

CERIDAP

RIVISTA INTERDISCIPLINARE SUL
DIRITTO DELLE
AMMINISTRAZIONI PUBBLICHE

Estratto

FASCICOLO
1 / 2026

GENNAIO - MARZO

La nuova “gold rush” dell’intelligenza artificiale: l’AI Action Plan negli Stati Uniti della seconda presidenza Trump

Elena Falletti

DOI: 10.13130/2723-9195/2026-1-87

L’“America’s AI Action Plan” stabilisce le linee strategiche e di policy dell’amministrazione americana in materia di deregulation, investimenti e sviluppo dell’intelligenza artificiale, potenziando l’azione degli operatori privati e riducendo al minimo l’intervento pubblico. L’Action Plan si distingue per l’abbandono del criterio, seppur minimo, di prudenza previsto dall’Executive Order n. 14110, emanato durante la presidenza Biden e successivamente revocato il 20 gennaio 2025, giorno dell’Inauguration Day e dell’avvio del secondo mandato presidenziale di Donald J. Trump. Il piano è stato concepito come una duplice sfida: da un lato nei confronti della Cina, individuata quale principale concorrente, e dall’altro verso l’Europa, ritenuta mera produttrice di norme e, pertanto, fonte di ostacolo. L’obiettivo dichiarato consiste nel trasformare la corsa all’intelligenza artificiale in una moderna “corsa all’oro”, rievocando il mito della ricchezza americana di fine Ottocento, in coerenza con lo slogan elettorale di Trump “Make America Great Again”.

The New “Gold Rush” of Artificial Intelligence: The AI Action Plan in the United States under Trump’s Second Presidency

The “America’s AI Action Plan” sets out the U.S. Government’s strategic and policy guidelines on deregulation, investment, and the development of artificial intelligence, strengthening the role of private-sector actors and minimising public intervention. The Action Plan stands out for abandoning the criterion of prudence, albeit minimal, provided for in Executive Order No. 14110, issued during the Biden presidency and subsequently revoked on 20 January 2025, the day of the inauguration of Donald J. Trump’s second presidential term. The Action Plan was conceived as a twofold challenge: on the one hand, against China, identified as the

leading competitor, and on the other, against Europe, considered merely a producer of regulations and, therefore, a source of obstruction. The stated goal is to transform the race for artificial intelligence into a modern “gold rush”, evoking the myth of American wealth at the end of the 19th century, in line with Trump’s election slogan “Make America Great Again”.

Sommario: 1. Introduzione.- 2. Il First Pillar: fondi e deregulation per l’innovazione AI.- 3. La protezione dei “valori americani”: il “Free Speech”.- 4. La promozione dei modelli Open-Source per l’adozione dell’AI.- 5. Il potenziamento delle competenze AI dei lavoratori americani.- 6. Next Generation Manufacturing e AI-Enabled Science.- 7. Il contrasto dei “synthetic media” nell’ordinamento giuridico statunitense.- 8. Gli elementi strategici di chiusura del First Pillar.- 9. Il Secondo Pilastro: la costruzione dell’infrastruttura.- 10. Il Third Pillar: il ruolo guida degli Stati Uniti nello sviluppo dell’AI e i rapporti internazionali.

1. Introduzione

L’America’s AI Action Plan (d’ora in poi AIAP)^[1] presenta le policy della seconda e 47^a presidenza Trump in materia di sviluppo e implementazione dell’intelligenza artificiale negli Stati Uniti. Siffatto piano illustra un ambizioso programma secondo cui «*America must have the most powerful AI systems in the world, but we must also lead the world in creative and transformative application of these systems. Achieving these goals requires the Federal government to create the conditions where private-sector-led innovation can flourish*»^[2].

Esso si inserisce in un quadro globale che progressivamente si sta formando e dove il confronto comparatistico propone visioni differenti che rispecchiano le diverse culture e mentalità giuridiche^[3]. Ad esempio, in Europa, l’Unione Europea ha introdotto l’AI Act^[4], caratterizzato da un approccio particolarmente prudente, orientato alla mitigazione dei rischi^[5]; il Regno Unito, con l’AI Opportunities Action Plan^[6], mira a bilanciare «*sustainability and security risks of AI infrastructure*». In Oriente, la Cina adotta una prospettiva fortemente autocratica e centralizzata^[7], il Giappone privilegia una logica di promozione

invece che di regolamentazione, in coerenza con i propri valori culturali^[8], la Corea del Sud, infine, ha adottato il modello di prevenzione del rischio ispirandosi all'AI Act^[9], l'India, infine, mantiene un atteggiamento attendista^[10]. In tale scenario, l'AIAP si distingue ponendosi in antitesi rispetto agli altri ordinamenti giuridici. Tale circostanza assume rilievo significativo, sotto il duplice profilo giuridico e politico, poiché le principali "AI factories" risultano essere radicate nel contesto statunitense, con conseguenti implicazioni in ordine alla definizione degli standard normativi, dei modelli regolatori e degli equilibri geopolitici connessi allo sviluppo dell'intelligenza artificiale.

A questo proposito, l'intitolazione del primo paragrafo dell'AIAP, «*Remove Red Tape and Onerous Regulation*» manifesta l'essenza di un programma di strategia politica, che intende virare da una regolamentazione prescrittiva a una politica di *laissez faire*^[11]. Infatti, ad esclusione del sistema giudiziario, l'AIAP si pone in convinta ed argomentata opposizione a ogni ipotesi o idea di disciplinare il settore AI in via preventiva e positiva seguendo l'approccio culturale del "try first"^[12]. Pertanto l'AIAP si prefigge di impostare la strategia americana ai fini del raggiungimento del dominio globale, fissando i termini della competizione, preconizzando una nuova «*new golden age of human flourishing, economic competitiveness, and national security for the American people*»^[13].

Si tratta di un obiettivo imperativo, il cui perseguimento è equiparabile alla conquista della Luna nella corsa allo spazio, con un riferimento dichiarato: «*Just like we won the space race, it is imperative that the United States and its allies win this race*»^[14], coerente con la retorica del "Make America Great Again".

Il tono del documento non è distante da quello usato nella campagna elettorale per le elezioni del novembre 2024^[15], considerando l'AI come una arena di combattimento già dal primo giorno di insediamento^[16], quando Trump firmò platealmente l'Executive Order 14179^[17] che cancellava quello precedente n. 14110 di Biden^[18].

Sembrerebbe così che la guida del treno lanciato sui binari della "Industry 4.0"^[19] sia riposta nelle mani di una tecno-élite poco interessata al benessere dei suoi passeggeri, a meno che tra costoro non si ritrovino gli azionisti o i possessori di stock options delle Big Tech company coinvolte nella costruzione di quei binari^[20]. Ne conseguirebbe che il ruolo del governo federale e delle relative agenzie deve essere minimo. Siffatta prospettiva è coerente con la strategia di

smantellamento dei fondi federali^[21] (posta in essere dal DOGE, Department of Governmental Efficiency, il cui primo esponente è stato Elon Musk^[22], figura^[23] di primo piano della oligarchia tecnologica americana^[24]).

In questo quadro, l'AIAP identifica gli specifici obiettivi potenzialmente raggiungibili con relativa facilità se il settore venisse deregolamentato: infatti, soltanto in assenza di vincoli normativi si può realizzare «*(A)n industrial revolution, an information revolution, and a renaissance – all at once*»^[25].

Al netto di siffatti toni profetici, apparentemente utili a mantenere una connessione con l'elettorato trumpiano più fondamentalista e fedele^[26] e nonostante si tratti di un documento di programmazione politica, l'AIAP presenta spunti rilevanti di riflessione giuridico-comparatistica. Esso si fonda su tre pilastri: il primo, di maggiore interesse giuridico, è dedicato agli aspetti innovativi dell'AI. Il secondo e il terzo riguardano aspetti più tecnici e politici, cioè la costruzione di una “infrastruttura americana” dedicata all'AI, nonché al mantenimento della leadership statunitense in ambito internazionale in materia di rapporti diplomatici e sicurezza.

2. Il First Pillar: fondi e deregulation per l'innovazione AI

L'eliminazione di ogni vincolo giuridico sembrerebbe essere, secondo i promotori dell'AIAP, il modo più semplice ed efficace per raggiungere siffatta accelerazione dello sviluppo dell'AI, dato che l'AI «è *troppo importante per essere soffocata in questa fase iniziale dalla burocrazia statale o Federale*»^[27]. Pertanto, il governo federale non dovrebbe permettere che i finanziamenti federali relativi all'AI vengano indirizzati verso Stati con normative così onerose che provocherebbero uno spreco di tali fondi^[28]. Anzi, addirittura il governo federale non dovrebbe nemmeno interferire con il diritto degli Stati di approvare leggi che non siano indebitamente restrittive per l'innovazione.

Parimenti, questo orientamento trova conforto con la teoria originalista che influenza gli organi di controllo giudiziario secondo cui l'interpretazione della Costituzione e della normativa federale deve essere effettuata con un rigoroso criterio letterale restrittivo facendo riferimento al significato inteso dare al testo normativo dai legislatori costituzionali^[29] (cioè i Founding Fathers) al momento della sua stesura^[30].

Le policy raccomandate dall'AIAP sono del tutto coerenti con siffatta ricostruzione e riguardano il significativo ridimensionamento, e in certi casi addirittura la cancellazione, della disciplina vigente all'inizio della seconda presidenza Trump. In realtà l'AIAP era già stato preceduto da un Executive Order diretto a ridurre al minimo l'impalcatura normativa^[31], di ridurre o cessare i finanziamenti agli Stati che ponessero limiti giuridici o responsabilità, le quali gravino indebitamente sull'innovazione AI.

A seguito di ciò, la dottrina^[32] aveva evidenziato che successivamente alla cancellazione dell'EO 14110 la strategia trumpiana in materia di AI avrebbe potuto prendere due direzioni: lasciare spazio a una regolamentazione statale decentralizzata con un minimo di sorveglianza federale, oppure centralizzare l'iniziativa a livello federale con la prevalenza legislativa. In realtà l'AIAP sembra effettuare una scelta a metà tra le due opzioni, cioè: accentuare la sorveglianza federale ai fini di evitare che i fondi federali venissero impiegati in Stati ove le disposizioni normative approvate contraddicessero il *laissez faire* governativo e ponessero limiti troppo rigorosi allo sviluppo dell'AI.

Invece, nel contesto statale, l'AIAP si è inserito in un panorama normativo già popolato e frammentato. A questo proposito, il National Conference of State Legislatures ha censito almeno 100 interventi legislativi in 36 Stati americani nel solo 2025^[33].

Ai fini di "misurare" la distanza tra la preoccupazione regolatoria dei legislatori statali e la *deregulation* federale si propone una sommaria indagine dei provvedimenti più significativi che parrebbero essere passibili del suddetto vaglio federale ai fini della stretta sui fondi federali^[34].

Per l'analisi dei diversi progetti di legge in corso di approvazione in materia di AI, sono stati scelti due temi importanti come la protezione dei consumatori^[35] e la tutela della salute. Tale scelta è orientata a verificare l'attenzione dei legislatori statali nei confronti delle parti deboli nonostante la scure ai finanziamenti federali minacciata dall'AIAP nel perseguimento della summenzionata strategia di *deregulation*.

Sotto il primo profilo si segnalano provvedimenti quali il SB 24/205^[36] (Colorado), H 516^[37] (Alabama), S 238^[38] e S 259^[39] (California), HB 95 (2025)^[40], H 518^[41] e H 140^[42] (Pennsylvania), il H 1246^[43] e il S 1363^[44] (Tennessee), il S 2966^[45] (Texas), il S 226^[46] (Utah), H 208^[47] (Vermont), H 2094^[48], H 2250^[49], H 2411^[50]

(Virginia), D 149^[51] (Wyoming).

Parimenti, le previsioni dell'AIAP si sovrappongono alle iniziative limitative dell'AI in materia di medica e diagnostica quali il «*Wellness and Oversight for Psychological Resources Act*» (Illinois) promulgato dal Governatore il 4 agosto 2025 che interdice l'uso degli strumenti di intelligenza artificiale per effettuare diagnosi mediche e elaborare terapie sanitarie. Si tratta di una normativa rilevante, in considerazione dell'ampio uso dell'AI e in particolare dei software predittivi in ambito diagnostico^[52]. Per sottolineare quanto importante (economicamente e giuridicamente) è il tema si citano, seppur sommariamente, i progetti legislativi che intendono disciplinare la materia a favore della cura dei pazienti e che verrebbero ostacolati dall'approccio dell'AIAP, quali il H 2175^[53] (Arizona), H 1816^[54] (Arkansas), S 10^[55] (Connecticut), S 2259^[56] (Illinois), H 2313^[57] (Kansas), LR 1768^[58] (Maine), A 290^[59], A. 295^[60], S 128^[61], S186^[62], S 398^[63] (Nevada), A 6545^[64] (New York), S 287^[65] (North Carolina), S 611^[66] (Oklahoma), H 3229^[67] (Oregon), il H 452^[68] (Utah).

Alla luce di tale sommaria ricognizione delle normative statali, appare legittimo domandarsi se sia fondata l'obiezione proveniente specie da voci tanto intra^[69] quanto extra UE^[70] su una presunta “over regulation” in materia di intelligenza artificiale – particolarmente veemente in riferimento all'AI Act europeo, ma non disinteressata alla critica, in particolare, del GDPR, del DMA e DSA e del Data Act^[71].

Ci si può chiedere se siffatte critiche non rappresentino in realtà più uno stereotipo che un effettivo ostacolo allo sviluppo tecnologico. Infatti, negli Stati Uniti, la crescita delle Big Tech Company è avvenuta nonostante un quadro regolatorio frammentato, ma non del tutto assente, mentre i successivi interventi federali, come l'AIAP, di matrice trumpiana, hanno assunto piuttosto la forma di misure di deregolamentazione *ex post*, in favore della deresponsabilizzazione delle grandi compagnie tecnologiche.

Ulteriormente, merita una riflessione l'incidenza della differente cultura giuridica tra common law e civil law nella regolazione dell'innovazione tecnologica. In particolare, un'impostazione maggiormente deregolamentata può risultare coerente con la tradizione di common law, la quale, a differenza dei sistemi di civil law, postula che la valutazione giudiziaria, fondata sul precedente vincolante, possa intervenire solo successivamente all'introduzione di nuove tecnologie.

Nei sistemi di civil law, al contrario, l'emergere di innovazioni tecnologiche richiede, in via preventiva, l'adozione di una regolamentazione normativa specifica. In ogni caso, lo sviluppo dell'intelligenza artificiale ha ormai superato una fase embrionale, tanto da rendere concreto il rischio di pregiudizi già occorsi a soggetti coinvolti, i quali necessitano di un'adeguata tutela sia normativa sia giurisdizionale, a garanzia della protezione dei loro diritti fondamentali e della responsabilità civile e amministrativa degli operatori.

Le proposte di legge (bill) depositati presso i parlamenti degli Stati dimostrano che a livello locale, cioè statale, sussiste un diffuso interesse politico a disciplinare, ovvero moderare, gli effetti discriminatori o nocivi dell'applicazione delle procedure automatizzate in ambito della tutela dei consumatori e della salute. Ci si può chiedere se questa strategia regolatoria, stigmatizzata dall'AIAP, possa influenzare il fundraising ovvero lo sviluppo dell'innovazione tecnologica^[72], come sostengono molti critici dell'AI Act europeo^[73].

Secondo certuni^[74], la regolamentazione che intervenga *ex ante* sull'implementazione dell'AI nei processi produttivi provoca una diminuzione sulla probabilità di ottenere finanziamenti, soprattutto a favore delle start up^[75], dato che tale regolamentazione potrebbe aumentare i rischi percepiti o i costi di conformità per gli investitori. Si tratta di un costo sull'accesso al capitale di finanziamento, ma non impatta altrettanto sulla fiducia che gli investitori nelle aziende che riescono ad adeguarsi al contesto normativo.

Inoltre, andrebbe vagliato l'effetto distorsivo provocato dalla diffusione delle proposte normative in materia di AI, dato che vi è un periodo di tempo intercorrente tra il deposito della proposta e l'approvazione legislativa della medesima in cui le pressioni esercitate dalle lobby possono riuscire nell'intento di indebolire le previsioni originarie^[76].

In tale prospettiva, assume particolare significato il fatto che l'AIAP formalizzi un comportamento già riscontrabile nella prassi, consistente nella possibile relazione tra un attenuato livello di controllo normativo e una più marcata capacità di acquisizione di finanziamenti.

Ci si potrebbe invece chiedere se l'aspetto di maggiore influenza sia la capacità di raccogliere capitali finanziari. Ciò sembra essere plausibile se si considera che in Cina, ordinamento di riferimento di altre grandi Big Tech Company come TikTok, Temu e Alipay, la regolamentazione e la direzione pubblica sono ancora

più penetranti che nell'Unione Europea. Tuttavia il governo cinese considera interesse nazionale la creazione e lo sviluppo di compagnie tecnologiche che siano in grado di dominare i mercati stranieri, oltre a essere di fatto monopoliste nel mercato interno dei rispettivi settori^[77].

