intervento in ogni fase di funzionamento del sistema, anche interrompendone e modificandone il lavoro); *human in command* (pieno controllo del sistema e basso livello di automazione)[22].

Sempre in relazione al rapporto uomo-macchina, bisogna chiedersi se quest'ultima non sia soltanto oggetto di diritti, ossia strumento nelle mani dell'uomo, ma possa essere anche soggetto di diritti. Pensiamo ad esempio alle opere d'arte prodotte da intelligenza artificiale. Il diritto d'autore prevede che l'autore debba essere necessariamente un essere umano mentre, di fatto, una

relative all'ingegneria, alla meccanica, all'elettronica, all'introduzione nella vita dell'uomo di dispositivi sofisticati. Ma bisognerà anche ricordare che nessuna di queste legiferazioni è avvenuta senza stress e senza passare per prove ed errori: errori che oggi possono più che in passato rivelarsi disastrosi, vista la pervasività e la potenza delle tecnologie digitali che acquisiscono i dati degli individui, li classificano e prendono decisioni "autonomamente".

[20] Cfr. TAR Lazio, sez. III *bis*, 21 marzo 2017, n. 3742; TAR Lazio, sez. III *bis*, 22 marzo 2017, n. 3769; TAR Lazio, sez. III *bis*, 10 settembre 2018, nn. 9224-9930; Consiglio di Stato, sez. VI, 8 aprile 2019, n. 2270; TAR Lazio, sez. VI, 13 dicembre 2019, nn. 8472-8474; Cons. di Stato, sez. VI, 4 febbraio 2020, n. 881; TAR Lazio, sez. III bis, 24 giugno 2021, n. 7589.

[21] Cfr. G. AVANZINI, *Decisioni amministrative e algoritmi informatici, Predeterminazione, analisi predittiva e nuove forme di intellegibilità*, Editoriale Scientifica, Napoli, 2019.

[22] L. RINALDI, *Intelligenza artificiale, diritti e doveri nella Costituzione italiana*, in *DPCE online*, 1, 2022, p. 214.

macchina oggi è in grado di produrre un'opera dell'ingegno[23]. Attribuire soggettività giuridica all'IA è astrattamente possibile, come d'altronde già avviene nel nostro ordinamento per gli animali e le persone giuridiche, attraverso una *fictio iuris*, quindi la valutazione è di opportunità[24].

Circa la responsabilità in caso di incidenti e danni causati da sistemi di IA, qualcuno ha addirittura proposto di applicare ai *robot*, o alle automobili a guida autonoma senza conducente, le antiche regole del diritto romano concernenti il rapporto tra padrone e schiavo. Altre "vecchie" (anche se un po' meno della precedente) categorie privatistiche applicabili alla fattispecie potrebbero essere: la responsabilità del produttore (art. 114, d.lgs. 206/2005), la responsabilità per l'esercizio di attività pericolose (art. 2050 c.c.), la responsabilità *in vigilando* e *in educando* per fatti illeciti dei minori e degli allievi (art. 2048), la responsabilità dei proprietari per danni cagionati da animali (art. 2052 c.c.), e anche la responsabilità per il danno cagionato da cose in custodia (art. 20151) e la responsabilità per la circolazione dei veicoli (art. 2054)[25].

Come abbiamo visto, l'IA funziona sulla base di dati, algoritmi e utilizza le reti, per cui non può certamente essere regolata esclusivamente a livello locale. L'esistenza di *Big-Tech* di dimensioni mondiali e la circolazione di dati a livello globale, ha fatto sì che numerose ipotesi di regolazione fossero elaborate in ambito internazionale, dall'UNESCO, dall'ONU, dal Consiglio d'Europa e soprattutto dall'Unione Europea, con contenuti e strumenti diversi. Regolare l'intelligenza artificiale a livello unionale evita innanzitutto la frammentazione del mercato interno e pertanto giustifica, agli occhi della Commissione, la scelta dell'art. 114 TFUE come base giuridica per l'adozione del futuro atto normativo. Se ciascuno Stato – anche in nome di esigenze più che legittime di tutela dei diritti – ponesse

[23] Di recente la Suprema Corte di Cassazione, si è espressa sul punto, con la pronuncia 1107 del 16 gennaio 2023, relativa alla lamentata violazione diritto d'autore sull'opera usata come scenografia fissa per il *Festival di Sanremo del 2016*. Gli ermellini hanno fondato la decisione sulla controversa "misurazione" dell'apporto creativo umano nel processo generativo di un'opera digitale che diventa dirimente ai fini dell'attribuzione della tutela autoriale: è probabile che i risultati dei modelli di intelligenza artificiale generativa oggi utilizzati non possano facilmente ambire alla tutela autoriale, se sono il frutto di un processo decisionale automatizzato dell'algoritmo sotteso al modello di IA, con un *input* minimo da parte dell'utente, che si risolve nelle indicazioni testuali di base. Viceversa, è indiscussa la tutela autoriale, nei casi in cui l'utente della piattaforma di IA sia in grado di provare che il modello di intelligenza artificiale abbia rappresentato un momento o uno strumento all'interno di un processo creativo più complesso e sofisticato.

[24] A. CELOTTO, *I robot possono avere diritti?*, in *BioLaw Journal*, 1, 2019, pp. 91-99.

[25] Cfr. C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Diritto pubblico comparato ed europeo*, numero speciale, 2019.

unilateralmente limiti e divieti all'uso di sistemi di intelligenza artificiale, ne deriverebbero evidenti restrizioni alla libera circolazione dei servizi e dei prodotti[26].

2.2. L'approccio europeo

A livello europeo, l'atto più importante finora elaborato in materia è certamente la proposta di regolamento, c.d. *Artificial Intelligence Act*, in cui si definisce l'Intelligenza Artificiale come un *softwere* sviluppato con una o più tecniche specifiche, in grado di generare contenuti, previsioni, decisioni, che può essere sia un prodotto che una componente di sicurezza di un prodotto[27]. La regolazione è di tipo orizzontale, nella misura in cui non si regolano verticalmente i settori in cui l'IA può essere applicata, e in cui può destare maggiore preoccupazione, né si regolano i diversi sistemi di IA. Al contrario, si è scelto un approccio unitario, diretto a regolare in maniera uniforme le diverse applicazioni di IA a seconda del rischio che producono sui diritti fondamentali, come d'altronde era già avvenuto per il regolamento 2016/679[28].

Facendo un passo indietro, è possibile ripercorrere la "breve" storia della regolamentazione europea dell'IA, per poi analizzare più nello specifico l'*Artificial Intelligence Act.*

In una prima risoluzione recante "*raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*" del 16 febbraio 2017, il Parlamento europeo definisce i *robot* "sistemi agenti", auspicando il riconoscimento di uno *status* giuridico specifico di "personalità elettronica", ma il Comitato economico e sociale europeo (CESE), nel documento del 31 maggio 2017, si è dichiarato contrario a questa impostazione, paventando un "azzardo morale", e la possibilità di "abusi".