Sotto questo profilo, l'AIAP predispone una sorta di zona franca, una forma di *deregulation* a favore delle Big Tech già esistenti sul mercato sia sotto il profilo di accesso ai finanziamenti pubblici federali, sia sotto il profilo normativo, cancellando di fatto il concetto di responsabilità, in particolare quelle legate alla produzione di beni destinati all'uso dei consumatori.

Essa si realizza attraverso delle azioni di policy raccomandate, cioè l'Office of Science and Technology Policy (OSTP) deve lanciare una indagine (Request for Information)^[78] nei confronti delle imprese e il pubblico in generale sulla normativa federale che ostacoli l'innovazione AI e adottare politiche deregolative al riguardo. In coerenza con l'Executive Order 14192^[79], l'Office of Management and Budget (OMB) insieme alle agenzie federali deve identificare, revisionare o cancellare regole, norme, memoranda, ordini amministrativi, linee guida, policy statement e accordi tra agenzie che ostacolano “*unnecessarily*” lo sviluppo dell'AI o il suo impiego.

Parimenti, il medesimo OMB e le Agenzie federali, che abbiano una discrezionalità ed autonomia nell'erogare i finanziamenti agli Stati, limitino siffatti finanziamenti se lo Stato richiedente abbia adottato normative che possano ostacolare l'effettivo impiego di tali fondi o premi. Tale valutazione è guidata dalla Federal Communications Commission (FCC), la quale decide se le normative statali sull'AI interferiscano con la capacità della FCC stessa di portare a termine i suoi obblighi ai sensi del Communications Act 1934^[80], mentre alla Federal Trade Commission è devoluto il compito di verificare tutte le indagini iniziate sotto le precedenti amministrazioni al fine di assicurare che non vengano perorate teorie sulla responsabilità. Pari indagine deve essere effettuata per gli ordini, i decreti e le ingiunzioni e dove appropriato modificare quelle che, secondo i redattori del AIAP sono «*unduly burden AI innovation*»^[81].

La spinta verso la *deregulation* promossa dall'AIAP solleva importanti interrogativi. Innanzitutto, perché rinunciare preventivamente a un sistema di garanzie dei consumatori e degli utenti? Seppure nel sistema di common law sia considerato accettabile un modello di sviluppo di “frontiera” che preveda la

regolamentazione *ex post*, a seguito della soluzione dei conflitti tra gli attori del sistema (imprese, consumatori, utenti, enti di ricerca, anche lo stesso Stato) attraverso la giurisprudenza o l'espletamento di azioni collettive dai risvolti risarcitori dirompenti^[82].

Siffatto approccio sembra rievocare la conquista del West, celebrata dalla cinematografia ed esplicitamente richiamata nel documento in esame. Oggi, tuttavia, esso appare di difficile sostenibilità, soprattutto alla luce dell'incidenza gravosa che le infrastrutture digitali esercitano su beni comuni essenziali per la vita umana, quali l'acqua e l'energia. Autorevole dottrina ha affermato che la tecnologia non può vivere di sola autoregolazione, giacché «*l'assenza di norme non elimina i rischi, ma li sposta interamente sulla collettività*»^[83].

3. La protezione dei “valori americani”: il “Free Speech”

Un punto di significativa importanza culturale e giuridica dell'AIAP riguarda il ruolo che i sistemi di AI svolgeranno nell'educazione dei “nostri figli” (children), nello svolgimento del “nostro lavoro” e nel consumo dei “media”.

È un argomento che provoca tensioni e fraintendimenti tra Stati Uniti e Europa perché presenta un confronto valoriale basato su presupposti differenti. La visione “originalista”^[84] statunitense si radica su una visione individualista, legata alla massima esclusione possibile dello Stato nella vita del cittadino soprattutto in relazione al suo spazio autodeterminativo su ciò che pensa e come lo esprime, fondato su una visione del diritto di libertà attinente a Locke, secondo cui i diritti naturali riconosciuti dallo Stato riguardano solo la vita, la libertà e la proprietà^[85].

Nella frase introduttiva di questa breve, ma importante, sezione dell'AIAP, concepita come l'espressione di una visione originalista radicale, vengono impiegati termini e toni estranei al linguaggio tecnico-giuridico o tecnologico, ma riconducibili alla dimensione quotidiana dell'esperienza comune, quali, ad esempio, “children”, “job”, “media”, “consume”. A tal proposito, l'AIAP adotta una strategia di carattere bifronte, volta a differenziare, in base alla relativa fonte, i contenuti ritenuti ammissibili ai fini dell'utilizzo e della divulgazione. Da un lato, viene rimarcato un approccio di *laissez faire* nei confronti dei valori culturali ereditati dalla tradizione, riconducibili a una visione religiosa di matrice cristiano-conservatrice; dall'altro, si registra una marcata censura verso il riconoscimento di

posizioni più aperte ma antitetiche alle precedenti, quali il multiculturalismo, le istanze LGBTIQ+, le rivendicazioni egalarie e, più in generale, le prospettive orientate all'accettazione della diversità, dell'uguaglianza e dell'inclusione, qualificate come *woke* e considerate contrarie alla "verità".

Pertanto, è essenziale che i sistemi di intelligenza artificiale siano costruiti e sviluppati seguendo il principio relativo al freedom of speech and expression e che le policy del governo federale americano non interferiscano con questo obiettivo. «*We must ensure*»^[86] che il freedom of speech fiorisca nell'era dell'AI e che l'AI fornita dal Governo federale oggettivamente rifletta la verità invece che agende di ingegneria sociale.

Questa frase rispecchia pienamente la politica trumpiana di retroguardia in relazione allo smantellamento effettuato delle politiche di promozione della (D)iversità, (E)quality (nel senso di uguaglianza) e (I)nclusione effettuata con una serie di executive order presidenziali^[87], anche questi a partire dal primo giorno dell'insediamento della seconda presidenza Trump^[88]. La linea di azione sembra orientata non alla completa apertura dello spazio informativo, ma a una chiusura selettiva verso ciò che non è completamente aderente alla dottrina "MAGA"^[89] (Acronimo di «*Make America Great Again*»)^[90].

L'AIAP incarica il Department of Commerce (DOC), con la cooperazione del National Institute of Standards and Technology (NIST), di revisionare il NIST AI Risk Management Framework^[91], le cui previsioni sono state emanate nel 2023, al fine di eliminare i riferimenti a ciò che è considerato inaccettabile secondo l'ideologia MAGA, cioè: «*misinformation, (D)iversity, (E)quity and (I)nclusion, and climate change*»^[92]. Parimenti devono essere aggiornate le "procurement guidelines" su forniture e contratti pubblici per assicurare che il governo possa stipulare contratti con sviluppatori di Large Language Model (LLM) di frontiera che assicurino che i loro sistemi siano oggettivi e liberi da «*top-down ideological bias*».

La questione in esame tocca un punto cruciale. Sebbene la policy si presenti come strumento volto alla tutela della verità, essa realizza, in concreto, due effetti: da un lato, introduce una strategia di carattere censorio; dall'altro, produce una distorsione della realtà. Ne consegue che l'attività di fact checking diventa irrilevante sia perché, in nome della libertà di pensiero intesa in modo strumentale, viene attribuito lo status di verità a ciò che veritiero non è; sia perché

la viralità^[93] della disinformazione^[94] rende nei fatti impossibile l'attività di controllo delle fonti^[95], con il pesante rischio dell'avvelenamento dei pozzi informativi^[96].

Ciò nonostante, il Freedom of Speech, garantito dal Primo Emendamento della Costituzione statunitense, costituisce il fondamento della libertà di parola, e sul punto l'AIAP si richiama a un'interpretazione rigorosamente originalista. Resta tuttavia da chiarire quale significato venga attribuito ai concetti di "verità", "oggettività" e "libertà". Un'interpretazione imposta dall'alto e orientata ideologicamente comporta, infatti, un rovesciamento semantico di tali nozioni^[97]. A questo proposito, non dovrebbe essere ignorata la domanda effettuata da Pilato all'imputato del processo più noto della storia del cristianesimo e cioè: «*Quid est veritas?*» (Giovanni 18,38). Ora, come allora, siffatta cruciale domanda rimane senza risposta, tanto più che entrambe le summenzionate questioni concernono la commistione tra politica e religione^[98].

In aggiunta a quanto sopra, si osserva che viene applicata un'imposizione "dall'alto" di parametri interpretativi nell'impiego della cosiddetta generative AI (GenAI)^[99], e in particolare nei modelli linguistici di grandi dimensioni (LLM)^[100], basati su un processo di apprendimento automatico (machine learning).

Come è noto, tali strumenti producono le risposte richieste dai "prompt"^[101] degli utenti mediante machine learning, il quale determina la risposta attraverso un'elaborazione statistica ponderata, basata sulla probabilità che una determinata parola segua un'altra all'interno di un testo. Nonostante i dati inseriti nel database del programma di intelligenza artificiale generativa possano essere i più accurati e appropriati possibile, detta modalità di elaborazione può dar luogo a fenomeni comunemente definiti "allucinazioni" ("*hallucinations*")^[102], ossia errori derivanti dalla natura stessa del calcolo automatizzato, effettuato su vaste quantità di dati, secondo una logica che tende a conferire ai software una percezione antropomorfa delle capacità cognitive.

Tuttavia, tale scelta semantica scaturisce forti dubbi, perché se da un lato l'allucinazione è provocata da uno stato mentale alterato curabile in particolare con certe terapie farmacologiche, il programma che ha elaborato la risposta "allucinata" non solo non conosce alcun stato mentale alterato e neppure è in grado di essere sottoposto ad una cura all'uopo: anche da questa circostanza si

può dedurre quanto sia foriera di errori, equivoci e incomprensioni la tendenza a “umanizzare” i software di elaborazione linguistica a generazione di contenuti errati, o comunque non rispondenti al vero, che costituisce invece un tratto strutturale del loro funzionamento.

Vi è un ulteriore aspetto da considerare, ovvero ci si potrebbe domandare se i risultati prodotti dagli LLMs debbano rientrare nella tutela della libertà di espressione. In tal caso, occorrerebbe identificare il soggetto destinatario della protezione: l'autore del prompt, la macchina stessa o l'ente proprietario del modello?

Si tratta di questioni di rilevante portata, sulle quali la fonte di policy in esame lascia piena discrezionalità alle Corti, rimarcando paradossalmente l'avversione per regole precise e confidando di avere la Corte federale di vertice, cioè la Corte Suprema, dalla propria parte^[103].

Non sembra, peraltro, ammissibile negare questo dato fattuale, che sembrerebbe spingersi fino a tentare di modificare il significato stesso del concetto di “verità” (truth) sulla base della provenienza politica delle asserzioni che la riguardano. Infatti, l'AIAP stabilisce che l'intelligenza artificiale di frontiera debba tutelare la libertà di espressione e i cosiddetti “valori americani”. Tuttavia, detta impostazione, caratterizzata da un approccio di matrice millenaristica e più prossima alla fantascienza che alla scienza, distoglie l'attenzione dall'analisi di ciò che effettivamente l'intelligenza artificiale compie, concentrandosi invece su ciò che ci si immagina essa possa essere o sia in grado di fare.

La questione è rilevante poiché gli LLMs si pongono come intermediari tra l'utente e le fonti originarie, generando risultati che l'utente tende ad assumere come veritieri e affidabili, rinunciando a ogni verifica critica e delegando integralmente l'analisi delle informazioni alla black box, pertanto è bene ribadire che i sistemi di GenAI, compresi gli LLMs, non sono “pensatori profondi”, bensì modelli statistici addestrati su enormi quantità di testi. Tale addestramento consente loro di riprodurre la regolarità del linguaggio, ma senza alcun accesso diretto alla realtà. In questo contesto, le parole non veicolano ragionamenti causali, ma rappresentano vettori in spazi multidimensionali, la cui combinazione deriva da una distribuzione di probabilità^[104].

Conseguentemente, i contenuti generati non sono frutto di logica argomentativa, bensì di un campionamento statistico. La mancanza di regolamentazione di tali

processi si rivela quindi altamente rischiosa, poiché anche in presenza di dati “puliti” da bias o da elementi discriminatori, i modelli possono produrre frasi false, ma plausibili. L’accuratezza non costituisce infatti un obiettivo progettuale, bensì un effetto collaterale, dipendente dalla quantità di dati di addestramento. La maggiore potenza computazionale accresce la precisione del dettaglio, ma non la veridicità dei risultati^[105].

In siffatto contesto, l’AIAP sembra promuovere la libertà di espressione, ma “a corrente alternata”, a seconda se i contenuti e i valori espressi non assecondino i già menzionati “progetti di ingegneria sociale”. Ne deriva un’impostazione che si pone in antitesi con la lotta alle discriminazioni, lasciando intravedere un ritorno a logiche discriminatorie, incentrate sull’esclusione di tutte le persone che non rispondano ai canoni ritenuti culturalmente “tradizionali”, a partire dall’eteronormatività eurocaucasica^[106].

Le raccomandazioni di policy suggerite appaiono pertanto emblematiche: a) sotto la guida del Dipartimento del Commercio (DOC) e attraverso il National Institute of Standards and Technology (NIST), si propone di rivedere il NIST AI Risk Management Framework per eliminare ogni riferimento a disinformazione, diversità, equità, inclusione e cambiamento climatico; b) aggiornare le linee guida sugli appalti federali, prevedendo che il governo contratti esclusivamente con sviluppatori di LLM “di frontiera” in grado di garantire sistemi dichiaratamente oggettivi e privi di pregiudizi ideologici di matrice politica o culturale^[107].

Resta infine il profilo geopolitico: la parte conclusiva del documento AIAP affronta, l’“elefante nella stanza”, cioè il tema del rapporto tra Stati Uniti e la Cina nello sviluppo dell’intelligenza artificiale. Si prevede, infatti, che il Department of Commerce (DPC), tramite il NIST’s Center for AI Standards and Innovation (CAISI), conduca ricerche e, ove opportuno, pubblici valutazioni sui modelli cinesi, con particolare riguardo alle politiche censorie adottate dal Partito Comunista.

4. La promozione dei modelli Open-Source per l’adozione dell’AI

Uno degli spunti più interessanti dell’AIAP sembrerebbe provenire dal background di startupper tecnologici degli autori e riguarda l’invito a utilizzare e

promuovere i modelli di open-source AI^[108] e open-weight AI^[109]. Siffatti modelli, data la loro apertura all'utilizzo e alla modifica consentono ai prodotti soggetti a questo tipo di licenza di essere distribuiti in una modalità più flessibile rispetto a quelli collegati alla proprietà intellettuale tradizionale a (teorico) vantaggio degli sviluppatori che, ovunque nel mondo, possano scaricarli e modificarli.

In realtà, l'AI open-source può rivestire un ruolo significativo per superare la mancanza di interoperabilità e accesso promuovendo l'innovazione con l'abbassamento delle barriere all'ingresso, in particolare per gli operatori più piccoli e con minori risorse^[110]. Infatti, gli sviluppatori possono creare modelli e applicazioni di AI personalizzate senza dover approvvigionarsi di ingenti capitali per investimenti nella potenza di calcolo, supporto energetico. Ulteriormente, l'open-source sostiene anche la ricerca nell'interesse pubblico sulla sicurezza e l'affidabilità dell'IA, garantendo ai ricercatori l'accesso ai modelli di base o ai loro dati di addestramento, al fine di effettuare valutazioni sui pregiudizi dannosi.

Ciò nonostante, questo approccio presenta alcune importanti criticità quali, ad esempio il fatto che non è chiaro cosa si intenda per "open-source"^[111] nel contesto dell'AI^[112] e in siffatto contesto può accadere che le aziende tecnologiche dominanti offrano modelli che sembrano open-source, in grado di mascherare la loro natura proprietaria. Quale esempio significativo potrebbe essere indicata la strategia di Meta^[113], che ha tentato di differenziarsi rilasciando i propri modelli AI, come Llama2, su licenze dichiarate come open-source^[114], nonostante la comunità abbia espresso il proprio scetticismo sull'aderenza di tale iniziativa ai modelli formali di open-source^[115].

Questo accesso, apparentemente aperto, è in realtà vincolato a tutta una serie di condizioni, tra cui restrizioni d'uso, in particolare per ciò che concerne l'utilizzo di Llama e dei suoi derivati per il miglioramento di altri LLMs^[116] ovvero «*se alla data di rilascio della versione Llama 2, gli utenti attivi mensili dei prodotti o servizi resi disponibili dal Licenziatario o per conto dello stesso, o dalle affiliate del Licenziatario, sono superiori a 700 milioni di utenti attivi mensili nel mese solare precedente, è necessario richiedere una licenza a Meta, che Meta potrà concedere a sua esclusiva discrezione, e non si è autorizzati ad esercitare alcuno dei diritti previsti dal (...) Contratto a meno che o fino a quando Meta non conceda espressamente tali diritti*»^[117].

In dottrina si evidenzia la possibilità che le Big Tech Company possano utilizzare

siffatte clausole restrittive al fine di soffocare^[118] i potenziali concorrenti che emergono sulla scia della sua tecnologia e pertanto vadano evitate strategie dirette esclusivamente all' "openwashing" garantendo che i modelli open-source siano effettivamente tali^[119].

Inoltre, ciò che attrae l'attenzione degli studiosi riguarda il fatto che il modello promosso dall'AIAP trae linfa dal principio del "try first", il quale solleva specifiche preoccupazioni in determinati ambiti, come quello sanitario. In particolare, desta attenzione il rischio che i nuovi prodotti non riflettano adeguatamente la diversità delle popolazioni di pazienti cui sono destinati, nonché la possibilità che una valutazione preliminare limitata possa compromettere la fiducia di medici e pazienti nei confronti dei prodotti innovativi di intelligenza artificiale.^[120]

Tale impostazione si pone in aperto contrasto con il modello europeo delineato dall'AI Act, che si basa, invece, sulla valutazione preventiva dei rischi. In questa divergenza si rinvengono i principali elementi critici evidenziati dall'approccio europeo, soprattutto nei settori maggiormente esposti a effetti discriminatori derivanti dall'uso dell'intelligenza artificiale, come appunto quello sanitario^[121].

Secondo l'AIAP, il principale ostacolo allo sviluppo dell'AI non sarebbe costituito dalla mancanza di modelli, strumenti o applicazioni, bensì dai presunti limiti nell'adozione della tecnologia, soprattutto da parte delle organizzazioni consolidate. Pertanto, sono i settori strategici che soffrono i ritardi più gravi nell'implementazione dei servizi negli Stati Uniti, come la sanità.

Siffatte criticità sono imputate a molteplici fattori: non solo di diffidenza o scarsa conoscenza della tecnologia, ma sembrerebbero essere riconducibili alla complessità del quadro normativo e alla carenza di standard chiari in materia di governance e mitigazione del rischio. Sul punto si potrebbe suggerire degli interventi soft nella gestione di tale trasformazione, quali «*soft components (institutional culture, inter-cultural awareness, and organizational needs) to facilitate the mental shift and thus the buy-in*»^[122]. Ciò nonostante, a giudizio dell'AIAP, un intervento coordinato a livello federale potrebbe favorire la diffusione di una cultura dinamica e sperimentale dell'IA nell'industria americana.

Tuttavia, le indagini della dottrina sembrerebbero invece dimostrare che i limiti sopra considerati, in particolare nel settore sanitario, riguardino la gestione degli

aggiornamenti legislativi, il trattamento dei dati, privacy, cybersecurity, l'opacità delle black box, le questioni etiche, i risultati discriminatori ovvero influenzati da bias^[123]. L'emersione di siffatti problemi confermano le perplessità suscitate dall'applicazione del summenzionato principio "try first" dal punto di vista della tutela dei diritti fondamentali^[124].

Si evidenzia, inoltre, una contraddizione di fondo: o esiste un quadro normativo complesso, o vi è assenza di standard di governance e mitigazione del rischio. La tesi proposta dall'AIAP appare, pertanto, funzionale a giustificare la promozione di una sostanziale deregolamentazione. Il modello del "try first" si pone in netta antitesi con il principio stesso di mitigazione del rischio e persino gli strumenti di sperimentazione normativa^[125] (regulatory sandbox) presuppongono l'esistenza di un quadro regolatorio unitario e omogeneo, nel quale le sperimentazioni vengano effettuate a parità di condizioni.

Ciò nonostante parrebbe sussistere uno spazio comune, probabilmente di convergenza, tra il modello europeo e quello statunitense, ovvero nella promozione di sperimentazioni controllate, sia in ambienti virtuali sia in contesti reali, come dimostra l'approccio comparato relativo alla realizzazione di tali sandbox^[126] in ambienti virtuali^[127] (disciplinate dagli artt. 57 e ss. Reg. 1689/2024) oppure nel contesto reale^[128], per esempio attuato per la sperimentazione dei taxi a guida autonoma Waymo^[129] negli Stati Uniti^[130], in particolare in Texas, Arizona e California^[131]. Tuttavia, in quest'ultimo caso, siffatte prassi sperimentali hanno prodotto una frammentazione delle competenze normative e, sebbene diano l'impressione di coinvolgere utenti e cittadini, in realtà tendono a marginalizzarne o silenziarne le istanze. Si tratta, forse, di una forma di "democrazia apparente"?

5. Il potenziamento delle competenze AI dei lavoratori americani

L'intento dell'Amministrazione Trump, da realizzarsi attraverso le policy previste dall'AIAP sembrerebbe essere la promozione di un programma che ponga "al centro" i lavoratori, migliorando le loro competenze nell'AI e quindi la loro produttività e la creazione di nuovi settori^[132]. Sebbene l'evoluzione tecnologica costituisca storicamente un passaggio evolutivo e la rappresentazione dell'AI

nell'immaginario collettivo attraverso film e opere letterarie^[133] abbia prodotto più equivoci che stimoli^[134], nel documento che si commenta, essa viene investita di un mandato migliorativo per l'innovazione e la creazione di nuove opportunità.

In passato, la dottrina aveva già affrontato il tema dell'automazione del lavoro intellettuale^[135].

In linea di principio, come già comprovato dall'esperienza delle delocalizzazioni delle produzioni manifatturiere^[136], non può ritenersi fondata la tesi secondo cui l'automazione sia destinata a sostituire esclusivamente le professioni caratterizzate da mansioni ripetitive e da un basso livello di qualificazione. Al contrario, e paradossalmente, le mansioni maggiormente esposte a processi di riduzione dei costi sono spesso quelle che rappresentano un onere più elevato per l'impresa in quanto potenzialmente creative o più qualificate. Inoltre, non è affatto certo che la sostituzione di figure professionali considerate obsolete o deboli rispetto all'inarrestabile avanzata dell'automazione delle professioni intellettuali, comporti la creazione di nuovi impieghi negli stessi contesti ovvero luoghi produttivi. È possibile, invece, che tali opportunità si sviluppino in aree geografiche differenti.

Tuttavia, secondo l'AIAP, tale automazione può costituire strumento a vantaggio dell'economia americana, poiché l'AI trasformerà modalità e contenuti delle prestazioni lavorative in ogni settore, imponendo una risposta adeguata per governare la transizione, in particolare per ciò che concerne la prestazione di servizi ripetitivi. In tale direzione, l'Amministrazione Trump ha adottato gli Executive Order n. 14277^[137] e n. 14278^[138] dell'aprile 2025, rispettivamente «*Promuovere l'istruzione sull'intelligenza artificiale per i giovani americani*» e «*Preparare gli americani a lavori qualificati e ben retribuiti del futuro*». La strategia prevede azioni prioritarie: ampliamento della conoscenza e delle competenze in AI, monitoraggio dell'impatto sul mercato del lavoro e sperimentazione di innovazioni volte alla rapida riqualificazione professionale.

Le azioni politiche raccomandate pongono al centro lo sviluppo delle competenze in materia di Intelligenza Artificiale quale obiettivo strategico. Sotto la guida del Department of Labor (DOL), del Department of Education (DED), della National Science Foundation (NSF) e del Department of Commerce (DOC), i flussi di finanziamento federali per istruzione e forza lavoro dovranno

prioritariamente sostenere programmi che integrino lo skill development in AI, includendo Career and Technical Education (CTE), workforce training, apprenticeship e altre iniziative federali. Con il coordinamento del Department of Treasury, dovranno essere emanate linee guida che chiariscano come i programmi di AI literacy e skill development possano rientrare nell'assistenza educativa ammissibile ex Section 132 Internal Revenue Code, consentendo ai datori di lavoro rimborsi tax-free per la formazione, favorendo l'investimento privato e la tutela occupazionale.

Parallelamente, il Bureau of Labor Statistics (BLS), il Census Bureau e il Bureau of Economic Analysis (BEA), sotto il DOC, dovranno studiare l'impatto dell'AI sul mercato del lavoro, tramite dati già raccolti (es. Business Trends and Outlook Survey), producendo analisi su adozione, creazione/sostituzione di posti di lavoro ed effetti salariali. Infine, dovrà essere istituito, sotto il DOL, l'AI Workforce Research Hub, quale centro federale permanente per la valutazione degli impatti occupazionali e socio-economici dell'AI, in collaborazione con BLS e DOC attraverso il Census Bureau e il BEA.

L'AI Workforce Research Hub, sotto la guida del DOL, produrrebbe analisi ricorrenti, scenari previsionali e approfondimenti attuabili per orientare le politiche educative e occupazionali. Il DOL potrà impiegare fondi discrezionali per finanziare la rapida riqualificazione dei lavoratori colpiti dalla perdita del posto a causa dell'adozione di AI, emanando linee guida per individuare i disoccupati ammissibili nei settori in trasformazione e per chiarire l'uso dei fondi statali di risposta rapida nella prevenzione del rischio occupazionale. Congiuntamente al DOC, dovranno essere sperimentati nuovi approcci alle sfide della workforce AI-driven, includendo progetti pilota su riqualificazione rapida, mutamento dei requisiti di competenza e adattamento dei ruoli entry-level. Tali sperimentazioni, attuabili dagli Stati e dagli intermediari della forza lavoro tramite le autorità previste dal Workforce Innovation and Opportunity Act e dal Public Works and Economic Development Act, dovranno individuare strategie scalabili e misurabili per adeguare il sistema ai rapidi mutamenti del mercato del lavoro.

6. Next Generation Manufacturing e AI-Enabled Science

Osservano i redattori dell'AIAP che l'automazione supportata dall'intelligenza

artificiale^[139] apre la strada a un'ampia gamma di innovazioni nel mondo fisico tanto in ambiti d'uso pacifico ovvero duale^[140] (cioè anche bellico). Esempi della diffusione di tali tecnologie ad uso pacifico possono riguardare la domotica, cioè l'applicazione di strumenti robotici nell'ambito domestico^[141], oppure la robotica applicata alle tecnologie ospedaliere, in particolare per la domiciliazione delle cure^[142]. Siffatti strumenti possono intervenire in diverse fasi della cura del paziente, per esempio essere utilizzati durante un intervento chirurgico oppure nella cura degli anziani^[143] o dei malati cronici. In entrambi questi esempi le questioni giuridiche paiono focalizzarsi in particolare sulla tutela della privacy ovvero sulla responsabilità del produttore per prodotto difettoso. Nel caso dell'uso di strumenti automatizzati in ambito medico potrebbero emergere questioni di responsabilità professionale del medico curante che li utilizzi, qualora la sua valutazione professionale si adagi esclusivamente sull'operato dello strumento, sia per possibili elementi discriminatori presenti nel data base del prodotto.

Come già discusso in precedenza^[144], la visione dell'AIAP è orientata verso una *deregulation* della normativa a vantaggio del principio del "try fist". Ciò comporterebbe la limitazione della protezione dei pazienti/utilizzatori di siffatte tecnologie, con la conseguente *deminutio* della tutela di salute e integrità fisica poiché. I profili etici e giuridici derivanti dall'impiego di queste tecnologie devono essere attentamente considerati, soprattutto quando le medesime incidono direttamente sulle funzioni vitali o cognitive dell'individuo, in particolare nei casi in cui gli aggiornamenti tecnologici indispensabili vengano interrotti o divengano eccessivamente onerosi, rendendo ingiustificata la prosecuzione dell'implementazione.

Altri prodotti robotici possono presentare differenti criticità, in particolare etiche^[145], per quel che concerne il loro utilizzo bellico, come accade per l'uso militare di droni ovvero di veicoli a guida autonoma^[146]. Tale distinzione è presente nell'AIAP: essa è rilevante per quel che concerne la responsabilità nell'uso in un'ottica più di accountability che di liability tanto dei produttori quanto degli utilizzatori. Su questo punto, nel testo è presente un esplicito richiamo alla difesa e alla sicurezza nazionale quando si afferma che «*il governo federale è chiamato a dare priorità agli investimenti in tali tecnologie emergenti, promuovendo una nuova stagione di sviluppo industriale*»^[147]. Tale inciso pare

indirizzato allo sviluppo dell'uso militare di siffatte tecnologie, in particolare il riferimento alla gestione della supply chain nella manifattura statunitense di robotica e droni, per il cui superamento delle criticità viene raccomandata la promozione di un confronto tra pubblico e privato sotto la guida del Department of Commerce (DOC), attraverso la National Telecommunications and Information Administration (NTIA).

Per quanto concerne la parte dedicata alla scienza, si osserva che anche in questo ambito l'AI avrà una influenza trasformativa, infatti i sistemi di AI sono già in grado di generare modelli di strutture proteiche, creazione di nuovi materiali e capacità di progettazione di esperimenti, consentendo l'accelerazione del progresso scientifico. Tuttavia, secondo l'AIAP, sarà possibile potenziare siffatto sviluppo solo attraverso cambiamenti su scala industriale nelle modalità con cui la sperimentazione scientifica viene condotta. A questo proposito, l'AIAP auspica una innovazione strutturale completa e il sostegno a nuove tipologie di organizzazioni scientifiche^[148]. Nello specifico l'AIAP intende promuovere la trasformazione della ricerca scientifica da attività di laboratorio a iniziativa ingegneristica su scala industriale^[149].

Si rimarca nuovamente l'importanza della condivisione non solo dell'AI in modalità open-source, ma pure di dataset "di alta qualità" che possano da questa venire utilizzati, nonché tenendo in considerazione l'impatto dei dataset scientifici e ingegneristici derivanti da precedenti attività finanziate nella valutazione delle proposte per nuovi progetti^[150]. Detti big data, necessari per i dataset, vanno considerati una risorsa strategica nazionale, per l'innovazione in ambito IA e per i benefici economici a essa connessi. Si sottolinea sul punto che molti Paesi, inclusi avversari strategici, hanno già superato gli Stati Uniti nella raccolta massiva di dati scientifici.

In questo punto sembrerebbe formarsi una contraddizione: da un lato l'AIAP si preoccupa di enfatizzare che per mantenere il ruolo di leader gli Stati Uniti devono migliorare i loro dataset scientifici rendendoli più accurati ed ottimizzati per l'AI. Dall'altro lato, al riguardo viene espresso esplicitamente il rispetto dei diritti individuali, delle libertà civili, della privacy e della riservatezza, in apparente contrasto con quanto affermato nel primo pilastro dell'AIAP, cioè la negatività dei vincoli giuridici allo sviluppo dell'AI e la necessità dell'applicazione del principio "try first".

Le azioni raccomandate per il raggiungimento degli obiettivi di miglioramento della scienza con l'AI concernono la definizione degli standard minimi di qualità dei dati per l'addestramento dei modelli di AI in ambiti come biologia^[151], scienza dei materiali, chimica e fisica^[152].

Infine, implementare un programma di sequenziamento completo del genoma di tutte le forme di vita presenti nei territori federali, al fine di generare una risorsa unica per l'addestramento dei futuri foundation models biologici. Sul punto si aprirebbe tuttavia una questione non trascurabile in materia di brevettabilità del genoma di siffatte forme di vita. Da un lato vi è la posizione di chi auspica di renderle proprietarie, dall'altro chi afferma la necessità della disponibilità pubblica del loro patrimonio genetico come common heritage^[153].

Su questo punto si era già pronunciata la Corte Suprema, con un noto e risalente precedente, cioè *Diamond v. Chakrabarty*^[154] sulla base del quale occorre distinguere un fenomeno naturale sconosciuto da un prodotto artificiale. Tuttavia, sulla base delle innovazioni tecnologiche di cui stiamo trattando, la distinzione si assottiglia sempre di più. Infatti, l'intervento degli LLMs sui materiali di training loro sottoposti è già stata riconosciuta come trasformativa dalla prima giurisprudenza federale intervenuta in materia con la decisione *Bartz v. Antropic*^[155], secondo cui l'effetto trasformativo dei modelli linguistici consente l'applicazione del principio del fair use. Tuttavia, la medesima trasformazione operata sui materiali biologici originari permetterebbe l'applicazione del summenzionato precedente *Chakrabarty* e pertanto la protezione proprietaria dei risultati.

Accanto alla promozione in ambito AI delle scienze biologiche, la progettualità proposta dall'AIAP si occupa anche di progressione dei LLMs e dei sistemi di AI generativa, i quali hanno rappresentato un cambiamento di paradigma nella scienza dell'AI. Inoltre, sul punto sono richiesti sforzi sull'interpretabilità, controllo e robustezza per superare il fatto che anche i sistemi avanzati, come gli LLMs, seppure si comprenda in linea generale come funzionino, rimangono opachi e imprevedibili limitandone l'uso in contesti critici quali sicurezza e difesa nazionale «*dove sono in gioco vite umane*»^[156].