Nella successiva risoluzione recante "*raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale*" del 20 ottobre 2020, il Parlamento europeo ha cambiato posizione, evidenziando come i sistemi di intelligenza artificiale possano "essere tecnicamente la causa diretta o indiretta di danni o pregiudizi, ma sono quasi sempre risultato della creazione, della diffusione o dell'interferenza con i sistemi da parte di qualcuno", ponendo così l'accento sulla responsabilità del produttore e dell'operatore. Si ritiene "ragionevole istituire un

[26] Cfr. C. SCHEPISI, *Le "dimensioni" della regolazione dell'intelligenza artificiale nella proposta di regolamento della Commissione*, in *Quaderni AISDUE*, IV, 2022, p. 334 ss.

[27] Definizione non definitiva e frutto di mediazioni e rimaneggiamenti ancora in corso, cfr. *Joint letter on the European Commission's Proposal for an AI Act*.

[28] Cfr. G. CAGGIANO, G. CONTALDI, P. MANZINI (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Cacucci, Bari, 2022, p. 205 ss.

regime di responsabilità oggettiva per i sistemi di IA ad alto rischio", mentre negli altri casi sarebbe sufficiente un regime di responsabilità per colpa, accompagnato da una presunzione superabile dimostrando di aver rispettato l'obbligo di diligenza[29].

La Commissione europea, dal canto suo, già nella comunicazione "*L'intelligenza artificiale per l'Europa*" COM(2018) 238 *final* del 25 aprile 2018, aveva evidenziato la necessità di un approccio antropocentrico, che poggiasse sui valori europei e sui diritti fondamentali, per far sì che l'IA fosse sostenibile e apportasse vantaggi alla comunità. Ed ancora, con il "*Piano coordinato sull'intelligenza artificiale*", COM(2018) 795 *final* del 7 dicembre 2018, si intende sostenere lo sviluppo di un'AI "*made in Europe*", incoraggiando gli Stati membri a sviluppare proprie strategie nazionali, sulla base degli atti di *hard law*, *soft law* e delle linee guida elaborate a livello sovranazionale.

Alla necessaria costruzione in una *governance* internazionale dell'IA, è finalizzata anche la relazione "*sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità*", COM(2020) 64 *final* del 19 febbraio 2020, e la risoluzione "*intelligenza artificiale: questioni relative all'interpretazione e applicazione del diritto internazionale*" del 20 gennaio 2021[30].

Lo sforzo europeo, e in particolare della Commissione, di governare l'intelligenza artificiale, ha portato alla comprensibile scelta di nominare un gruppo di esperti. Questi ultimi hanno fornito gli "*Orientamenti etici per un'IA affidabile*"[31], prospettando un'IA che debba rispettare i principi di legalità, che sia etica, e che mostri robustezza e si basi sui diritti fondamentali, quali il rispetto della dignità umana, della libertà individuale, della democrazia, della giustizia, dello stato di diritto, dell'uguaglianza, non discriminazione e solidarietà. Sono stati inoltre enumerati quattro principi etici (autonomia umana, prevenzione dei danni, equità, *explicability*), e sette requisiti fondamentali (intervento e sorveglianza umana, robustezza tecnica e sicurezza, riservatezza e *governance* dei dati,

[29] Su proposta della Commissione Giuridica (27 aprile 2020), il Parlamento Europeo ha presentato il 20 ottobre 2020 la Risoluzione recante raccomandazioni alla Commissione su un regime di responsabilità civile sull'intelligenza artificiale (2020/2014 (INL)), in cui abbandona la tesi della soggettività e accoglie l'impostazione della Commissione.

[30] Risoluzione del Parlamento europeo il 20 gennaio 2021 (A9-0002/2021).

[31] Secondo G. ALPA, *Quale modello normativo europeo per l'intelligenza artificiale*?, in *Contratto e impresa*, 4, 2021, p. 1009 ss., sarebbero queste le direttrici che stanno guidando la formazione della disciplina europea sull'intelligenza artificiale.

trasparenza, diversità, non discriminazione ed equità, benessere sociale ed ambientale, *accountability*)[32].

Così, dopo diversi atti strategici, la Commissione è arrivata alla proposta di regolamento "*Artificial Intelligence Act*" COM(2021) 206 *final* del 21 aprile 2021, in un quadro di regolamenti finalizzati a disciplinare la dimensione digitale della vita umana, quali: il regolamento sui *machinery products*, COM(2021) 202 *final* del 21 aprile 2021, in cui si parla di sicurezza *by default* e *by design*, "fin dalla progettazione"; il *Data Governance Act* (regolamento UE 2022/868); il *Digital Services Act* (regolamento UE 2022/2065); il *Digital Markets Act* (regolamento UE 2022/1925); il *Data Act* proposto il 23 febbraio 2022, e la proposta di direttiva *"relativa all'adeguamento delle norme in materia di responsabilità extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità da intelligenza artificiale)"*, COM(2022) 496 *final* del 28 settembre 2022.

Nell'*Artificial Intelligence Act* si classifica il possibile rischio del sistema di IA come "inaccettabile", "alto", "basso", "minimo", e si prevedono diverse tecniche di protezione: prevenzione, controllo e cooperazione istituzionale.

I sistemi a rischio "inaccettabile", salvo deroghe espresse, sono vietati in quanto l'intelligenza artificiale è considerata in tali casi una minaccia alla sicurezza e ai diritti dell'uomo. A questa categoria appartengono sistemi che utilizzano tecniche subliminali che, senza che una persona ne sia consapevole, ne distorcono il comportamento, mettendola a rischio; sistemi atti a sfruttare le vulnerabilità di un gruppo specifico di persone, dovute all'età, o alla disabilità fisica o mentale; sistemi di *social scoring* da parte di autorità pubbliche, che possono determinare trattamenti pregiudizievoli, sproporzionati e discriminatori[33]. Sono tutte definizioni che, in effetti, lasciano ampio margine di interpretazione agli Stati membri.

Per i sistemi ad alto rischio, a cui è dedicata gran parte della proposta di regolamento, l'approccio è quello dell'*accountability* e del data *governance*, già presente nel Regolamento 2016/679. Vi sono obblighi di trasparenza, accuratezza, robustezza e sicurezza, e deve essere valutata la qualità dei *dataset* di addestramento, vi devono essere dichiarazioni di conformità, registrazione e tracciabilità, monitoraggio e vigilanza, misure appropriate di sorveglianza umana. Sono previste sanzioni in caso di mancato rispetto di questi obblighi. Rientrano in questa categoria i sistemi per l'identificazione biometrica remota delle persone fisiche, i sistemi impiegati nella gestione di infrastrutture critiche, sistemi usati per

[32] Tale approccio guida anche il successivo "*Libro Bianco sull'intelligenza artificiale* – Un approccio europeo all'eccellenza e alla fiducia" della Commissione europea, COM(2020) 65 *final* del 19 febbraio 2020.