7. Il contrasto dei “synthetic media” nell’ordinamento giuridico statunitense

Un raro momento di discontinuità contenuto nell’approccio deregolativo dell’AIAP riguarda il richiamo enfatico al “TAKE IT DOWN Act^[157]” che intende contrastare l’uso e la diffusione dei deepfake malevoli, come registrazioni audio, video o fotografie, prodotti con AI, in particolare proteggere contro deepfake sessualmente espliciti e non consensuali^[158]. Si tratta di un passaggio importante, che pare contraddire l’enfasi mostrata sulla protezione estrema garantita dal Free Speech anche alle posizioni più discutibili, spesso oltre il limite della veridicità. Tuttavia, va riconosciuto che siffatta normativa sia necessaria nella protezione delle parti vulnerabili di fronte alla produzione artificiale ovvero manipolazione di immagini contenuti intimi o personalissimi.

L’urgenza e la necessità di siffatta normativa è dimostrata da un recente caso deciso^[159] dalla giurisprudenza federale durante l’iter legis della citata disciplina, in particolare relativo alla diffusione illecita di video realizzati negli spogliatoi di un college, ove sarebbero state installate delle telecamere nascoste. Prima facie, parrebbe un caso consueto ai sensi della Sezione 230, tuttavia ci sarebbero due circostanze rilevanti ai fini della decisione della causa, ma che non sono state tenute in considerazione:

a) nel corso del procedimento le parti attrici, cioè le vittime dell’abuso, hanno sottolineato che numerose caratteristiche del design del sito web escluderebbero i gestori delle piattaforme di video sharing convenuti dall’immunità prevista dalla Sezione 230 data la creazione di thumbnail, la modifica dei tag (cioè di attività non neutre), di condivisione di materiali pedopornografici (sempre illeciti), la creazione di sezioni separate a favore di utenti selezionati, la non neutralità degli algoritmi utilizzati dalle piattaforme.

b) Dall’altro lato il mutamento normativo in corso di causa, cioè l’adozione del summenzionato TAKE IT DOWN Act.

Ciò nonostante, la Corte rigetta le istanze delle parti pur riconoscendo il grave danno subito dai ricorrenti, traditi da un dipendente del college e osservando che un episodio di oltre dieci anni fa continua a perseguirli poiché i video caricati online possono riemergere lungo tempo dopo^[160].

Tuttavia il TAKE IT DOWN Act non è sufficiente a impedire l’utilizzo nei

procedimenti giudiziari di prove artefatte elaborate con l'AI o analoghe minacce e pertanto l'AIAP suggerisce di adottare uno standard sui deepfake simile alla proposta di Rule 901(c) delle Federal Rules of Evidence sui requisiti per l'autenticazione delle prove in video, attualmente in esame da parte dell'Advisory Committee on Evidence Rules^[161].

8. Gli elementi strategici di chiusura del First Pillar

Per chiudere gli aspetti programmatici del Primo Pilastro, l'AIAP si focalizza sull'implementazione strategica dell'AI nelle attività pubbliche governative sia a favore del miglioramento dei servizi ai cittadini, sia nell'efficientamento dei processi interni attraverso programmi di formazione e implementazione trasparente, coordinata e sicura.

In questo contesto, si possono osservare alcune interazioni tra il piano di dismissione di massa del personale delle agenzie federali con la “rapida” assunzione di esperti di AI nelle agenzie con maggiori necessità^[162] al fine di istituire un “AI procurement toolbox” che fornisca modelli conformi a norme su privacy e trasparenza^[163], oltre a un catalogo di soluzioni già adottate^[164].

Specifiche attenzioni vengono anticipate in questa parte del Piano (e sviluppata nel secondo pilastro) e cioè la promozione dello sviluppo dell'AI nelle operazioni militari con accesso prioritario a risorse di calcolo e di cloud in particolare per quel che concerne dell'automazione dei flussi di lavoro più critici, all'interno di queste va sicuramente ricompreso l'utilizzo militare degli strumenti AI, come le già citate armi automatiche.

Infine, si rileva una contraddittorietà: nonostante l'apparente apertura verso i sistemi di Open AI, permane in realtà una prevalente e consolidata tutela della proprietà intellettuale delle innovazioni in ambito AI, finalizzata a bilanciare lo sviluppo tecnologico con la sicurezza nazionale. Tale approccio risulta particolarmente rilevante in seguito all'immissione sul mercato di modelli rappresentativi della competizione tecnologica, volti a ridurre i costi e incrementare le prestazioni, come nel caso del competitor cinese di Open AI, Deep Seek^[165].

In questo senso assume un significativo interesse l'Executive Order n. 14352 «*Saving TikTok While Protecting National Security*»^[166] in cui le parti hanno

formalizzato gli accordi sul trattamento dei dati degli utenti statunitensi della nota piattaforma cinese, considerato un elemento strategico sotto un profilo di difesa della sicurezza nazionale^[167]. Si tratta di un accordo quadro secondo cui la cessione qualificata di parte delle quote di TikTok, ai sensi del Protecting Americans from Foreign Adversary Controlled Applications Act, trovando una soluzione alle preoccupazioni in materia di sicurezza nazionale statunitense collegate al controllo da parte di avversari stranieri, in questo caso cinesi, sui dati personali e sui contenuti pubblicati sulla piattaforma da cittadini statunitensi. L'Executive Order n. 14352 concede un rinvio di 120 giorni nell'applicazione della legge al fine di portare a termine la formazione di una joint venture con sede negli Stati Uniti, ma con il mantenimento di una quota del 20% da parte della controparte cinese, la quale assumerebbe anche il controllo dell'algoritmo^[168]. Pertanto le agenzie quali il Department of Defense, il Center for AI Standards and Innovation e il Department of Homeland Security devono creare partneri con gli sviluppatori che rafforzino la protezione delle innovazioni da minacce informatiche, rischi interni e furti di proprietà intellettuale.

9. Il Secondo Pilastro: la costruzione dell'infrastruttura

I pilastri 2 e 3 riguardano aspetti extragiuridici e pertanto verranno trattati sommariamente e per ragioni di completezza nella ricostruzione del quadro emergente dall'AIAP.

Il secondo pilastro dell'AIAP si occupa della costruzione della rete infrastrutturale necessaria per lo sviluppo dell'AI in particolare per ciò che concerne la capacità energetica, che viene considerata inadeguata e in ritardo nello sviluppo rispetto a quella cinese. In questa parte emerge esplicitamente la sfida concorrenziale americana con l'avversario cinese. La prospettiva degli autori dell'AIAP è di questa tendenza, sembrerebbe, anche per l'enfasi da documento programmatico, a qualsiasi costo poiché «*America's path to AI dominance depends on changing this troubling trend*».

In realtà, per ribaltare il trend, il costo verrebbe pagato dalla (in)sostenibilità, tanto energetica quanto ambientale^[169] delle strategie adottate, a scapito della restrizione a carico degli utenti risorse naturali ed energetiche essenziali^[170].

La sfida in realtà non è soltanto con la Cina e la sua crescita industriale e

tecnologica raggiunta a passi da gigante, ma il rapporto tra sostenibilità dello sviluppo dell'AI e le risorse naturali necessarie, sia nell'approvvigionamento delle materie prime, soprattutto dell'acqua, sia nell'allocazione delle fabbriche di semiconduttori e di dotazione di fonti energetiche affidabili, comprese le reti per il loro trasporto.

In questo senso, il complesso sistema di permessi ambientali e regolamentari degli Stati Uniti, già sottoposti a restrizioni^[171] e oggetto di contenziosi federali per la tutela ambientale^[172], sono considerati un ostacolo alla costruzione rapida di tali strutture^[173].

Per migliorare il rapporto tra fabbisogno energetico e lo sviluppo dell'AI, l'AIAP suggerisce di delegare agli strumenti automatizzati, come il tool PermitAI, del dipartimento dell'energia le valutazioni ambientali, ai fini di velocizzare l'iter autorizzativo, nonché ai fini di aumentare la qualità delle analisi ambientali. In questo ambito uno dei settori più innovativi riguarda lo sviluppo di modelli in grado di generare risultati attraverso un processo di raffinamento iterativo (iterative refinement)^[174], eliminando progressivamente il “rumore” potenzialmente produttore di errori (le summenzionate allucinazioni^[175]) da un campione in più fasi^[176].

Altresì viene promossa l'implementazione delle variational autoencoders (VAE)^[177] e le generative adversarial networks (GAN)^[178], le quali, pur differendo nella loro architettura, perseguono lo stesso obiettivo: ricostruire strutture globali complesse a partire da dati sparsi. Questi modelli vengono solitamente applicati in ambiti in cui le dipendenze a lungo raggio si estendono su più dimensioni spaziali o strutturali, come il ripiegamento delle proteine, la dinamica atmosferica o la sintesi dei materiali, cioè in ambiti scientifici considerati dall'AIAP tra i più innovativi.

Anche nel Secondo Pilastro vi è un riferimento al rapporto tra innovazione tecnologica e coinvolgimento della forza lavoro. Il punto critico riguarda se l'AI svolgerà un ruolo di supporto allo svolgimento della realizzazione e del mantenimento delle infrastrutture tecnologiche sicure oppure se condurrà alla completa sostituzione del lavoro manuale ovvero intellettuale svolto da strumenti automatizzati.

Quali esempi di stretta connessione tra lavoratori altamente qualificati e sviluppo di tecnologie molto specializzate l'AIAP si riferisce alla costruzione e protezione

dei data center contro minacce informatiche e attacchi da parte di attori statali ostili. Parallelamente, occorrerebbe investire in formazione tecnica avanzata^[179] per la creazione delle competenze necessarie alla costruzione, gestione e manutenzione di queste strutture strategiche, come le figure professionali che si occupano tanto di infrastrutture fisiche, quanto digitali.

L'amministrazione deve colmare le carenze in questi ruoli attraverso politiche mirate e partnership pubblico-private. All'uopo si raccomanda di indentificare le occupazioni essenziali dell'infrastruttura IA a livello nazionale e definire framework di competenze, utili a progettare curricula, certificazioni e investimenti formativi.

Le strategie suggerite riguardano la ripetuta richiesta di ridurre gli ostacoli per le imprese, ma al contempo espandere la formazione pratica e la ricerca coinvolgendo università, college tecnici e comunitari per preparare e riqualificare la forza lavoro del futuro, sotto la guida del Department of Education.

Infine, il Secondo Pilastro suggerisce il rafforzamento della cybersecurity, ove l'AI diventa allo stesso tempo uno strumento di difesa e una potenziale minaccia, pertanto occorre proteggere le infrastrutture critiche per prevenire attacchi informatici. Sul punto le policy suggerite riguardano la previsione di linee guida per individuare le criticità e condividere una gestione strutturata delle minacce ai fini di progettare sistemi di AI "secure-by-design", nonché coordinare una capacità di risposta agli incidenti AI a livello federale. A questo proposito viene promossa la condivisione responsabile delle criticità alla luce dell'Executive Order 14306^[180].

10. Il Third Pillar: il ruolo guida degli Stati Uniti nello sviluppo dell'AI e i rapporti internazionali

Nelle intenzioni dei redattori dell'AIAP, il First Pillar di questo documento attribuisce un ruolo di leader degli Stati Uniti nella corsa all'AI per guidare la diplomazia tecnologica e la sicurezza internazionale nel quadro di competizione strategica globale per la supremazia nella corsa dell'AI. Se nel First Pillar l'AIAP evoca la «AI gold race», nel Third Pillar indica il luogo dove siffatta nuova corsa all'oro si svolge, cioè la scena globale.

Tale impostazione riflette la volontà di consolidare una leadership non solo

scientifica e industriale, ma anche geopolitica e giuridica, fondata sull'esportazione di modelli, standard e infrastrutture tecnologiche conformi ai principi di sicurezza, trasparenza e libertà economica tipici dell'ordinamento statunitense.

Questa prospettiva appare in continuità con il programma elettorale "America First", non solo sotto il profilo della politica dei dazi, ma anche in ambito diplomatico, con l'obiettivo di contrastare, anche in maniera incisiva e mediante l'applicazione strumentale, le strategie protezionistiche e le politiche daziarie relative alla presenza di piattaforme straniere concorrenti appartenenti a Stati rivali, come i sistemi della Repubblica Popolare Cinese, ad esempio nel già citato contenzioso inerente TikTok.

Ai fini dell'attuazione di una strategia multilivello di tutela degli interessi strategici americani, l'AIAP elabora una combinazione tra l'azione normativa, la diplomazia economica e la cooperazione internazionale partendo dall'esportazione del c.d. "full stack tecnologico"^[181] dell'intelligenza artificiale, comprendente hardware, software, modelli, applicazioni e protocolli^[182], il quale rappresenta uno strumento di consolidamento geopolitico.

Gli Stati Uniti intendono, infatti, promuovere la diffusione controllata di tecnologie di origine nazionale verso Paesi alleati e partner affidabili, onde evitare che tali soggetti dipendano da soluzioni sviluppate da potenze ostili, quasi rendendoli dipendenti dalla loro tecnologia, invece che di quella degli avversari^[183]. In questo spazio non sembra esserci posto per una regolamentazione in contrasto con l'approccio americano. Ci si riferisce da un lato alla prospettiva di prevenzione del rischio nell'uso dell'AI, che è contenuta nel Regolamento UE 1689/2024, esattamente agli antipodi del già analizzato approccio statunitense relativo al principio "try first"^[184], dall'altro lato al mantenimento sotto l'influenza statunitense degli organi internazionali deputati alla definizione degli standard tecnici e giuridici^[185].

Ulteriormente, la politica statunitense prevede il rafforzamento dei controlli sulle esportazioni di componenti critici, in particolare dei semiconduttori e delle tecnologie di calcolo avanzato, la cui rilevanza strategica si estende tanto al settore economico quanto a quello militare^[186]. Siffatto regime di export control enforcement si fonda su un approccio preventivo e dinamico, volto a chiudere le lacune normative e a rafforzare la cooperazione con gli alleati nella costruzione di

un quadro regolatorio condiviso, realizzando una strategia che combini la disciplina di diritto positivo con il soft law contenuto nelle previsioni tecniche. In tal senso, gli Stati Uniti intendono promuovere una progressiva armonizzazione dei regimi di controllo tecnologico, onde evitare fenomeni di backfill tecnologico, ossia la fornitura indiretta di tecnologie sensibili da parte di partner non vincolati da restrizioni equivalenti^[187].

Il principio di sicurezza tecnologica viene, inoltre, esteso alla sfera della diplomazia multilaterale. Tale cooperazione giuridico-diplomatica mira a garantire la coerenza tra la normativa interna statunitense e quella dei Paesi partner, creando così un sistema integrato di protezione dei settori critici, in particolare della difesa e delle infrastrutture strategiche. L'obiettivo è quello di assicurare che gli avversari strategici non possano accedere a tecnologie di frontiera, preservando al contempo la libertà di innovazione e il commercio lecito tra Stati alleati^[188].

Sul piano interno, il mantenimento della leadership statunitense nella valutazione dei rischi di sicurezza nazionale associati ai modelli di IA avanzata assume rilievo costituzionale, poiché incide direttamente sulla protezione dell'ordine pubblico, della difesa e delle infrastrutture critiche^[189]. Parallelamente, l'ordinamento deve prevedere la valutazione delle implicazioni derivanti dall'impiego di sistemi di IA stranieri nelle reti e nei servizi strategici nazionali, con particolare attenzione alla possibilità di backdoor o comportamenti algoritmici intenzionalmente malevoli. In tale contesto, la formazione di competenze scientifiche di eccellenza presso enti quali il National Institute of Standards and Technology (NIST), il Department of Energy, il Department of Defense e le agenzie d'intelligence si configura come un'esigenza giuridica di natura preventiva, funzionale alla costruzione di un sistema di vigilanza tecnico-normativa permanente. In questo caso si potrebbe aprire una discussione sull'ammissibilità dell'applicabilità dei software predittivi in ambito penale ovvero investigativo, come ad esempio l'uso del software proprietario "Gotham", elaborato e commercializzato dalla società americana "Palantir", specializzata nell'organizzare sistemi operativi in grado di sviluppare modelli capaci di gestire enormi quantità di dati, raccolti in operazioni di sorveglianza massiva ai fini di prevenzione dei crimini^[190]. Da un punto di vista comparatistico siffatto software ha già avuto due riscontri negativi: da un lato il Bundesverfassungsgericht tedesco ha sanzionato l'incostituzionalità dell'uso in

quanto il trattamento massivo di dati personali contenuti in banche dati, effettuato da programmi di analisi ovvero di valutazione automatizzata, rappresenta una interferenza sul diritto di autodeterminazione informativa dei titolari di siffatti dati ai sensi del combinato disposto dell'art 1 e dell'art. 2 Grundgesetz^[191]. Dall'altro lato il Reg. 1689/2024 li considera addirittura proibiti in quanto effettuano una valutazione predittiva della commissione di un reato penale basandosi esclusivamente sulla profilazione dei comportamenti o della personalità ex art. 5 c), relativo alle pratiche di AI vietate^[192].