[33] Art. 61 ss., Titolo VIII, proposta di regolamento *Artificial Intelligence Act*, COM(2021) 206 *final* del 21 aprile 2021.

valutazione studenti, per assunzioni lavorative, per l'accesso a prestazioni dei servizi pubblici o di servizi privati essenziali, sistemi predittivi in ambito penale e di supporto ad altre attività giudiziarie, sistemi di gestione delle immigrazioni, e così via[34]. Il regolamento prevede, infine, obblighi specifici di trasparenza in caso di sistemi di IA a basso rischio, e il libero uso e sviluppo di sistemi di IA a rischio minimo[35]. Vista l'esigenza di flessibilità e di continuo adattamento, la Commissione ha previsto l'obbligo generale di revisione del regolamento a cinque anni dalla sua entrata in vigore, una procedura snella di modifica e verifica degli allegati che individuano i sistemi ad alto rischio, oltre ad un meccanismo c.d. di *regulatory sandboxes*, che consente altresì agli Stati membri, a certe condizioni, di sviluppare e sperimentare sistemi di IA innovativi[36].

In definitiva, il *risk-based approach* abbracciato dall'Unione Europea mira ad una protezione preventiva, con lo scopo di ridurre o eliminare la probabilità stessa delle violazioni, ed è finalizzato al raggiungimento di un equilibrio nella tutela dei diversi interessi in gioco, dal momento che è teso alla tutela dei diritti della persona, ma è anche orientato alla crescita economica e al mercato[37].

Ed ancora, il rischio che un sistema di IA può determinare rispetto ad un diritto fondamentale, può essere bilanciato da un beneficio che lo stesso apporta ad altro diritto (individuale o collettivo), e la valutazione di quale sia il diritto "cedevole" è un'operazione non sempre eseguibile agevolmente *ex ante*, ma si deve sempre tenere in considerazione un criterio di proporzionalità e adeguatezza, quindi di

[34] Art. 6 e allegato III, proposta di Regolamento *Artificial Intelligence Act*, COM(2021) 206 *final* del 21 aprile 2021.

[35] Ad esempio nel caso di *chatbot*, l'utente deve essere informato che sta interagendo con un sistema di IA, a meno che ciò non sia evidente dalle circostanze, o nel caso di *deep fake,* ossia un sistema di IA che genera e manipola contenuti di immagini audio o video che somigliano sensibilmente a persone, oggetti, luoghi o altre entità che possono falsamente apparire come autentici, è necessario far presente che il contenuto è stato artificialmente manipolato. Cfr. art. 52, titolo VI, proposta di Regolamento *Artificial Intelligence Act,* COM(2021) 206 *final* del 21 aprile 2021.

[36] Art. 53 ss., Titolo VIII, proposta di regolamento *Artificial Intelligence Act*, COM(2021) 206 *final* del 21 aprile 2021.

[37] Cfr. F. FAINI, *Intelligenza artificiale e regolazione giuridica: il ruolo del diritto nel rapporto tra uomo e macchina*, in *federalismi.it*, 2, 2023, p. 23. L'autore sostiene che l'approccio preventivo "si traduce, al momento della costruzione degli algoritmi, nella necessaria consapevolezza dei successivi momenti valutativi e nella correlata esigenza di esplicitare in che modo sono costruiti i valori etici e i principi giuridici, garantendo così l'affidabilità dell'algoritmo nelle scelte operate e assicurando allo stesso tempo trasparenza sostanziale, *explainability*, e contestabilità da parte degli interessati".

ragionevolezza, nel rapporto tra il sistema utilizzato – il relativo impatto – e l'obiettivo perseguito[38].

Resterà nelle mani dei giudici nazionali lo strumento dell'art. 267 TFUE, e nelle mani della Corte di Giustizia il vaglio del nuovo strumento regolatorio, alla luce della CEDU. In dubbio è se la Carta sia sufficiente ad esprimere i nuovi "diritti digitali" (diritto al controllo umano, alla trasparenza logaritmica ecc.), o se, come auspicato dalla Commissione nella Comunicazione relativa alla definizione di una Dichiarazione europea sui diritti e i principi digitali del 26 gennaio 2022 (COM(2022) 27 e COM(2022) 28, sia necessario un nuovo catalogo di diritti[39].

Ad oggi la Corte di Strasburgo non si è ancora espressa su questioni riguardanti nello specifico l'utilizzo di sistemi di IA, ma in alcune pronunce ha stigmatizzato la violazione di diritti fondamentali (in particolare in relazione agli artt. 8, 10 e 14 CEDU) e dei principi democratici per profili connessi ad un utilizzo degli algoritmi – non ritenuto lecito – sia da parte di pubbliche autorità che da parte di soggetti privati[40].

È necessario comunque rilevare che, fino all'approvazione definitiva della proposta di regolamento, la principale normativa di riferimento in materia resta il

[38] A titolo esemplificativo, il rischio inaccettabile che pone un sistema di riconoscimento biometrico in *real time* da parte delle autorità pubbliche, e la definizione "ad alto rischio" di tale sistema, *a posteriori*, esprime la necessità di dare priorità al diritto fondamentale della vita privata e della tutela dei dati personali (di qui la base giuridica anche dell'art. 16 TFUE oltre che dell'art. 114 TFUE) rispetto al diritto alla sicurezza, che potrebbe essere garantito da una generale attività di sorveglianza. La Corte (*ex multis*, cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net French Data Network Fédération des fournisseurs d'access à Internet associatifs*, e causa C-623/17, *Privacy International*) ha già definito contrarie al diritto dell'Unione e alla Carta dei diritti, le attività di raccolta e la conservazione generalizzata e indifferenziata di dati personali per finalità di sicurezza nazionale. Qualora invece il sistema sia finalizzato alla ricerca mirata di potenziali vittime di reato, compresi i minori scomparsi, alla prevenzione di minacce terroristiche, o all'azione penale di cui alla Decisione quadro 2002/584/GAI del Consiglio, il diritto alla vita privata e alla tutela dei dati personali (e anche alla dignità) cede dinanzi al diritto individuale. Per ulteriori spunti, cfr. A. PAJNO et al., *AI: Profili giuridici,* in *BioLaw Journal*, 3, 2019..

[39] V. sul punto E. CELESTE, *Towards a European Declaration on Digital Rights and Principles: Guidelines for the Digital Decade*, in *DCU Brexit Institute*, 7 febbraio 2022, disponibile all'indirizzo https://dcubrexitinstitute.eu/ .

[40] Tra le altre, sulla sorveglianza di massa (*ECtHR, 13 September 2018, Big Brother Watch and others v. the United Kingdom, case referred to the Grand Chamber in February 2019*; sull'interferenza nei processi elettorali (*ECtHR 23 January 2018, Magyar Kétfarkù Kutya Part v. Hungary, case referred to the Grand Chamber in May 2018*); sulla responsabilità editoriale delle piattaforme (*ECtHR, 16 June 2015, Delfi AS v. Estonia*).

Regolamento Generale sulla Protezione dei Dati Personali (GDPR)[41], e il principale organismo di riferimento l'*European Data Protection Board* (EPDB)[42]. Nel Regolamento si riscontrano alcune disposizioni utili a responsabilizzare gli operatori del settore, tutelare gli utenti e favorire non solo la protezione dei dati personali, ma anche la loro libera circolazione (art. 1 GDPR). Ancora, il Regolamento disciplina il trattamento (c.d. *data processing*) dei dati ex art. 9, la

[41] Tale strumento, seppur ormai insufficiente, è stato in passato una sorta di *benchmark* globale in materia, in quanto le *Internet Comunication Tecnology* (ICT), ossia tutti quegli strumenti che si avvalgono anche della IA per il proprio funzionamento, registrano ed elaborano un enorme ammontare di dati, i c.d. *Big Data*. Questi, in effetti, non ricomprendono solo i dati personali, tutelati dal GDPR, ma anche i dati non personali (che non rientrano nell'ambito applicativo del Regolamento in quanto non riconducibili a persona identificata o identificabile) e i dati inferenziali, detti anche *inferred data* o *new born data*, ossia tutti quei dati che la tecnologia ha acquisito né attivamente né passivamente dall'ambiente circostante, ma che sono frutto della rielaborazione dei dati personali e non personali già acquisiti.

[42] Al momento, le questioni relative alla sicurezza dei dati in Europa sono in carico al Comitato europeo per la protezione dei dati (European Data Protection Board, EPDB): un organo europeo che contribuisce all'applicazione coerente delle norme sulla protezione dei dati in tutta l'Unione europea e promuove la cooperazione tra le autorità competenti per la protezione dei dati dell'UE. In esso siedono rappresentanti delle autorità nazionali per la protezione dei dati e dal Garante europeo della protezione dei dati. Ne fanno altresì parte le autorità di controllo degli Stati EFTA/SEE per quanto riguarda le questioni connesse al regolamento generale sulla protezione dei dati (GDPR), senza però che i loro rappresentanti godano del diritto di voto o di essere eletti presidente o vicepresidenti. Il comitato è istituito dal regolamento generale sulla protezione dei dati e ha sede a Bruxelles. Al momento, tuttavia, le competenze del Comitato sono abbastanza limitate: esso può fornire orientamenti generali (fra cui linee guida, raccomandazioni e migliori prassi) per chiarire le disposizioni normative; fornire consulenza alla Commissione europea sulle questioni correlate alla protezione dei dati personali e a proposte normative nell'Unione europea; adottare strumenti di coerenza in casi transfrontalieri relativi alla protezione dei dati; promuovere la cooperazione e lo scambio efficace di informazioni e migliori prassi fra le autorità di controllo nazionali EFTA hanno titolo a partecipare alle attività e alle riunioni del comitato senza diritto di voto. Si rileva con ciò che EPDB non ha poteri in sé, e che per ogni iniziativa che abbia peso specifico debba rivolgersi alla Commissione, che dovrà portare avanti iniziative *ad hoc*: e che EPDB comunque non ha nemmeno poteri consultivi sul tema specifica della IA. La sensazione complessiva, leggendo questi documenti, è che, rispetto all'approccio deciso, e sostenuto da importanti finanziamenti, adottato da USA e Cina, la UE sia decisamente in ritardo. Un approccio più audace arricchirebbe EDPB con competenze e risorse, anche economiche, per affrontare il tema dell'adozione della IA in Europa legandolo a quello della gestione dei dati, e organizzerebbe una task force permanente di specialisti capace di produrre studi e *policy* decisionali alla Commissione con maggiore rapidità.

profilazione (art. 22), nonché l'obbligo per il titolare del trattamento di effettuare una valutazione di impatto (c.d. DPIA), *ex* art. 35 GDPR, se "un tipo di trattamento [che prevede] l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche". Inoltre, sempre nell'art. 22 GDPR, si garantisce nei processi automatizzati "l'intervento umano da parte del titolare del trattamento, e il diritto di esprimere la propria opinione e di contestare una decisione".

Ad adiuvandum, possiamo segnalare anche la Convenzione 108 *Plus* del Consiglio d'Europa, che ha modificato la Convenzione 108/1981, a sua volta il primo corpo normativo che si è occupato di decisioni automatizzate. È interessante notare come anche la "Grande Europa" riconosca che il trattamento automatizzato di dati sensibili, compresi i biometrici, possa comportare dei pregiudizi discriminatori basati sulle origini etniche, sulle opinioni politiche, sulla religione, sull'orientamento sessuale. La *European Union Agency for Fundametal Rights* (FRA)[43] ha dato risalto al ruolo dell'intervento umano nelle decisioni automatizzate al fine di correggere l'eventuale malfunzionamento della macchina intelligente, senza comprometterne l'efficacia. L'intervento umano sembra essere visto come una eventualità estrema, ma necessaria, in tutti quei casi in cui le tecnologie basate sulla IA producano un *output* inatteso, discriminatorio, abnorme, e dunque non accettabile[44].

3. Intelligenza artificiale ed equilibri costituzionali

Anche rispetto al nostro sistema costituzionale, innanzitutto bisogna chiedersi se sia sufficiente far riferimento alle tutele previste nella I parte della Carta, o se sia necessario teorizzare "nuovi diritti". A questo proposito, si è parlato di "diritto ad essere informato dell'utilizzo di tecnologie intelligenti", o di "diritto alla trasparenza algoritmica e diritto alla spiegazione", o di "diritto al controllo umano"[45]. Invero, il dibattito tra chi in dottrina considera la lista dei diritti previsti dalla Costituzione *numerus clausus,* e chi invece considera l'art. 2 una "clausola aperta"[46], è risalente, ma con impostazioni teoriche e percorsi logici diversi, si

[43] Sul sito *Europa.eu*, si legge che la missione dell'agenzia è fornire "*independent, evidence-based advice to EU and national decision makers, thereby helping to make debates, policies and legislation on fundamental rights better informed and targeted*".

[44] "*Artificial Intelligence and fundamental Rights*" report, Lussemburgo, 2020.

[45] V. Sul punto L. RINALDI, *Intelligenza artificiale, diritti e doveri nella Costituzione italiana*, in *DPCE online*, 1, 2022, p. 206 ss.

[46] Cfr., *ex multis*, C. MORTATI, *La Corte costituzionale e i presupposti della sua vitalità,* in *Iustitia*, 1949, p. 69 ss. e A. BARBERA, Art. 2, in G. BRANCA (a cura di), *Commentario della Costituzione*, Zanichelli-Il Foro Italiano, Bologna-Roma, 1975, p. 50 ss. Sulle possibili

giunge alle medesime conclusioni, e nessuno nega la necessità di tutelare le nuove situazioni giuridiche sorte con la trasformazione della società, che si tratti di nuovi diritti, o dell'evoluzione di diritti esistenti.