L'AIAP conclude il Third Pillar facendo un richiamo agli investimenti nella biosecurity, la quale costituirebbe una declinazione emergente della sicurezza nazionale nell'era dell'IA. L'interconnessione tra biotecnologie e intelligenza artificiale apre, oltre alle nuove frontiere di ricerca, anche a rischi significativi connessi alla possibilità di sintesi di patogeni o biomolecole pericolose. Di conseguenza, il diritto della sicurezza scientifica impone l'adozione di un approccio multilivello, che combini obblighi di due diligence per i fornitori di materiali biologici, controlli sugli attori potenzialmente malevoli e cooperazione internazionale in materia di monitoraggio e scambio informativo^[193]. Tutte le istituzioni beneficiarie di fondi federali sono tenute a utilizzare fornitori di sintesi dotati di procedure certificate di verifica e screening dei clienti, in conformità a meccanismi di enforcement obbligatori^[194].

Nel suo complesso, il Third Pillar si configura, dunque, come un paradigma normativo integrato di politica estera e sicurezza tecnologica, che, attraverso l'esportazione controllata di innovazione, l'allineamento regolatorio e la diplomazia della sicurezza, mira a riaffermare la centralità del diritto statunitense quale fonte di legittimazione e protezione dell'ordine tecnologico globale. Tuttavia, si rileva che l'intero AIAP non presenta alcuna analisi economico-finanziaria delle strategie propuginate, come se si volesse evitare, se non addirittura negare, l'ipotesi condivisa da diversi esperti dei mercati finanziari^[195], ossia l'eventualità dello scoppio di una bolla finanziaria.

1. The White House, “*Winning the Race, America’s AI Action Plan, July 2025*”, <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>, firmato in data 23 luglio 2025 e redatto dai consiglieri del Presidente Trump M. J Kratsios (cioè il *Chief Technology Officer of the United States*), D. O. Sacks (ovvero il “*White House AI and Crypto Czar*”) e M. A. Rubio (il quale è il 72° Segretario di Stato

- americano); B. Graves, *EDUCAUSE Joins Comments to Inform Trump Administration's AI Action Plan*, in *EDUCAUSE Review (Online)*, 2025.
2. AIAP, *cit.*, p. 1
 3. C. van Noordt, R. Medaglia, L. Tangi, *Policy initiatives for Artificial Intelligence-enabled government: An analysis of national strategies in Europe*, in *Public Policy and Administration*, 40, 2, 2025, pp. 215-253.
 4. Regolamento 2024/1689/UE del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti n. 2008/300/CE, n. 2013/167/UE, n. 2013/168/UE, 2018/858/UE, 2018/1139/UE e 2019/2144/UE e le direttive 2014/90/UE, 2016/797/UE e 2020/1828/UE (regolamento sull'intelligenza artificiale).
 5. Nel frattempo in Italia è entrata in vigore la legge 23 settembre 2025, n. 132, pubblicata sulla G. U. 25 settembre 2025, n. 223 e rubricata «*Disposizioni e deleghe al Governo in materia di intelligenza artificiale*». Tra i primi commenti in dottrina, I. Forgione, *Intelligenza artificiale e principio di legalità nella legge 132/2025*, in *Quotidiano Giuridico*, 16 ottobre 2025; E. Raffiotta, *La legge italiana sull'intelligenza artificiale e la sfida cruciale dell'innovazione da realizzare*, in *Diritto e Giustizia*, 13 ottobre 2025; R. Perlusz, *Dalla proposta AS 1146 alla legge 132/2025: il quadro normativo italiano sull'IA prende forma* in *Medialaws*, 10.10.2025, <https://www.medialaws.eu/22350-2/>; B. Fragasso, *Profili penalistici della legge sull'intelligenza artificiale: osservazioni a prima lettura: Legge 23 settembre 2025, n. 132, recante «Disposizioni e deleghe al Governo in materia di intelligenza artificiale»*, in *Sistema penale*, 10, 2025, pp. 157-179; B. N. Romano, *Intelligenza artificiale e piattaforme digitali: opportunità e rischi alla luce del recente quadro regolatorio*, in *Diritto Pubblico Europeo – Rassegna online*, 2, 2025; A. Pellegrino, *Dal procedimento digitale all'amministrazione algoritmica responsabile: la nuova disciplina dell'intelligenza artificiale nella pubblica amministrazione dopo la Legge n. 132/2025*, in *Amministrazione e contabilità dello Stato e degli enti pubblici*, 16 ottobre 2025.
 6. Secretary of State Science, Innovation and Technology, AI Opportunities Action Plan, 13 g e n n a i o 2 0 2 5 , <https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan>.
 7. A. H. Zhang, *The promise and perils of China's regulation of artificial intelligence*, in *Columbia Journal of Transnational Law*, 63, 2025, p. 1; S. Wang, Y. Zhang, Y. Xiao, Z. Liang, *Artificial intelligence policy frameworks in China, the European Union and the United States: An analysis based on structure topic model*, in *Technological Forecasting and Social Change*, 212, 2025, art. 123971; S. Sforza, D. L. Totaro, *Governance dell'IA nell'epoca dei deepfake: note comparatistiche sulle esperienze di Cina e Giappone*, in *Cyberspazio e diritto*, in *Rivista internazionale di informatica giuridica*, 1, 2025, pp. 139-158.
 8. Il 28 maggio 2025 è stata approvata la “Legge sulla promozione della ricerca, dello sviluppo

- e dell'utilizzo delle tecnologie legate all'intelligenza artificiale". In dottrina, Y. Ikkatai, Y. Itatsu, T. Hartwig, J. Noh, N. Takashi, Y. Yaguchi, H. M. Yokoyama, *The relationship between the attitudes of the use of AI and diversity awareness: comparisons between Japan, the US, Germany, and South Korea*, in *AI & Society*, 4, 2025, pp. 2369-2383.
9. F. Busch, R. Geis, Y. C. Wang, J. N. Kather, N. A. Khori, M. R. Makowski, I. K. Kolawole, D. Truhn, W. Clements, S. Gilbert, L. C. Adams, E. Ortiz-Prado, K. K. Bressemer, *AI regulation in healthcare around the world: what is the status quo?*, in *medRxiv*, 1, 2025.
 10. B. Lund, Z. Orhan, N. R. Mannuru, R. V. K. Bevara, B. Porter, M. K. Vinaih, P. Bhaskara, *Standards, frameworks, and legislation for artificial intelligence (AI) transparency*, in *AI and Ethics*, 2025, pp. 1-17. Tuttavia, il 5 novembre 2025, il Ministry of Electronics and Information Technology ha emanato le "India AI Governance Guidelines" per bilanciare un'adozione dell'IA favorevole all'innovazione con misure volte a mitigare i rischi per individui, comunità e sicurezza nazionale consultabili al seguente link <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf>.
 11. Sul punto vi è chi si esprime in termini di "light-touch governance" (C. Meinhardt, D. Zhang, J. King, A. Haupt, E. Cryst, *Inside Trump's Ambitious AI Action Plan*, Stanford Institute for Human-Centered AI (HAI), 24 luglio 2025, <https://hai.stanford.edu/news/inside-trumps-ambitious-ai-action-plan>).
 12. D. Blumenthal, *The Trump Administration's Recent Policy Proposals Regarding Artificial Intelligence*, in *NEJM AI*, vol. 2, 10, 2025, pp. 65-74.
 13. AIAP, *cit.* p. 1.
 14. AIAP, *ult. op. loc. cit.*
 15. E. Logan, *The 2024 US presidential election & the politics of race: responding to a moment of crisis with analysis, insight & action*, in *Ethnic and Racial Studies*, 15, 2025, pp. 1-18; W. Echikson, *Trump, tech and transatlantic Turbulence*, in *European View*, vol. 24, 1, 2025, pp. 65-74.
 16. D. Krause, *Implications of the EU AI Act for US Regulatory Strategy and Corporate Risk Management*, 8 maggio 2025, disponibile in SSRN: <https://ssrn.com/abstract=5247258>.
 17. Dopo la cancellazione dell'EO 14110, la Presidenza Trump non è rimasta inerte, ma nell'aprile 2025 ha emanato due Executive Order: l'EO 14277 intitolato «*Advancing Artificial Intelligence Education for American Youth*» e l'EO 14278 rubricato «*Preparing Americans for High-Paying Skilled Trade Jobs of the Future*». In dottrina, A. Shubham, *The Impact of Artificial Intelligence on the Lifestyle and Future Prospects of Youth*, in A. Beniwal, *Artificial Intelligence, Ethics, and the Digital Society: Pathways to Sustainable Development*, Deep Science Publishing, 2025, p. 140; V. Lubello, *From Biden to Trump: Divergent and Convergent Policies in The Artificial Intelligence (AI) Summer*, in *DPCE Online*, 1, 2025, <https://ssrn.com/abstract=5302544>.
 18. Per completezza di analisi, si consenta di rinviare a E. Falletti, *Uno sguardo oltre i confini dell'UE: l'esperienza degli Stati Uniti d'America*, in R. Cavallo Perin, D.U. Galetta, *Diritto*

- dell'Amministrazione Digitale, Giappichelli, Torino, II ed., 2025, p. 453 ss., di cui questo contributo è di ideale prosecuzione e completamento. In dottrina si veda anche T. Davtyan, *The US approach to AI regulation: federal laws, policies, and strategies explained* in *Journal of Law, Technology, & the Internet*, 2025, vol. 16, 2, 223.
19. Altrimenti conosciuta come “Fourth Industrial Revolution” (R. Morrar, H. Arman, S. Mousa, *The Fourth Industrial Revolution (Industry 4.0): A Social Innovation Perspective*, in *Technology Innovation Management Review*, vol. 7, 11, 2017, pp. 12-20.
 20. J. F. Caron, *Artificial Intelligence and Life in the Fourth Industrial Revolution: Summoning the Demon?*, Taylor & Francis, 2025.
 21. C. M. Pease, *The Destruction DOGE Has Wrought on Science Is Immense*, in *Env't F.*, 42, 2025, p. 17.
 22. P. J. Phillips, G. Pohl, *Elon Musk and the Strategy of DOGE*, 2025, disponibile su SSRN: <https://ssrn.com/abstract=5104698>; A. C. Arslan, *Techno-Populist Leadership under Techno-Politics: The Case of the Musk Effect*, in «*International Journal of Public Leadership*», 1, 2025, pp. 1-20.
 23. Definito anche come “tech mogul” (C. Ibled, ‘*Founder as Victim, Founder as God*’: Peter Thiel, *Elon Musk and the Two Bodies of the Entrepreneur*, in *Journal of Cultural Economy*, 5, 2025, pp. 1-21).
 24. Musk cessò di rivestire siffatto ruolo il 29 maggio 2025 (I. Sentner, *After four months of disruption, Elon Musk signals he's leaving government*, in *Politico*, 29 maggio 2025).
 25. AIAP, *ult. loc. op. cit.*
 26. A. L. Whitehead, S. L. Perry, *Christian Nationalism and the Vote for Donald Trump in the 2024 Presidential Election: A State Level Analysis*, in *Nations and Nationalism*, 6 aprile 2025.
 27. «*AI is far too important to smother in bureaucracy at this early stage, whether at the state or Federal level*» (AIAP, *cit.* p. 1).
 28. AIAP, *cit.*, p. 3.
 29. P. Brest, *The Misconceived Quest for the Original Understanding*, in *Boston University Law Review*, 60, 1980, p. 204; M. L. Pulido, *Originalism and Non-Originalism as Legal Hermeneutics*, in *University of Bologna Law Review*, 9, 2024, p. 17.
 30. L. J. Strang, *Originalism and Conservatorism: An American Story*, The Heritage Foundation, 2024, p. 1; D. Pearlstein, *The Impact of Movement “Originalism” on American Legal Polarization*, in *The Law & Ethics of Human Rights*, vol. 19, 1, 2025, pp. 51-88; F. Tonello, *La Costituzione degli Stati Uniti*, Bruno Mondadori, Milano, 2010.
 31. Si tratta dell'Executive Order 14192 del 31 gennaio 2025, intitolato «*Unleashing Prosperity Through Deregulation*», ove si incaricano l'Office of Science and Technology Policy (OSTP), il quale si occupava di censire, attraverso il coinvolgimento delle imprese, le normative ostative allo sviluppo dell'AI e collaborare con tutte le agenzie federali per identificare, rivedere o abrogare regolamenti, norme, memorandum, ordini amministrativi, documenti di orientamento, dichiarazioni politiche e accordi tra agenzie e la Office of Management and Budget (OMB) di verificare se i regimi normativi dell'IA dello Stato

possono ostacolare l'efficacia del finanziamento o dell'assegnazione; alla Commissione Federale per il Commercio (FTC) di analizzare le politiche avviate sotto la precedente amministrazione per garantire che non avanzino teorie di responsabilità che gravino indebitamente sull'innovazione dell'IA.

32. C. Novelli, A. Gaur, A. L. Floridi, *Two Futures of AI Regulation under the Trump Administration*, 31 marzo 2025, disponibile su SSRN: <https://ssrn.com/abstract=5198926>.
33. Dati aggiornati al 10 luglio 2025, consultati il 10 ottobre 2025 disponibili al seguente sito Internet: <https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation>.
34. Ai fini di bloccare l'iniziativa legislativa statale, in data 11 dicembre 2025, la Presidenza Trump ha emanato un nuovo *Executive Order* intitolato «*Ensuring a National Policy Framework for Artificial Intelligence*» (consultabile sul sito: <https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/>). Secondo tale provvedimento presidenziale, la regolamentazione dell'AI a livello statale creerebbe un sistema frammentato di 50 regimi diversi complicando il quadro normativo, soprattutto per le start-up. Inoltre, alcune leggi statali imporrebbero l'inserimento di presunti bias ideologici nei modelli, arrivando talvolta a incentivare risultati apparentemente distorti per evitare trattamenti differenziali, in contrasto con le altre politiche poste in essere dalla Presidenza Trump, quali il contrasto ai c.d. "DEI". Altre norme eccederebbero la competenza statale, incidendo sul commercio interstatale. Sarebbe quindi necessario l'intervento governativo per costruire un quadro normativo nazionale federale unitario e poco oneroso, prevalente sulle leggi statali in conflitto, che tuteli minori, proprietà intellettuale, comunità e libertà di espressione, nonché sia in grado di consentire agli Stati Uniti di competere nell'AI, come programmato dall'AIAP in commento in questa sede.
35. S. Booth, *Strong Consumer Protection is an Inalienable Defense for AI Safety in the United States*, in *Forty-Second International Conference on Machine Learning – Position Paper Track*, 17 luglio, 2025.
36. Intitolato: *Act Concerning consumer protections in interactions with artificial intelligence systems*, modellato sull'AI Act europeo, firmato dal Governatore del Colorado il 17 maggio 2024, che entrerà in vigore il 1 febbraio 2026 e che contiene norme per lo sviluppo e per l'implementazione di sistemi di AI ad alto rischio. In dottrina, M. Jariwala, *A Comparative Analysis of the EU AI Act and the Colorado AI Act: Regulatory Approaches to Artificial Intelligence Governance*, in *International Journal of Computer Applications*, 975, 2024, p. 8887; E. Razis, J. C. Cooper, *The Federalist's Dilemma: State AI Regulation & Pathways Forward*, in *George Mason Law & Economics Research Paper*, n. 25, 7, 2025.
37. Intitolato: Consumer Protection. Relates to consumer protection, use of a computer to interact with a consumer when consumer believes the interaction is with a human is an unlawful trade practice.