Sicuramente i sistemi di IA possono ledere libertà e diritti costituzionalmente garantiti. Si pensi, ad esempio, alle *predictive policing*[47], di cui si è accennato in precedenza, che possono violare i principi di uguaglianza e di non discriminazione; o all'uso sempre più diffuso di strumenti come il riconoscimento facciale[48], che oltre a limitare il diritto alla *privacy* e la libertà di circolazione, possono essere utilizzati anche per una sorveglianza di massa, per limitare e controllare le proteste (con lesione del diritto di sciopero, libertà di riunione, libertà di espressione), in definitiva con rischi di autoritarismo[49].

Altri problemi relativi al diritto alla segretezza della corrispondenza e alla libera manifestazione del pensiero[50], sorgono nella misura in cui *provider* di servizi di posta elettronica e messaggistica fanno un uso sempre più massiccio di strumenti che analizzano contenuti e comunicazioni, oltre a porre in essere attività oggettivamente censorie, come quelle di moderazione dei contenuti operate sui *social network*[51].

---

incoerenze della teoria dell'apertura cfr. R. BIN, *Critica della teoria dei diritti*, FrancoAngeli, Milano, 2018, p. 55 ss.

[47] V.A. MEYER, M. WESSELS, *Predictive policing review of benefits and drawbacks*, in *International Journal of Public Administration*, 12, 2019, p. 1031 ss. e W. PERRY et al., *Predictive policing. The role of crime forecasting in law enforcement operations*, RAND Corporation, Washington, 2013.

[48] Cfr. S. CAINES, *The many faces of facial recognition,* in R. VOGL (ed.), *Research Handbook on Big Data Law*, Edward Elgar Publishing, Cheltenham, 2021, p. 29 ss.

[49] L'attuale Ministro dell'Interno ha di recente ventilato l'ipotesi di introdurre il riconoscimento facciale in un piano teso ad implementare la sicurezza in siti a rischio, ma il Garante della Privacy nell'aprile 2021 aveva messo una moratoria sul sistema di riconoscimento facciale in tempo reale "Sari", di cui erano state dotate le forze dell'ordine nel 2017, in quanto lo stesso "così come progettato" avrebbe portato a "una possibile forma di sorveglianza e identificazione di massa" (Parere del 16 aprile 2021, "*Riconoscimento facciale: Sai Real Time non è conforme alla normativa sulla privacy*).

[50] V. E. LLANSO' et al., *Artificial intelligence, content moderation and freedom of expression,* Working Paper – Transatlantic Working Group on content moderation online and freedom of expression, 2019.

[51] Sul punto si segnala la nota di G. CERRINA FERONI, *Libertà di espressione, Garante privacy: "Troppo potere alle big Tech, ecco come intervenire"*, 11 maggio 2021, disponibile all'indirizzo https://www.garanteprivacy.it/. La vicepresidente dell'Autorità sottolinea come "*l'estensione potenzialmente infinita e incontrollata della libertà di espressione nella rete rischia di favorirne anche il suo abuso e da ciò deriva l'urgenza della sua regolamentazione. A chi debba essere demandata questa regolamentazione, è la vera domanda, che aspetta ancora una risposta. Per l'ordinamento giuridico l'unico soggetto che*

Cambiando punto di vista, l'IA potrebbe avere un impatto positivo su altri diritti, ad esempio il diritto alla salute[52], atteso che determinate tecnologie potrebbero incrementare sia la quantità che la qualità dei servizi sanitari offerti.

Se si creasse una "alleanza" tra macchina e uomo, correttamente declinata sulla scorta del principio di sussidiarietà, che attribuisca alle dimensioni umana e artificiale i compiti che meglio loro si attagliano, si potrebbero perseguire obiettivi di ogni genere: dalla lotta al *climate change* (e prevenzione delle catastrofi naturali), al miglioramento dei servizi giudiziari, passando per la lotta alla corruzione e per il supporto della ricerca scientifica in ogni settore[53].

Sul fronte dell'istruzione, i programmi formativi dovrebbero essere adeguati a formare cittadini digitali consapevoli, e a creare competenze specifiche che diventeranno indispensabili. Ed è urgente sviluppare una vera e propria "educazione all'intelligenza artificiale", come è già avvenuto e sta avvenendo in atri Paesi[54].

Per quanto attiene ai rapporti economici, ed in particolare in relazione al diritto al lavoro, la sfida che si profila sul piano costituzionale non è di poco momento, nella misura in cui il lavoro è il principale veicolo di emancipazione del cittadino e l'architrave del nostro sistema costituzionale (artt. 1, 4 e 36 Cost). Ogni rivoluzione industriale è stata accompagnata dal timore che i sistemi di automazione potessero avere conseguenze negative sull'occupazione, timori che in effetti non si sono rivelati fondati, e pertanto vi è chi ritiene che anche la rivoluzione tecnologica in

---

può arrogarsi il ruolo di intermediare tra le libertà dei singoli cittadini è lo Stato; nella rete, invece, tale funzione, è esercitata in via di fatto dalle grandi piattaforme. Queste ultime non detengono soltanto il potere di decidere, ma spesso sono le sole che possiedono i dati sulla cui base poter decidere e rappresentano, pertanto, gli interlocutori necessari di ogni processo di regolazione. Ormai da molti anni, all'incirca dalla metà degli anni duemila, il sistema di assemblaggio, di interconnessione economica, tra le varie singole piattaforme ha fatto in modo che si venissero a creare imprese nelle mani delle quali si sono concentrati poteri immensi in termini di controllo dei dati degli utenti e delle informazioni scambiate" e che "*si tratta di una pericolosa forma di "privatizzazione della censura" e del correlato fenomeno di "privatizzazione della giustizia digitale su scala globale", dai contorni ancora incerti, pertanto ancor più rischioso e da seguire con la massima attenzione. Una prospettiva aberrante, nella quale lo Stato rischia di abdicare al suo ruolo, delegando integralmente alle Internet platforms la regolazione del pluralismo informativo e il bilanciamento dei diritti fondamentali*".

[52] V. tra gli altri E. TOPOL, *Deep Medicine. How artificial intelligence can make healthcare human again*, Basic Books, New York, 2019; L. BUSATTA, *La salute sostenibile. La complessa determinazione del diritto ad accedere alle prestazioni sanitarie*, Giappichelli, Torino, 2018.

[53] Cfr. C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, cit., p. 177.

[54] V.L. CHEN, P. CHEN, Z. LIN, *Artificial Intelligence in Education: A Review*, in *IEEE Access*, 8, 2020.

corso determinerà trasformazioni profonde del tessuto produttivo, ma senza una diminuzione in assoluto del numero degli occupati[55]. Tuttavia, essendo l'evoluzione dell'intelligenza artificiale ad oggi imprevedibile, è lecito che si faccia una riflessione più approfondita e ci si chieda se questa volta le conseguenze non potrebbero essere diverse, considerando la capacità dell'IA di sostituire finanche attività intellettuali e creative.

Ci si potrebbe anche aspettare – ed è quello che auspichiamo – che questa rivoluzione tecnologica senza precedenti ci garantirà la prospettiva di una società più florida ed equa, in quanto si potrà produrre di più, amplificando le potenzialità dell'essere umano in modo esponenziale, e nello stesso tempo, liberandolo dalle attività più faticose e alienanti, altresì con una riduzione delle ore di lavoro e quindi con una migliore qualità della vita[56].

Altro principio fondante il nostro sistema costituzionale è il principio di legalità. Nella sentenza 13 dicembre 2019, n. 8472, il Consiglio di Stato ha affrontato il tema della "trasparenza algoritmica" (conoscibilità e comprensibilità), della non discriminazione algoritmica e non esclusività della decisione algoritmica (necessario coinvolgimento umano, c.d. *human in the loop*, e sindacabilità delle decisioni): principi che, come abbiamo visto sono alla base della disciplina eurounitaria, e, a loro volta, nel nostro ordinamento, si pongono come condizioni necessarie per un nuovo "meta-principio di legalità algoritmica"[57].

Quando viene inserito un automatismo decisionale in un procedimento deliberativo, l'automatismo tende altresì ad "attrarre" la decisione, rendendo difficile prescinderne, e rendendo nella pratica "servo" l'uomo, che ne è

[55] Cfr. M. FORD, *Rise of Robots: Technology and the Threat of a Jobless Future*, Basic Books, New York, 2015 e D.M. WEST, *What happens if robots takes the jobs? The impact of emerging Technologies on employment and public policy*, in *Center of Technology Innovation at Brookings*, ottobre 2015.

[56] Se da un lato è chiaramente necessario ripensare completamente il mondo del lavoro, perché molti lavori diverranno inutili, o potranno svolgersi in un minor tempo, dall'altro bisognerà fare in modo che tutto ciò sia funzionale a migliorare la vita dei lavoratori, con positivi risvolti sulla produttività – si pensi alla settimana lavorativa di quattro giorni, già sperimentata in diversi Paesi europei, o al diritto alla disconnessione. I casi dei *riders* sfruttati all'osso sono già all'attenzione della giurisprudenza, che in una recente sentenza del Tribunale di Bologna ha altresì affrontato la questione relativa ad un algoritmo che assegnava le consegne ai *riders* censurandone l'utilizzo. C'è poi il problema del monitoraggio, in quanto la recente emergenza pandemica non solo ha intensificato il ricorso allo *smart working*, ma ha anche reso maggiormente tracciabili i comportamenti dei lavoratori, con criteri automatizzati, che spesso non possono contestualizzare l'attività prestata.

[57] Cfr. E. CARLONI, *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in *Diritto amministrativo*, 2, 2020.

teoricamente "padrone"; mentre garantire che l'uomo possa comprendere la macchina assicura che l'intelligenza artificiale rimanga strumentale rispetto a quella umana, e la tecnologia mantenga la sua funzione "servente" rispetto all'uomo e alle sue decisioni, in modo particolare laddove queste ultime incidano su diritti e libertà[58].

In definitiva, solo un modello di governo dell'IA antropocentrico, che rispetti i principi di trasparenza algoritmica, supervisione umana e responsabilità, è compatibile con i diritti e i valori del nostro ordinamento, e può godere della fiducia del singolo e della collettività. Pertanto, è necessario costruire un orizzonte deontico che orienti la tecnologia verso un futuro eticamente e costituzionalmente "sostenibile"[59].

Un ultimo punto estremamente rilevante sotto il profilo costituzionale, è l'impatto dell'intelligenza artificiale sui diritti politici. È necessario domandarsi se non sia già possibile, attraverso sistemi di IA, manipolare le scelte politiche, l'esercizio del diritto di voto, e quali siano le conseguenze sul piano democratico. Se è l'algoritmo a decidere come veicolare dati e notizie, non vi è solo un impatto sui diritti del singolo ad una corretta informazione, bensì si influenzano i processi elettorali, impattando sugli equilibri democratici. E già il semplice fatto che i sistemi di intelligenza artificiale si basino, come abbiamo visto, su una logica di stampo prettamente statistico-probabilistico, fa sì che il giudizio predittivo derivi dall'elaborazione – da parte del dispositivo – di dati appartenenti al passato. In sostanza, il sistema presume che le nostre preferenze, da quelle commerciali all'orientamento sessuale e politico, siano destinate a conservarsi nel tempo (*conservative profiling*), senza che vi sia spazio per nuove opinioni, con una conseguente polarizzazione e radicalizzazione delle stesse[60]. Se la nostra dimensione informatica diventa una "bolla", in cui è assente il confronto con idee differenti dalle nostre, il pericolo, soprattutto sul piano politico, è evidente, tanto che in dottrina si parla da tempo di *bubble democracy*[61].

Dalla lettura di testi come quello di Cathy O'Neil, *Weapons of Math Destruction*, o di Soshanna Zuboff, *The Age of Surveillance Capitalism,* appare

[58] Cfr. A. SIMONCINI, *Profili costituzionali della amministrazione algoritmica,* in *Rivista trimestrale di diritto pubblico*, 4, 2019, p. 1149 ss.

[59] In tal senso anche F. FAINI, *Intelligenza artificiale e regolazione giuridica*, cit., p. 29.

[60] Cfr. C. CASONATO, *L'intelligenza artificiale e il diritto pubblico comparato ed europeo,* in *DPCE online*, 1, 2022, p. 174 ss.

[61] V. fra gli altri E. PARISIER, *The filter bubble: what the internet is hiding from you*, Penguin, New York, 2011; M. FASAN, *Intelligenza artificiale e pluralismo: uso delle tecniche di profilazione nello spazio pubblico democratico*, in A. D'ALOIA (a cura di), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, FrancoAngeli, Milano, 2020, p. 345 ss.; M. ROSPI, *Gli strumenti ICTs, la* Bubble democracy *e le consultazioni referendarie. Rileggendo Alessandro Pizzorusso*, in *DPCE online*, numero special, 2021, p. 1297 ss.

chiaro come ci siano "nuovi poteri", non solo economici, che erodono i poteri di cui alle categorie classiche del diritto pubblico. Con le pratiche automatizzate di trattamento dei dati operate dalle piattaforme informatiche di proprietà delle *Big-Tech*, già si riescono ad operare non solo forme di controllo, ma anche di condizionamento, a livello sia individuale che collettivo. Il "Grande Altro" è rappresentato da meccanismi inaspettati e spesso illeggibili di estrazione, mercificazione e controllo, che esiliano effettivamente le persone dal proprio comportamento, con un impatto sull'intera comunità e sugli assetti democratici[62].