CERIDAP

38. Intitolato: Workplace Surveillance Tools, Requires an employer to annually provide a notice to the Department of Industrial Relations, in the Labor and Workforce Development Agency, of all the workplace surveillance tools the employer is using in the workplace. Requires the notice to include, among other information, the data that will be collected from workers and consumers and whether they will have the option of opting out of the collection of personal data.
39. Intitolato: Fair Online Pricing Act. Provides for the Fair Online Pricing Act. Prohibits a price offered to a consumer through the consumer's online device from being generated based on certain input data, including the presence or absence of any software on the online device. Requires, if an online device cannot display a certain link because it lacks a physical display, a person to create an alternate mechanism for providing access to the list of input data.
40. Intitolato: Unfair Trade Practices and Consumer Protection. Amends the act known as the Unfair Trade Practices and Consumer Protection. Law; provides for definitions.
41. Intitolato: Unfair Trade Practices. Amends the act known as the Unfair Trade Practices and Consumer Protection Law; provides for definitions and for unlawful acts or practices and exclusions.
42. Intitolato: Law. Amends the act known as the Unfair Trade Practices and Consumer Protection Law; provides for definitions.
43. Intitolato: Consumer Protection. Requires the office of the attorney general and reporter to submit to the chair of the house committee having jurisdiction over consumer protection and the chair of the commerce and labor committee of the senate a report on the number of investigations into violations of the Tennessee Consumer Protection Act of 1977 in which AI was used to effectuate an unfair or deceptive act or practice affecting the conduct of any trade or commerce between the specified date.
44. Intitolato: Consumer Protection. Requires the office of the attorney general and reporter; submits to the Chair of the House Committee having jurisdiction over consumer protection and the Chair of the Commerce and Labor Committee of the senate a report on the number of investigations into violations of the State Consumer Protection Act of 1977 in which artificial intelligence was used to effectuate an unfair or deceptive act or practice affecting the conduct of any trade or commerce between the specified date, and a specified date.
45. Intitolato: Establishing a Framework to Govern the Use of AI. Relates to establishing a framework to govern the use of AI systems in critical decision-making by private companies and ensure consumer protections; authorizes a civil penalty.
46. Intitolato: AI Consumer Protection Amendments. Enacts provisions related to the use of generative AI in consumer transactions and regulated services; requires certain disclosures when generative AI is used in consumer transactions and regulated services; establishes liability for violations of consumer protection laws involving AI; provides a safe harbor for certain disclosures.
47. Intitolato: Consumer Data, Privacy. Relates to consumer data privacy and online

CERIDAP

- surveillance.
48. Intitolato: High Risk AI. Relates to high-risk AI; relates to development, deployment, and use; relates to civil penalties; provides that each developer of a high-risk AI system shall use a reasonable duty of care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination arising from the intended and contracted uses.
 49. Intitolato: Consumer Data Protection Act. Relates to consumer Data Protection Act; relates to AI Training Data Transparency Act; allows consumers to authorize a third party, acting on the consumer's behalf, to opt out of the processing of the consumer's personal data; provides that such authorization may be made using technology that indicates the consumer's intent to opt out, including a browser setting, browser extension, global device setting, or other user-selected universal opt-out mechanism.
 50. Intitolato: Division of Consumer Counsel. Relates to Division of Consumer Counsel; relates to duties; relates to AI fraud and abuse; expands the duties of the Division of Consumer Counsel to include establishing and administering programs to address AI fraud and abuse; provides that such programs would include establishing a statewide fraud and abuse alert system to be administered by the Division.
 51. Intitolato: Misleading Synthetic Media. Relates to consumer protection; prohibits the dissemination of synthetic media as specified; provides definitions; provides remedies; provides penalties; provides for an effective date.
 52. K. Marselas, *AI-Shortened Nursing Home Stays Drive Potential Class Action Suit Against Insurer*, in *McKnight's Long-Term Care News*, 2023; E. Jang, *Oops? Interdisciplinary Stories of Sociotechnical Error. When Faulty AI Falls Into the Wrong Hands: The Risks of Erroneous AI-Driven Healthcare Decisions*, in *International Journal of Communication*, 19, 2025, p. 7. In giurisprudenza: La prima causa è Estate of Gene B. Lokken v. UnitedHealth Group1 (UHG). Si tratta di una causa in cui UHG fu citata in giudizio per dinieghi di copertura automatizzati tramite intelligenza artificiale all'interno dei suoi piani Medicare Advantage, in cui veniva utilizzato un algoritmo, noto come nH Predict, utilizzato per determinare se i sottoscrittori del summenzionato programma dovessero ricevere cure post-acute. La questione controversa riguardava la circostanza che il software predittivo sovvertiva i pareri dei sanitari curanti, elaborando previsioni imprecise sul recupero dei pazienti, con conseguenti dimissioni ospedaliere premature di beneficiari vulnerabili con gravi conseguenze sulla loro salute. Simili controversie riguardano i casi United States ex rel. Shea v. eHealth, Inc. et al. (Massachusetts District Court, 1:21-cv-11777); Barrows et al v. Humana (Kentucky Western District Court, 3:23-cv-00654), e Estate of Gene B. Lokken v. United Health Group (Minnesota District Court, Docket No. 0:23-cv-03514). Tuttavia, l'AIAP sembra andare in senso contrario a quanto stabilito dalle Corti. Sul punto, P. McLaughlin, *AI Under Scrutiny: Federal Court Allows Class Action to Proceed Against United Health Over Coverage Decisions*, in *Journal of Health Care Compliance*, 27(3), 2025.
 53. Intitolato: Claims and Prior Authorization. Provides that before a health care insurer may deny a claim submitted by a provider on the basis of medical necessity, the medical

CERIDAP

- director shall individually review the denial. Provides that during each individual review, the medical director shall exercise independent medical judgment and may not rely solely on recommendations from any other source.
54. Intitolato: Health Care Providers. Prohibits health care providers and health care insurers from using AI in the delivery of health care services or the generation of medical records unless certain requirements are met.
 55. Intitolato: Health Insurance and Patient Protection. Provides that each utilization review, there shall be a rebuttable presumption that each health care service under review is medically necessary if such health care service was ordered by a health care professional acting within such health care professional's scope of practice; provides that any utilization review company performing such review of a health care service shall have the burden of proving that such health care service is not medically necessary.
 56. Intitolato: Medical Practice Act. Amends the Medical Practice Act; defines terms; provides that a health facility, clinic physician's office, or office of a group practice that uses generative AI to generate written or verbal patient communications pertaining to patient clinical information shall ensure that the communications meet certain criteria; provides that a communication that is generated by generative AI and read and reviewed by a human licensed or certified health care provider.
 57. Intitolato: Technology Produced by Certain Foreign Countries;Relates to AI platforms; prohibits the use of AI platforms of concern on state-issued devices and networks; prohibits medical and research facilities from using genetic sequencers or operational software used for genetic analysis that is produced in or by a foreign adversary; provides that any state agency that utilizes an AI platform of concern or has an account with such platform shall deactivate and delete such account and shall no longer use the platform.
 58. Intitolato: Use of AI in the Denial of Health. Prohibits the use of AI in the denial of health insurance claims.
 59. Intitolato: Medical or Dental Care. Revises provisions relating to prior authorization for medical or dental care under health insurance plans.
 60. Intitolato: Health Insurance. Revises provisions relating to health insurance.
 61. Intitolato: Health Care. Prohibits certain health insurers, including insurance for public employees, from solely using, employing or relying upon an AI system or an automated decision tool to, among other things, deny a request for prior authorization for medical or dental care; relates to plans of self insurance; encourages physicians, physician assistants, advanced practice registered nurses, and osteopathic physicians to inform patients of options related to donating, banking or storing stem cells.
 62. Intitolato: Use of AI In Health Care. Relates to health care; requires a medical facility or a provider of health care who uses generative AI to generate certain communications to ensure that those communications include certain information; provides other matters properly relating there to; closes title an act relating to health care; requires a medical facility or a provider of health care who uses generative AI to generate certain communications to ensure that those communications include certain.

CERIDAP

63. Intitolato: Certain Medical and Dental Care Authorization. Relates to insurance; revises provisions relating to prior authorization for certain medical and dental care; revises provisions relating to the coverage of autism spectrum disorders for certain persons; prohibits health insurers from considering the availability of certain public benefits for certain purposes; provides other matters properly relating thereto; closes title an act relating to insurance; revises provisions relating to prior authorization for certain medical and dental care.
64. Intitolato: Liability for Damages Caused by Chatbot. Imposes liability for damages caused by a chatbot impersonating licensed professionals or giving any medical or psychological advice.
65. Intitolato: Health Benefit Plans. Ensures that health benefit plan determinations of the medical necessity or appropriateness of healthcare services continue to be made by licensed and qualified healthcare providers.
66. State Government. Relates to state government; creates the Citizen's Bill of Rights; provides short title; defines terms; (...) prohibits certain entities from taking certain actions relating to medical procedures.
67. Medical Assistance Program Provider Enrollment. Directs the state Health Authority to expedite the process for enrolling providers in the medical assistance program and study the feasibility of developing and implementing an automated, online tool for provider enrollment applications.
68. Intitolato: AI Amendments. Establishes protections for users of mental health chatbots that use AI technology; prohibits certain uses of personal information by a mental health chatbot; requires a mental health chatbot to make certain disclosures to users; provides enforcement authority to the Division of Consumer Protection; establishes requirements for creating and maintaining policies for mental health chatbots; creates rebuttable presumptions for suppliers who comply with policy requirements.
69. Sul rischio di una frantumazione del diritto dei consumatori proveniente dalla normativa in materia di regolamentazione dei mercati digitali si veda F. de Elizalde, *Fragmenting Consumer Law through Data Protection and Digital Market Regulations: The DMA, the DSA, the GDPR, and EU Consumer Law*, in *Journal of Consumer Policy*, vol. 48, 2025, pp. 1-35; C. Buttaboni, G. Colangelo, L. Floridi, *Governing Platform Power in the EU: A Legal and Ethical Assessment*, 2025, disponibile su SSRN: <https://ssrn.com/abstract=5110753>; E. A. Raffaelli, *I mercati digitali e le norme di regolazione: tra limiti del diritto antitrust e nuove modalità di intervento "ex ante"*, in *Rivista di diritto industriale*, 2, 2024, pp. 45-91; E. Stamboliev, T. Christiaens, *How Empty Is Trustworthy AI? A Discourse Analysis of the Ethics Guidelines of Trustworthy AI*, in *Critical Policy Studies*, vol. 19, 1, 2025, pp. 39-56.
70. S. Wang, Y. Zhang, Y. Xiao, Z. Liang, *Artificial Intelligence Policy Frameworks in China, the European Union and the United States: An Analysis Based on Structure Topic Model*, in *Technological Forecasting and Social Change*, 212, 2025, p. 123971; S. Pan, G. T. Goodnight, X. Zhao, Y. Wang, L. Xie, J. Zhang, "Game Changer": *The AI Advocacy*

- Discourse of 2023 in the US*, in *AI & Society*, vol. 40, 4, 2025, pp. 2807-2819; K. Meding, C. Sorge, *What Constitutes a Deep Fake? The Blurry Line Between Legitimate Processing and Manipulation Under the EU AI Act*, in *Proceedings of the 2025 Symposium on Computer Science and Law*, 2025, pp. 152-159.
71. F. de Elizalde, *Fragmenting Consumer Law through Data Protection and Digital Market Regulations*, cit.
 72. A. Bradford, *The false choice between digital regulation and innovation*, in *Nw. UL Rev.*, vol. 119, 2, 2024, 377; J. Mulla, *AI Regulation and Entrepreneurship*, 15 ottobre 2024, disponibile su SSRN.
 73. N. Nevejans, *European Union's Regulation on the placing on the market and use of AI systems: a critical overview of the AI Act* in *Research Handbook on the Law of Artificial Intelligence*, 1, 2025, 489-540.
 74. J. Mulla, *AI Regulation and Entrepreneurship*, cit.
 75. Le start up, forma d'impresa comune nei settori a forte innovazione, potrebbero superare siffatte criticità optando per l'acquisizione da parte di aziende più grandi e meglio attrezzate per gestire l'onere della conformità normativa (J. Mulla, *ult. op. loc. cit.*).
 76. J. Mulla, *ult. op. loc. cit.*; V. Bertola, S. Quintarelli, *The Regulated Internet, Europe's Quest for Digital Sovereignty*, Springer, Cham, 2025, passim.
 77. Sia consentito rinviare a E. Falletti, *Sovranità digitale, tutela della sicurezza nazionale e libertà di manifestazione del pensiero: i faticosi equilibri della sentenza Tiktok v. Garland*, in *Dir. Inf. Informatica*, 1, 2025, 81 ss.
 78. AIAP, *cit.*, p. 3.
 79. Pubblicato il 31 gennaio 2025 e rubricato, *Unleashing Prosperity Through Deregulation*. Tra i primi commenti, L.A. Fennell, *From WTP to WTF: Valuation and Distributive Discourse*, in *University of Chicago Coase-Sandor Institute for Law & Economics Research Paper*, n. 25, 14, 2025, pp. 25-12.
 80. Il *Communications Act of 1934* è una legge federale degli Stati Uniti che istituisce la *Federal Communications Commission (FCC)* ai fini di regolamentare le comunicazioni via radio, televisione, onde radio, satellite e cavo a livello interstatale e internazionale. In dottrina, M. Connolly, *The 80th anniversary of the 1934 Communications Act and the inception of the Federal Communications Commission*, in *Review of Industrial Organization*, vol. 45, 3, 2014, pp. 201-202; R. R. John, *How Media Concentration in the Age of Radio Prefigured Today's Big Tech Debate*, in *promarket.org*, 17 giugno 2025.
 81. AIAP, *ult. op. loc. cit.*
 82. E. Kempf, O. G. Spalt, *Litigating Innovation: Evidence from Securities Class Action Lawsuits*, Centre for Economic Policy Research, 2020; L. Caruso, *Digital Innovation and the Fourth Industrial Revolution: Epochal Social Changes?*, in *AI & Society*, vol. 33, 3, 2018, pp. 379-392.
 83. S. Rodotà, *Tecnologie e diritti*, Il Mulino, Bologna, 1995.
 84. Come è noto, il principio originalista sostiene che il testo costituzionale vada inteso e interpretato nel senso che aveva nel momento della sua entrata in vigore, cioè alla fine del

- XVIII Secolo, onde impedire che gli organi giudiziari diventino essi stessi legislatori, attraverso adattamenti delle norme, specie costituzionali, al contesto relativo al tempo dell'applicazione della norma medesima. In siffatto modo vengono però trascurati i mutamenti sociali da allora intercorsi. La dottrina originalista, promossa in seno alla Corte Suprema dal Justice Antonin Scalia, trova un suo spazio fondativo nell'affermazione che devono essere i corpi elettorali, attraverso i loro rappresentanti, a decidere per mezzo di un atto legislativo la disciplina normativa delle fattispecie, rigettando gli interventi (più o meno creativi) della giurisprudenza. Questa teoria rifiuta nel modo più assoluto le costruzioni interpretative c.d. "evolutive" che possono essere proposte dalle Corti, specie da quelle Supreme. In un certo senso si potrebbe richiamare il pensiero montesquieiano: «*les juges ne doivent être que la bouche qui prononce les paroles de la loi, des êtres inanimés qui n'en peuvent modérer ni la force ni la rigueur (EL, XI, 6)*». Sulla teoria dell'originalismo, R. Post, R. Siegel, *Originalism as a Political Practice: The Right's Living Constitution*, in *Fordham L. Rev.*, 75, 2006, p. 545; L. K. Weis, *What comparativism tells us about originalism*, in *International Journal of Constitutional Law*, vol. 11, 4, 2013, pp. 842-869; J. E. Fleming, *Living Originalism and Living Constitutionalism as Moral Readings of the American Constitution*, in *BUL Rev.*, 7, 2012, p. 1171; S. E. Sachs, *Originalism Without Text*, in *Yale Law Journal*, vol. 127, 2017, pp. 156-168.
85. D. Bogen, *The Origins of Freedom of Speech and Press*, in *Maryland Law Review*, vol. 42, 1983, pp. 429 ss.; D. L. Doernberg, *We the People: John Locke, Collective Constitutional Rights, and Standing to Challenge Government Action*, in *California Law Review*, vol. 73, 1985, pp. 52 ss.; S. J. Heyman, *The Light of Nature: John Locke, Natural Rights, and the Origins of American Religious Liberty*, in *Marquette Law Review*, vol. 101, 2017, pp. 705 ss.; R. M. Smith, *Lockean Liberalism and American Constitutionalism in the Twenty-First Century: The Declaration of Independence or "America First"?*, in *American Political Thought*, vol. 8, 2, 2019, pp. 283-295; M. Minakov, *Freedom and Progress at the Dawn of the Age of Will: The Struggle of Two Enlightenments in the Current Euro-Atlantic Debate*, in *The Ideology and Politics Journal*, vol. 1, 27, 2025, pp. 97-144.
86. AIAP, *cit.*, p. 4
87. D. A. Farber, *The Imperious Presidency: Brazen Power Plays and Executive Overreach*, in *UC Berkeley Public Law Research Paper*, 23 agosto 2025.
88. Si tratta degli a) «*Ending Radical and Wasteful Government DEI Programs and Preferencing (Executive Order 14151)*», il quale si prefigge lo scopo di cancellare l'Executive Order 13985 di promozione dell'uguaglianza razziale ed emanato dall'allora presidente Biden. Questo EO ha eliminato tutti i mandati federali relativi alla DEI, i programmi e i relativi finanziamenti. Inoltre, ha imposto alle agenzie federali di segnalare qualsiasi tentativo di mascherare le iniziative relative alla DEI. L'Ufficio della gestione del personale (OPM) ha emesso una circolare che dispone il congedo retribuito dei dipendenti DEI. b) *Ending Illegal Discrimination and Restoring Merit-Based Opportunity (Executive Order 14173)*: questo EO mira ad eliminare le pratiche DEI in tutte le agenzie federali, revocando i precedenti ordini che promuovevano le pari opportunità. Inoltre, obbliga il

Procuratore Generale a fornire raccomandazioni su come influenzare il settore privato affinché ponga fine alle pratiche DEI. Richiede inoltre indagini su organizzazioni con dotazioni o patrimoni consistenti. c) *Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government (Executive Order 14168)*: questo ordine esecutivo revoca le politiche e le iniziative che prioritizzano l'identità di genere rispetto al sesso biologico, all'interno del governo federale. In dottrina, E. Ng, T. Fitzsimmons, M. Kulkarni, M. B. Ozturk, K. April, R. Banerjee, S. L. Muhr, *The Anti-DEI Agenda: Navigating the Impact of Trump's Second Term on Diversity, Equity and Inclusion*, in *Equality, Diversity and Inclusion: An International Journal*, vol. 44, 2, 2025, pp. 137-150; A. S. Gottlieb, R. Jagsi, *Removing Diversity, Equity, and Inclusion Infrastructure in Medicine in Public Health, and Science: The Cost of Overcorrection*, in *BMJ*, 388, 2025.