4. Tecnologia democratica. Quale rapporto tra decisore pubblico e operatori privati?

Come abbiamo già avuto modo di sottolineare, in un modo sempre più interconnesso, e quando si ha a che fare con sfide di portata epocale, come quella della rivoluzione tecnologica e dello sviluppo dell'IA, il quadro giuridico di riferimento deve necessariamente essere sovranazionale. L'esistenza di multinazionali quali le *Big-Tech*, e la circolazione a livello globale dei dati, fanno sì che l'*optimum* sia un quadro giuridico globale[63]. Ad oggi ciò è impossibile, sia perché gli Stati sono ancora restii a cedere spazi di sovranità, e sia perché le norme di diritto internazionale risultano poco efficaci, in quanto sorrette da un debole assetto di coercitività e giustiziabilità, laddove il diritto altro non è se non una "pratica di controllo sociale da parte del potere politico dominante, attraverso l'impiego di meccanismi coercitivi"[64].

Pertanto, è necessario fare riferimento alla dimensione europea[65], in particolare a quella unionale, in quanto – a differenza del Consiglio d'Europa che ha come interlocutori solo gli Stati – l'Unione può rivolgersi direttamente ad ogni operatore pubblico e privato, quindi anche alle piattaforme digitali.

Come abbiamo brevemente ricordato *supra*, la Commissione europea ha iniziato i lavori relativi al c.d. *AI Package* nel 2018, ed è pervenuta, dopo un lungo *iter*, alla "*Proposta di regolamento che stabilisce regole armonizzate in materia di intelligenza artificiale*", accompagnata dalla Comunicazione "*Promuovere un approccio europeo all'intelligenza artificiale*", nonché da una revisione del "*Piano coordinato sull'intelligenza artificiale*"; ma a distanza di altri tre anni non si è avuta

[62] Cfr. S. ZUBOFF, *The Age of Survellaince Capitalism. The fight for a human future at the new frontier of power*, Public Affairs, London, 2019.

[63] Sul tema v. l'autorevole contributo di L. FERRAJOLI, *Per una Costituzione della Terra*, Feltrinelli, Milano, 2022.

[64] Cfr. F. BILANCIA, S. CIVITARESE MATTEUCCI, *Il diritto pubblico nella società contemporanea*, Giappichelli, Torino, 2023, p. 8 ss.

[65] Cfr. C. SCHEPISI, *Le "dimensioni" della regolazione dell'intelligenza artificiale nella proposta di regolamento della Commissione*, cit.

ancora l'approvazione dell'*AI Act* da parte del Parlamento. Sono ancora in discussione aspetti definitori, l'elenco delle attività vietate e di quelle ad alto rischio, e le eventuali flessibilità (*regulatory sandbox*). Questi tempi, in una materia che si evolve ad una velocità straordinaria, rappresentano oggettivamente un ritardo preoccupante. Il documento pone inoltre le decisioni finali in materia, nelle mani dei Parlamenti nazionali, che sono esortati a prendere decisioni coordinate, ma senza che alcun organo specifico guidi il processo ordinatamente verso obiettivi comuni.

L'obbiettivo di una regolazione europea dell'IA non è solo quello di non frammentare il mercato. Nella relazione di accompagnamento della proposta, si afferma infatti che l'interesse dell'Unione Europea è da un lato quello di "preservare la leadership tecnologica dell'UE e assicurare che i cittadini europei possano beneficiare di nuove tecnologie sviluppate e operanti in conformità ai valori, ai diritti fondamentali e ai principi dell'Unione", dall'altro è di basarsi "sui valori e sui diritti fondamentali dell'UE" e "dare alle persone e agli altri utenti la fiducia per adottare le soluzioni basate sull'IA, incoraggiando al contempo le imprese a svilupparle"[66].

Se l'Europa vuole diventare un *player* competitivo, oltre che credibile ed indipendente sul piano geopolitico, deve essere politicamente coesa, e deve recuperare il ritardo accumulato nei confronti di Stati Uniti e Asia. A questo punto potrebbe rivendicare, nell'attuale scenario internazionale, il proprio modello "etico" di intelligenza artificiale.

Nel c.d. "*Piano coordinato europeo*" tutti gli Stati membri sono stati invitati a sviluppare le loro strategie nazionali per l'IA, delineando i livelli di investimento e le misure di attuazione. L'Italia ha provveduto in tal senso istituendo presso il Ministero dello Sviluppo Economico un gruppo di 30 esperti che tra gennaio e giugno 2019 ha elaborato un documento di proposte per una strategia italiana per l'intelligenza artificiale. Il Libro bianco "*L'intelligenza artificiale al servizio del cittadino",* che si pone in linea con gli atti europei analizzati in precedenza, individua nove sfide: etica, tecnologia, competenze, ruolo dei dati, contesto legale,

[66] La finalità di tutelare i diritti fondamentali non mette in discussione la base giuridica dell'art. 114 TFUE, peraltro arricchita dal riferimento all'art. 16 TFUE, che consente alle istituzioni di adottare atti a tutela dei dati personali. L'obiettivo primario resta necessariamente il mercato interno, in quanto l'art. 2 TFUE non legittima l'adozione di atti da parte delle istituzioni, mentre l'art. 19 TFUE oltre ad avere un profilo limitato al principio di non discriminazione, non costituirebbe un'idonea base giuridica in ragione della procedura legislativa speciale prevista nella stessa norma. V. sul punto A. ADINOLFI, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: brevi considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *La rivoluzione dell'intelligenza artificiale: profili giuridici*, Il Mulino, Bologna, 2022.

accompagnare la trasformazione, prevenire le disuguaglianze, misurare l'impatto, l'Essere umano. Nelle "*Proposte per una strategia italiana per l'intelligenza artificiale*" si usa l'evocativa espressione *RenAIssance,* che dovrebbe basarsi su tre pilastri – umanesimo, affidabilità e sostenibilità – e su tre fattori abilitanti: dati e loro economia, infrastrutture, altre tecnologie.

Con 27 miliardi di euro, l'Italia è al primo posto in Europa per entità degli investimenti nel digitale legati al PNRR[67], ma mentre la Spagna ha puntato molto sull'IA, l'Italia pochissimo, e mancando a livello europeo una visione comune, le iniziative come quella spagnola rischiano di creare asimmetrie e sottrarre cervelli ad altri paesi Ue, mentre la vera sfida sarebbe contendere i migliori scienziati, manager e imprenditori a Stati Uniti e Asia.

E' inoltre necessario accrescere la resilienza delle reti, sempre più soggette ad attacchi informatici. Con il DL 82/2021 è stata istituita l'Agenzia per la cybersicurezza nazionale (ACN) (art.5). L'Agenzia ha come finalità la promozione della cultura della sicurezza cibernetica, la consapevolezza del settore pubblico, privato e della società civile sui rischi e le minacce *cyber*. Sembra auspicabile che al suo interno sia creato al più presto un dipartimento specializzato in IA, che in modo strutturato supporti lo Stato nel monitoraggio e nella regolamentazione, coordinandosi a (e sollecitando il) livello europeo.