89. La creazione dello slogan «*Make America Great Again*» è riconducibile ad un discorso pronunciato dall'allora candidato repubblicano alla carica di Presidente degli Stati Uniti Ronald Reagan il 1 settembre 1980, ove affermava: «*This country needs a new administration, with a renewed dedication to the dream of America—an administration that will give that dream new life and make America great again!*», R. Reagan, “*Labor Day Speech at Liberty State Park, Jersey City, New Jersey*,” September 1, 1980, New Jersey, <https://www.reaganlibrary.gov/archives/speech/labor-day-speech-liberty-state-park-jersey-city-new-jersey>; A. A. Volle, *MAGA Movement*, *Britannica*, 1 August 2025, <https://www.britannica.com/topic/MAGA-movement>; A. Coussens, *MAGALAND: Reagan, Trump, and The MAGA Slogan*, in *Indiana University South Bend Undergraduate Research Journal of History*, 9, 2023, pp. 20-32; S. R. Mukherjee, *Make America Great Again as White Political Theology*, in *Revue LISA/LISA e-journal. Littératures, Histoire des Idées, Images, Sociétés du Monde Anglophone – Literature, History of Ideas, Images and Societies of the English-Speaking World*, vol. 16, 2, 2018.
90. Il movimento Make America Great Again è sorto nella campagna presidenziale di Donald Trump nel 2016, esso si è imposto come forza politica capace di convogliare un'idea di “ritorno” a una grandezza perduta degli Stati Uniti. Lo slogan «*Make America Great Again*» è divenuto simbolo di promesse di protezionismo economico, restrizioni sull'immigrazione e difesa di valori tradizionali. Il MAGA propone una visione nostalgica, fondata su un passato idealizzato in cui le gerarchie sociali erano più nette e le norme culturali dominanti restavano incontestate. Dietro questa retorica si cela però il desiderio di riaffermare strutture di potere egemoniche e sistemi di privilegio che hanno storicamente alimentato disuguaglianze, in particolare su base razziale e di genere. Per le comunità non bianche, la questione cruciale è individuare a quale epoca storica i sostenitori del MAGA intendano riferirsi. Infatti, in considerazione della rigorosa applicazione della teoria originalista, più ci si spinge indietro nel tempo, maggiormente vengono giustificati episodi di discriminazione e oppressione. In questo senso, l'ideologia del MAGA rivela un'adesione implicita a narrazioni suprematiste bianche. L'idea di “riconquistare la gloria passata” presuppone un ordine sociale gerarchico basato su razza,

etnia e status economico. Il movimento, inoltre, funziona dentro una logica di dissonanza cognitiva: simboli e slogan patriottici vengono strumentalizzati per giustificare politiche escludenti e discriminatorie. Ne risulta un intreccio complesso tra costruzione identitaria collettiva e mantenimento di assetti di potere dominanti, che però evidenziano una realtà scomoda, cioè il riaffiorare di ideologie suprematiste sotto le spoglie di attivismo politico (J. Breckenridge, *Make America Great Again (MAGA): The Covert Call for Colonialism's Comeback*, 11 aprile 2024, disponibile su SSRN: <https://ssrn.com/abstract=4790796>).

91. E. Tabassi, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST *Trustworthy and Responsible AI*, National Institute of Standards and Technology, Gaithersburg, MD, 2023, disponibile online: <https://doi.org/10.6028/NIST.AI.100-1>, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=93622 (consultato il 22 settembre 2025); N. Swaminathan, D. Danks, *Application of the NIST AI Risk Management Framework to Surveillance Technology*, 3, 2024; R. Dotan, B. Blili-Hamelin, R. Madhavan, J. Matthews, J. Scarpino, *Evolving AI Risk Management: A Maturity Model Based on the NIST AI Risk Management Framework*, «arXiv preprint», 1, 2024.
92. AIAP cit., p. 4. S. Shaw, *Reclaiming the Narrative: A Cartographic Analysis of Diversity, Equity, and Inclusion (DEI) and Critical Race Theory (CRT) Misinformation Campaigns*, in «*Journal of College and Character*», vol. 26, 1, 2025, pp. 84-95.
93. A. Bessi, F. Petroni, M. Del Vicario, F. Zollo, A. Anagnostopoulos, A. Scala, G. Caldarelli, W. Quattrociocchi, *Viral Misinformation: The Role of Homophily and Polarization*, in *Proceedings of the 24th International Conference on World Wide Web*, 2015, pp. 355-356; R. Mulcahy, R. Barnes, R. de Villiers Scheepers, S. Kay, E. List, *Going Viral: Sharing of Misinformation by Social Media Influencers*, in «*Australasian Marketing Journal*», vol. 33, 3, 2025, pp. 296-309; P. Törnberg, *Echo Chambers and Viral Misinformation: Modeling Fake News as Complex Contagion*, in «*PLoS One*», vol. 13, 9, 2018,.
94. P. Thagard, *Falsehoods Fly*, New York, Columbia University Press, 2024, pp. 14 ss.; L. Gielow Jacobs, *Freedom of Speech and Regulation of Fake News*, in *The American Journal of Comparative Law*, 70, 2022, pp. i278-i311; O. Pollicino (a cura di), *Freedom of Speech and the Regulation of Fake News*, Cambridge, Intersentia, 2023; A. I. Goldman, D. Baker, *Free Speech, Fake News, and Democracy*, in *First Amendment Law Review*, 18, 2019, pp. 66.L. Gielow Jacobs, *Freedom of speech and regulation of fake news*, cit.; O. Pollicino, *Freedom of speech*, cit.; S. Lewandowsky, *Free Speech, Fact Checking, and the Right to Accurate Information*, in *Science*, vol. 387, 6734, 2025; A. Singh, I. Kaur, A. K. Upadhyay, M. Trivedi, *Safeguarding Free Speech While Tackling Misinformation on Social Media Platforms*, in *National Seminar on Enhancing Privacy Protection in the Digital Age: Legal Challenges & Innovations (NSEPPDA 2025)*, Atlantis Press, 2025, pp. 4-21.
95. L. Gielow Jacobs, *Freedom of speech and regulation of fake news*, cit.; O. Pollicino, *Freedom of speech*, cit.; S. Lewandowsky, *Free Speech, Fact Checking, and the Right to Accurate Information*, in *Science*, cit.; A. Singh, I. Kaur, A. K. Upadhyay, M. Trivedi, *Safeguarding Free Speech While Tackling Misinformation on Social Media Platforms*, in *National Seminar on Enhancing Privacy Protection in the Digital Age: Legal Challenges &*

- Innovations, op. cit.*, pp. 4-21.
96. E. C. Tandoc Jr, A. Duffy, S. M. Jones-Jang, W. G. Wen Pin, *Poisoning the Information Well? The Impact of Fake News on News Media Credibility*, in *Journal of Language and Politics*, vol. 20, 5, 2021, pp. 783-802.
 97. S. Gal, *Language Ideologies*, in *Oxford Research Encyclopedia of Linguistics*, 2023; D. de Bruin, J. M. van Baar, P. L. Rodríguez, O. FeldmanHall, *Shared Neural Representations and Temporal Segmentation of Political Content Predict Ideological Similarity*, in *Science Advances*, vol. 9, 5, 2023,.
 98. G. Zagrebelsky, *Il "Crucifige!" e la democrazia*, Einaudi, Torino, 1995, *passim*.
 99. J. P. Quintais, *Generative AI, Copyright and the AI Act*, in *Computer Law & Security Review*, 56, 2025, p. 106107; C. Li, T. Zhang, X. Du, Y. Zhang, H. Xie, *Generative AI Models for Different Steps in Architectural Design: A Literature Review*, in *Frontiers of Architectural Research*, vol. 14, 3, 2025, pp. 759-783; S. S. Sengar, A. B. Hasan, S. Kumar, F. Carroll, *Generative Artificial Intelligence: A Systematic Review and Applications*, in *Multimedia Tools and Applications*, vol. 84, 21, 2025, pp. 23661-23700.
 100. Z. Wang, Z. Chu, T. V. Doan, S. Ni, M. Yang, W. Zhang, *History, Development, and Principles of Large Language Models: An Introductory Survey*, in *AI and Ethics*, vol. 5, 3, 2025, pp. 1955-1971; M. Steyvers, H. Tejada, A. Kumar, C. Belem, S. Karny, X. Hu, ... P. Smyth, *What Large Language Models Know and What People Think They Know*, in *Nature Machine Intelligence*, vol. 7, 2, 2025, pp. 221-231; H. Naveed, A. U. Khan, S. Qiu, M. Saqib, S. Anwar, M. Usman, ... A. Mian, *A Comprehensive Overview of Large Language Models*, in *ACM Transactions on Intelligent Systems and Technology*, vol. 16, 5, 2025, pp. 1-72.
 101. Il prompt è l'input informativo, testuale o multimodale, inserito dall'utente nella maschera di un sistema di intelligenza artificiale. Le indicazioni contenute nel prompt sono finalizzate a guidare il suo funzionamento, nonché l'elaborazione dei dati e la generazione di output. In dottrina esso viene definito "riga di comando" (G. Sgueo, *La funzione pubblica sintetica. Tre domande su intelligenza artificiale generativa e pubblica amministrazione* in *Rivista Trimestrale di Diritto Pubblico*, 3, 2024, p. 1169 ss).
 102. A. M. Leventi-Peetz, N. Zacharis, *Hallucinations. A Paradigm Shift?*, in *Human Interaction and Emerging Technologies (IHET-FS 2025): Future Systems and Artificial Intelligence Applications*, 76, 2025; J. Fredrikzon, *Rethinking Error: "Hallucinations" and Epistemological Indifference*, in *Critical AI*, vol. 3, 1, 2025.
 103. Specie in considerazione della ormai costante divisione dei *Justice* nella maggioranza di 6 giudici conservatori vs 3 giudici liberal. In dottrina, L. Epstein, *Partisanship "All the Way Down" on the US Supreme Court*, in *Pepperdine Law Review*, 51, 2024, p. 489; N. T. Davis, M. P. Hitt, *Partisan Sorting, Fatalism, and Supreme Court Legitimacy*, in *American Journal of Political Science*, 25 gennaio 2025; M. Turek, *Polarization, Partisanship and Democratic Fragility in the United States of America*, in *Democracy and Its Fragility: Mapping the Unstable Equilibrium*, Routledge, London, 2025.
 104. C. Schindler, A. Rausch, *LLM-Based Design Pattern Detection*, 2, 2025; T. J. Sejnowski,

- ChatGPT and the Future of AI*, MIT Press, 2024.
105. E. Loru, J. Nudo, N. Di Marco, A. Santirocchi, R. Atzeni, M. Cinelli, V. Cestari, C. Rossi-Arnaud, W. Quattrociochi, *The Simulation of Judgment in LLMs*, in *Psychological and Cognitive Sciences*, 2025.
 106. O. Fagun, *The Future of Diversity, Equity and Inclusion in Higher Education in the United States*, in *International Journal of Research and Innovation in Social Science*, 15 marzo 2025, <https://doi.org/10.47772/ijriss.2025.903sedu0088>; S. Gündemir, R. Kanitz, F. Rink, I. Hoever, M. Slepian, *Beneath the Surface: Resistance to Diversity, Equity, and Inclusion (DEI) Initiatives in Organizations*, in *Current Opinion in Psychology*, vol. 60, 2024.
 107. AIAP, *cit.* p. 4.
 108. C. Osborne, *Why Companies “Democratise” Artificial Intelligence: The Case of open-source Software Donations*, 9, 2024.
 109. R. Wolfe, I. Slaughter, B. Han, B. Wen, Y. Yang, L. Rosenblatt, ... B. Howe, *Laboratory-Scale AI: Open-Weight Models Are Competitive with ChatGPT Even in Low-Resource Settings*, in *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency*, 2024, pp. 1199-1210.
 110. M. von Thun, D. Hanley, *Stopping Big Tech from Becoming Big AI: A Roadmap for Using Competition Policy to Keep Artificial Intelligence Open for All*, Open Markets Institute, 2024.
 111. L. Gimpel, *Toward Open-Source AI Systems as Digital Public Goods: Definitions, Hopes and Challenges*, in *New Frontiers in Science in the Era of AI*, Springer Nature Switzerland, Cham, 2024, pp. 129-142; M. Langenkamp, D. N. Yue, *How open-source machine learning software shapes AI*, in *Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society*, 2022, pp. 385-395.
 112. Secondo la definizione della «*open-source Initiative*», un modello di AI open-source è definibile come segue: «*An open-source AI is an AI system made available under terms and in a way that grant the freedoms (derived to Free Software Definitions): use the system for any purpose and without having to ask for permission; study how the system works and inspect its components; modify the system for any purpose, including to change its output; share the system for others to use with or without modifications, for any purpose*» (*Open-source Initiative, The open-source AI Definition*, <https://opensource.org/ai/open-source-ai-definition>). In dottrina, T. Paris, A. Moon, J. L. Guo, *Opening the Scope of Openness in AI*, in *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency*, giugno 2025, pp. 1293-1311).
 113. D. G. Widder, M. Whittaker, S. M. West, *Why “open” AI systems are actually closed, and why this matters*, in *Nature*, vol. 635, 8040, 2024, pp. 827-833.
 114. T. Schrepel, J. Potts, *Measuring the openness of AI foundation models: competition and policy implications*, in *Information & Communications Technology Law*, 5 marzo 2025, pp. 1-26; D. G. Widder, M. Whittaker, S. M. West, *Why “open” AI systems are actually closed, and why this matters*, in *Nature*, vol. 635, 8040, 2024, pp. 827-833.

115. M. von Thun, D. Hanley, *Stopping Big Tech from Becoming Big AI*, cit. 81; A. Liesenfeld, M. Dingemans, *Rethinking Open-source Generative AI: Open-Washing and the EU AI Act*, in *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency*, 2024, pp. 1774-1787.
116. «You will not use the Llama Materials or any output or results of the Llama Materials to improve any other large language model (excluding Llama 2 or derivative works thereof)», <http://ai.meta.com/llama/license>. In dottrina, M. von Thun, D. Hanley, *Stopping Big Tech from Becoming Big AI*, cit.
117. «Additional Commercial Terms. If, on the Llama 2 version release date, the monthly active users of the products or services made available by or for Licensee, or Licensee's affiliates, is greater than 700 million monthly active users in the preceding calendar month, you must request a license from Meta, which Meta may grant to you in its sole discretion, and you are not authorized to exercise any of the rights under this Agreement unless or until Meta otherwise expressly grants you such rights». <http://ai.meta.com/llama/license>. In dottrina, M. von Thun, D. Hanley, *ult. op. loc. cit.*
118. C. Rikap, B. Å. Lundvall, *Big Tech, Knowledge Predation and the Implications for Development*, in *Innovation and Development*, vol. 12, 3, 2022, pp. 389-416.
119. A. Basdevant et al., *Towards a Framework for Openness in Foundation Models: Proceedings from the Columbia Convening on Openness in Artificial Intelligence*, 5, 2024; C. Osborne, *The business of open-sourcing artificial intelligence: commercial interests and collaboration dynamics in machine learning developer communities*, tesi di dottorato, University of Oxford, 2025.
120. D. Blumenthal, *The Trump Administration's Recent Policy Proposals*, cit.
121. Si veda *supra*, par. 2. In dottrina, M. Sloane, E. Wüllhorst, A systematic review of regulatory strategies and transparency mandates in AI regulation in Europe, the United States, and Canada, in «*Data & Policy*», 7, 2025.
122. I. Mainardi, *Change management: artificial intelligence (AI) at the service of public administrations*, in *AI & Society*, vol. 40, 5, 2025, pp. 3953-3981.
123. M. Al-kfairy, *Strategic integration of generative AI in organizational settings: Applications, challenges and adoption requirements*, in *IEEE Engineering Management Review*, vol. 53, 2025, p. 80 ss.
124. D. Blumenthal, *The Trump Administration's Recent Policy Proposals*, cit.; M. Ebers, *Truly risk-based regulation of artificial intelligence: how to implement the EU's AI Act*, in *European Journal of Risk Regulation*, vol. 16, 2, 2025, pp. 684-703.
125. A. Galen, R. Schmidt, *The Emergence of an Object of Regulatory Concern: The European Union's Artificial Intelligence Act*, in *Santa Clara Journal of International Law*, vol. 23, 2, 2025, p. 24 ss.
126. Le "sandbox" (o "spazi di sperimentazione normativa per l'IA" come vengono definite dal Regolamento 1689/2024, cit.) sono «*Gli obiettivi degli spazi di sperimentazione normativa per l'IA dovrebbero essere la promozione dell'innovazione in materia di IA, mediante la creazione di un ambiente controllato di sperimentazione e prova nella fase di*