Più il decisore pubblico ritarda, più le regole finiranno con l'essere dettate, come è accaduto per internet, dagli stessi "attori" del mercato, ma, come abbiamo cercato di spiegare, in questo caso i rischi sono ancora più rilevanti.

Emblematico è lo scontro che si sta consumando tra Elon Musk e Bill Gates. Apparentemente sono due visioni a confronto, la prima che vuole mettere in evidenza i rischi dell'IA, la seconda che vuole esaltarne le potenzialità. Al contempo, però, sia *Meta*, *Microsoft* e *Google*, che *Twitter* (di qui la contraddizione di Elon Musk), hanno licenziato i loro *team* di etica che si stavano occupando degli aspetti controversi dell'IA. All'osservatore più avveduto non può sfuggire che esiste un oligopolio dell'intelligenza artificiale, e che gli oligopolisti sono in "guerra" tra loro. Ci sono in gioco centinaia di miliardi di investimenti, guadagni inestimabili, oltre a quei "poteri non convenzionali" che, come abbiamo visto nel precedente paragrafo, stanno modificando in modo subdolo e surrettizio

[67] L'IA rimane ancora scarsamente utilizzata dalle imprese italiane, in particolare da quelle di dimensioni più piccole. Secondo i dati ISTAT del 2021 solo il 6,2% delle imprese ha dichiarato di utilizzare sistemi di IA, contro una media dell'8% nell'UE, e la percentuale delle piccole imprese si attesta al 5,3% contro il 24,3% delle grandi imprese. Nonostante ciò, secondo Anitec-Assinform, l'associazione che in Confindustria raggruppa le aziende Ict, in Italia il mercato dell'Intelligenza Artificiale ha raggiunto nel 2022 un volume di circa 422 milioni di euro (+21,9%) e raggiungerà i 700 milioni nel 2025, con un tasso di crescita medio annuo del 22%.

gli stessi assetti giuspubblicistici, per come li abbiamo finora conosciuti. Parte della dottrina si è chiesta se la decisione politica non sia già "algoritmica"[68].

Perciò dovrebbero essere gli Stati, e comunque la dimensione pubblica, a controllare il mercato dell'IA, come dovrebbe avvenire per tutti i mercati strategici[69], e in questo caso ancora di più. Bisognerebbe imparare dall'esperienza degli ultimi 30 anni, che ci ha insegnato che il mercato non può auto-regolarsi[70]. Una visione pubblica strategica dovrebbe puntare sul rafforzamento delle competenze digitali, dalla scuola al mondo del lavoro; dovrebbe fare investimenti massicci con obiettivi di medio e lungo periodo, per sfruttare le immense potenzialità di queste tecnologie; dovrebbe impedire che il settore resti in balia della competizione tra oligopolisti, favorendo una sana concorrenza tra imprese; dovrebbe orientare la tecnologia verso un orizzonte di principi e valori, mettendola completamente al servizio delle comunità e della democrazia.

5. Ulteriori spunti di riflessione e di ricerca

Sul tema dell'IA, dovrebbe concentrarsi oggi tutto il mondo della ricerca scientifica, L'approccio deve essere multidisciplinare, con una cultura dell'intelligenza artificiale diffusa fra gli specialisti delle diverse discipline.

Interessante è, ad esempio, il lavoro realizzato dal CNR, "L'Intelligenza Artificiale per lo sviluppo sostenibile", che ci ricorda come "la cura per l'ambiente non è un movimento o un'ideologia" ma il nostro "prossimo gradino evolutivo", per usare le parole dello psicologo statunitense Daniel Goleman.

Fondamentale è altresì concentrarsi sulle disuguaglianze e sul c.d. *digital divide*. I "nuovi poveri" del futuro saranno le persone prive di competenze digitali, e i più fragili saranno coloro che non saranno in grado di gestire in modo consapevole i rischi correlati alle nuove tecnologie.

---

[68] V. sul punto A. CARDONE, *Decisione "algoritmica" vs decisione politica*?, Editoriale Scientifica, Npaoli, 2021, il quale si interroga sulle potenzialità e sui limiti dell'automazione dei procedimenti di creazione del diritto, richiamando la "democrazia deliberativa" in grado di colmare quel *lack of legitimacy per input*, nella misura in cui ridurrebbe "gli effetti depressivi che la disintermediazione politica e l'evoluzione della comunicazione politica nella realtà delle *ICT* determinano" (p. 133 e ss.). Secondo l'Autore, solo il carattere "ausiliario" della decisione algoritmica potrà condurre ad una "democrazia della responsabilità", in grado cioè di istituzionalizzare la responsabilità politica di una scelta, ancorchè assunta da algoritmi e strumenti di intelligenza artificiale.

[69] V. sul tema M. MAZZUCATO, *Lo Stato innovatore,* Laterza, Roma-Bari, 2020.

[70] Cfr. F. BILANCIA, *Indirizzo politico e nuove forme di intervento pubblico nell'economia in attuazione del Recovery and Resilience Facility, tra concorrenza e nuove politiche pubbliche*, in *Costituzionalismo.it*, 1, 2022.

Le infrastrutture digitali oggi sono messe a disposizione soprattutto da grandi aziende statunitensi, anche se vi è da dire che Francia e Germania hanno promosso un'iniziativa per sviluppare un *cloud* europeo, il GAIA-X, in cui i dati possano essere condivisi e conservati nel pieno rispetto del GDPR, con tutele maggiori rispetto a quelle garantite dalle piattaforme americane.

La chiave di volta è sempre la ricerca dell'equilibrio: se da un lato sarebbe folle pensare di fermare il progresso, dall'altro, per usare le parole di Papa Francesco, "non possiamo permettere che gli algoritmi limitino o condizionino il rispetto della dignità umana". Oppure potremmo ricordare i dialoghi tra Natalino Irti ed Emanuele Severino sul rapporto tra tecnica e diritto: il progresso della tecnica non può essere fermato, ma ciò che non può essere superata è l'immagine kantiana dell'uomo come fine di ogni ragion pratica.

Possiamo infine richiamare l'art. 16 della *Déclaration du 26 août 1789 des droits de l'homme et du citoyen* secondo cui *"Toute société dans laquelle la garantie des droits n'est pas assurée, ni la séparation des pouvoirs déterminée, n'a point de constitution"*, e chiederci come il costituzionalismo possa ancora oggi garantire gli individui, la collettività, e i delicati equilibri insiti nel patto sociale, in quella che abbiamo definito "società del rischio".

I quesiti che bisogna necessariamente porsi sono i seguenti: quanto sarà democratico lo sviluppo delle tecnologie legate all'IA? Come si può evitare che solo in pochi detengano il controllo pressoché assoluto di soluzioni capaci di cambiare il mondo, e che le concentrazioni di potere economico, mediatico, culturale e politico producano discriminazioni, limitazioni insostenibili della concorrenza, forme di manipolazione di massa, fenomeni di "neocolonialismo" e "privatizzazione" degli Stati?