- sviluppo e pre-commercializzazione al fine di garantire la conformità dei sistemi di IA innovativi al presente regolamento e ad altre pertinenti disposizioni di diritto dell'Unione e nazionale. Inoltre, gli spazi di sperimentazione normativa per l'IA dovrebbero avere come obiettivo il rafforzamento della certezza del diritto per gli innovatori e della sorveglianza e della comprensione da parte delle autorità competenti delle opportunità, dei rischi emergenti e degli impatti dell'uso dell'IA, l'agevolazione dell'apprendimento normativo per le autorità e le imprese, anche in vista del futuro adeguamento del quadro giuridico, il sostegno alla cooperazione e la condivisione delle migliori pratiche con le autorità coinvolte nello spazio di sperimentazione normativa per l'IA».* In dottrina, Á. Badinszky, *Regulating the Most Disruptive Technology - Understanding Why AI Should Be Sandboxed*, in *ELTE LJ*,1, 2025, p. 111 ss.
127. E. Perrone, “Regulatory Sandboxes”. *Spazi di sperimentazione normativa per l'intelligenza artificiale*, in *MediaLaws* 1, 2025, pp. 237-269; E. Cirone, *Gli spazi di sperimentazione normativa nell'Unione europea: regolamentare l'innovazione tra principi e prassi applicative*, in *Rivista italiana di informatica e diritto*, 1, 2025, pp. 257-278; F. Francesca, *L'istituto giuridico delle “regulatory sandboxes” tra diritto, protezione dei dati e intelligenza artificiale*, in *Cyberspazio e Diritto*, 1, 2025, pp. 161-170; V. Vinci, S. Ranchordas, *Regulatory sandboxes and innovation-friendly regulation: between collaboration and capture*, in *Italian Journal of Public Law*, 1, 2024, pp. 107-139.
128. Ai sensi dell'art. 60 del Regolamento UE 1689/2024, cit. In dottrina, E. Cirone, *Gli spazi di sperimentazione normativa nell'Unione europea: regolamentare l'innovazione tra principi e prassi applicative*, in *Rivista italiana di informatica e diritto*, 1, 2025, p. 22.
129. W. Riggs, H. Cornet, *Autonomous Vehicles and Public Transit Incentives: A Case Study of Waymo's Pilot Transit Credit Program in the San Francisco Bay Area*, 2025, <https://osf.io/g2r6v/download>.
130. Per quanto riguarda il progetto pilota con cui Waymo sta sperimentando i suoi taxi automatizzati, esso è stato autorizzato principalmente dalle autorità californiane quali la Public Utilities Commission of the State of California e poi da quelle locali di San Francisco e Los Angeles in California (L. Di Lillo, T. Gode, X. Zhou, M. Atzei, R. Chen, T. Victor, *Comparative Safety Performance of Autonomous and Human Drivers: A Real-World Case Study of the Waymo Driver*, in *Helijon*, 10, 2024; W. Hubbard, *Drivers of Effective Laws for Automated Vehicles*, in *Villanova Law Review*, 70, 2025, p. 115; I. Mehra, *AI-Driven Autonomous Vehicles: Safety, Ethics, and Regulatory Challenges*, in *Journal of Science, Technology and Engineering Research*, 2, 2024, pp. 18-31; K. Tiwari, S. Choudhary, *Autonomous Vehicles and Ethical AI: Legal and Safety Considerations*, in *International Journal of Sciences and Innovation Engineering*, 6, 2025, pp. 83-98.
131. A questo proposito, l'AIAP raccomanda di istituire sandbox normativi e centri di eccellenza per l'intelligenza artificiale (IA) a livello nazionale, nei quali ricercatori, startup e imprese consolidate possano sperimentare soluzioni condividendo dati e risultati. Tali iniziative sarebbero supportate da agenzie di regolazione come la Food and Drug Administration (FDA) e la Securities and Exchange Commission (SEC), nonché dal

- Department of Commerce (DOC) attraverso le attività di valutazione del National Institute of Standards and Technology (NIST). Il NIST dovrebbe inoltre promuovere progetti specifici per settore (sanità, energia, agricoltura) al fine di coinvolgere attori pubblici, privati e accademici nella definizione di standard nazionali e nella misurazione dell'impatto dell'IA sulla produttività. In ambito sicurezza, il Department of Defense (DOD), insieme all'Office of the Director of National Intelligence (ODNI), dovrebbe aggiornare periodicamente le valutazioni congiunte sul livello di adozione dell'IA negli Stati Uniti, nei Paesi concorrenti e nelle istituzioni di sicurezza degli avversari, così da adeguare le proprie strategie. Infine, l'Intelligence Community (IC), il Department of Energy (DOE), il DOC tramite il Center for Artificial Intelligence and Strategic Innovation (CAISI), il National Security Council (NSC) e l'Office of Science and Technology Policy (OSTP) dovrebbero collaborare nella raccolta e diffusione di informazioni sui progetti esteri di IA con implicazioni per la sicurezza nazionale.
132. P. Carvao, S. Jeloka, M. Yashiro, *The People Have Spoken: The Tech Industry, Civil Society, and the U.S. Artificial Intelligence Action Plan*, 2 giugno 2025, <https://ssrn.com/abstract=5278764>.
 133. N. Oliveri, *Imaginary Fantasies of Robotic Humanities and AI in Fictional Contexts*, in *The Ethics of Artificial Intelligence*, 5, 2025, pp. 1-25; J. Rhee, *AI in American Literature, in Oxford Research Encyclopedia of Literature*, 20 maggio 2025, <https://oxfordre.com/literature/view/10.1093/acrefore/9780190201098.001.0001/acrefore9780190201098-e-1505>; M. Punt, *Artificial Intelligence and the Technological Imaginary*, in *Leonardo*, 24 gennaio 2025, https://doi.org/10.1162/leon_a_0267.
 134. K. Einola, V. Khoreva, J. Tienari, *A colleague named Max: A critical inquiry into affects when an anthropomorphised AI (ro)bot enters the workplace*, in *Human Relations*, 77, 2023, pp. 1620-1649, <https://doi.org/10.1177/00187267231206328>; A. Zirar, S. Ali, N. Islam, *Worker and workplace Artificial Intelligence (AI) coexistence: Emerging themes and research agenda*, in *Technovation*, 124, 2023, <https://doi.org/10.1016/j.technovation.2023.102747>.
 135. S. Zuboff, *In the Age of the Smart Machine: The Future of Work and Power*, New York, Basic Books, 1988.
 136. M. N. O. Sadiku, A. J. Ajayi-Majebi, P. O. Adebo, *Offshore Manufacturing*, in *Emerging Technologies in Manufacturing*, Springer, Cham, 2023, https://doi.org/10.1007/978-3-031-23156-8_16.
 137. «*Advancing Artificial Intelligence Education for American Youth*» emanato il 23 aprile 2025. In dottrina, L. Loble, K. Stephens, *Taming the AI tools – education first, technology second: Artificial Intelligence and education*, in *Theory Into Practice*, Special Issue, vol. 64, 4, 2025, pp. 369-373.
 138. «*Preparing Americans for High-Paying Skilled Trade Jobs of the Future*» emanato il 23 aprile 2025.
 139. Si tratta dell'area di innovazione tecnologica inerente il c.d. "Internet of things" (IoT), il quale si riferisce a un'infrastruttura nella quale una pluralità di sensori è destinata alla

- raccolta, elaborazione e conservazione locale dei dati, nonché alla interazione reciproca tra i dispositivi stessi, sia a breve distanza – mediante l'utilizzo di tecnologie a radiofrequenza (quali RFID, Bluetooth, ecc.) – sia attraverso una rete di comunicazione elettronica. I dispositivi coinvolti non comprendono unicamente computer o smartphone in senso tradizionale, ma anche oggetti di uso quotidiano (“things”), quali dispositivi indossabili, apparecchi di domotica, strumenti di geolocalizzazione e dispositivi per la navigazione assistita. L'IoT designa, pertanto, un'evoluzione ulteriore della rete Internet, derivante dall'interconnessione di oggetti fisici. Tali oggetti possono essere dotati di un identificatore univoco (ad esempio, un numero di serie), riconoscibile anche mediante radiofrequenza. Tuttavia, l'identificazione di tali oggetti può essere effettuata anche senza il ricorso a etichette elettroniche a radiofrequenza, attraverso la combinazione di sensori e procedure automatiche di riconoscimento, quali, a titolo esemplificativo, la lettura di un codice a barre eseguita tramite un telefono mobile connesso a Internet (Sia consentito rinviare a E. Falletti, *Could Wearable Technology Transform the Traditional Concept of Habeas Corpus?*, n. 2937619, 2017, disponibile su SSRN. Più recentemente, R. Mishra, A. Mishra, *Current Research on Internet of Things (IoT) Security Protocols: A Survey*, in *Computers & Security*, vol. 151, 2025).
140. S. Schmid, T. Riebe, C. Reuter, *Dual-use and trustworthy? A mixed methods analysis of AI diffusion between civilian and defense R&D*, in *Science and Engineering Ethics*, vol. 28, 2, 2022, p. 12; A. Brenneis, *Assessing dual use risks in AI research: necessity, challenges and mitigation strategies*, in *Research Ethics*, vol. 21, 2, 2025, pp. 302-330.
141. S. Daniele, *Ontologies for the Reconfiguration of Domestic Living Environments: A Systematic Literature Review*, in *Information*, vol. 16, 9, 2025, p. 752.
142. D. Patel, H. Castro, *Hospital to Home: Bridging the Gap with Personalized Medicine*, in *Digital Health*, Academic Press, 2025, pp. 143-169.
143. A. Pilotto, C. Massone, G. Iaccarino, A. Genazzani, C. Trompetto, G. Arabia, ... R. Custereri, *A Digital-Health Program Based on Comprehensive Geriatric Assessment for the Management of Older People at Their Home: Final Recommendations from the MULTIPLAT_AGE Network Project*, in *Healthcare*, vol. 13, 10, 2025, p. 1105, MDPI.
144. *Supra* § 1.
145. M. Marsili, *Emerging and Disruptive Technologies: Strategic Implications and Ethical Challenges of Dual-Use Innovations*, in *Strategic Leadership Journal. Challenges for Geopolitics and Organizational Development*, vol. 1, 2025, pp. 57-71; H. O. Khogali, S. Mekid, *Intricate and Multifaceted Socio-Ethical Dilemmas Facing the Development of Drone Technology: A Qualitative Exploration*, in *AI*, vol. 6, 7, 2025, p. 155.
146. Si consenta il rinvio a E. Falletti, C. Gallese, *Ethical and Legal Limits to the Diffusion of Self-Produced Autonomous Weapons*, in *Proceedings of the 4th European Conference on the Impact of Artificial Intelligence and Robotics*, Academic Conferences and Publishing International, 2022, pp. 22-28, doi: <https://doi.org/10.34190/eciair.4.1.82>; J. Sliwa, *Internet of Military Things and Weaponized AI: Technology in the Age of Conflict*, in *Internet of Things A to Z: Technologies and Applications*, in Qusay F. Hassan, *Internet of*

- Things A to Z: Technologies and Applications, 2nd Edition*, Wiley-IEEE Press, 2025, pp. 465-494.
147. AIAP, cit. p. 7. Tra le azioni raccomandate vi è il sostegno, tramite DOD, DOC, DOE, NSF e di altre agenzie, dello sviluppo e la diffusione delle tecnologie manifatturiere di base e transnazionali, ricorrendo a strumenti quali Small Business Innovation Research, Small Business Technology Transfer, programmi CHIPS (Il CHIPS, acronimo di «*Creating Helpful Incentives to Produce Semiconductors*») and Science Act è uno statuto federale degli Stati Uniti emanato dal 117° Congresso degli Stati Uniti e firmato dal presidente Joe Biden il 9 agosto 2022. Invece, la divisione B è la legge su ricerca e sviluppo, concorrenza e innovazione; la divisione C è la legge sul finanziamento della sicurezza della Corte suprema del 2022.
 148. Le azioni politiche raccomandate dall'AIAP riguardano nuovamente l'intervento dei NSF, il DOE, il NIST presso il DOC e altri partner federali, investire in laboratori automatizzati basati su cloud per un'ampia gamma di campi scientifici, tra cui ingegneria, scienza dei materiali, chimica, biologia e neuroscienze, realizzati, quando opportuno, dal settore privato, dalle agenzie federali e dalle istituzioni di ricerca in coordinamento e collaborazione con i Laboratori Nazionali del DOE. Utilizzare accordi a lungo termine per sostenere *Focused-Research Organizations* o altre entità simili che impieghino l'AI e altre tecnologie emergenti per conseguire progressi scientifici fondamentali.
 149. «*Basic science today is often a labor-intensive process; the AI era will require more scientific and engineering research to transform theories into industrial-scale enterprises. This, in turn, will necessitate new infrastructure and support of new kinds of scientific organizations*» (AIAP, cit. p. 8).
 150. In particolare si sottolinea la richiesta ai ricercatori finanziati con fondi federali di divulgare dataset non proprietari e non sensibili utilizzati dai modelli di IA durante il corso della ricerca e della sperimentazione.
 151. P. V. Mohanan (a cura di), *Artificial Intelligence and Biological Sciences*, CRC Press, Taylor & Francis Group, 2025, *passim*.
 152. Del pari, il rafforzamento della presunzione di accessibilità e ampliando l'accesso sicuro ai dati federali, così da abbattere barriere e permettere un uso più efficace dell'AI da parte delle agenzie statistiche, garantendo al contempo protezione contro possibili usi impropri. Istituire ambienti di calcolo sicuri per applicazioni di AI con accesso controllato a dati federali riservati (AIAP, cit. p. 12).
 153. Negli Stati Uniti affinché un prodotto dell'ingegno umano (cioè «any new and useful process, machine, manufacture, or composition of matter») possa essere brevettato, e quindi sia patentable subject matter, esso deve presentare i requisiti previsti dal Title 35 of the United States Code. Nello specifico essi sono: novelty (§102), usefulness (§101), enablement (§112), non obviousness and technical accomplishment (§103).
 154. 47 U.S. 303 (1980). L'applicazione della normativa in tema di brevettabilità del vivente è stata oggetto di un importante contenzioso risolto dalla Corte Suprema nel 1980: *Diamond v. Chakrabarty*. Il caso riguardava la coltivazione e lo sviluppo da parte

- dell'ingegnere genetico, ricercatore alle dipendenze della General Electric Ananda M. Chakrabarty, di un batterio della specie *Pseudomonas* genus reso in grado di assorbire il petrolio greggio. Chakrabarty aveva presentato domanda per la concessione di un brevetto presso lo U. S. Patent and Trademarks Office, ma gli era rifiutato poiché il suo batterio, seppur modificato, era un essere vivente e quindi, ad opinione del U.S.P.T.O. non suscettibile di essere brevettato. Chakrabarty proponeva ricorso dapprima presso Board of Patent Appeals and Interferences, dove rimaneva soccombente, ma impugnava di fronte allo United States Court of Customs and Patent Appeals, il quale decideva in suo favore sostenendo il fatto che seppure i microorganismi fossero esseri viventi, ciò non era giuridicamente rilevante ai fini della loro brevettabilità. Di fronte a siffatto risultato Sidney Diamond, nel ruolo di Commissioner of Patents and Trademarks, ricorreva alla Corte Suprema, che deliberava con una maggioranza di cinque giudici contro quattro a favore di Chakrabarty. La Corte statuiva che il microorganismo vivente, modificato per mano umana e per il quale era stata domandata la brevettazione, poteva essere incluso nella definizione di “manufacture” ovvero di “composition of matter” ai sensi del 35 U. S. C. §101.
155. *Bartz v. Anthropic PBC (3:24-cv-05417) District Court, N.D. California*. La causa, avviata da Andrea Bartz e supportata da altri scrittori, si è ampliata dopo l'accusa ad Anthropic di aver scaricato oltre 7 milioni di opere da siti pirata. Il giudice Alsup ha stabilito che l'uso di libri protetti non è illecito in sé, dato l'uso trasformativo prodotto attraverso l'attività di training, ma l'acquisizione illegale sì. Pertanto le parti hanno raggiunto un accordo per l'uso illegale dei materiali protetti da copyright. Anthropic ha accettato un accordo stragiudiziale da 1,5 miliardi di dollari per chiudere una class action intentata da autori che accusavano l'azienda di aver usato copie pirata dei loro libri per addestrare il chatbot Claude. In dottrina, P. Samuelson, *Legally Speaking: Does Using In-Copyright Works as Training Data Infringe?*, in *Communications of the ACM*, forthcoming, *UC Berkeley Public Law Research Paper*, 15 luglio 2025.
156. AIAP, *cit.* p. 9.
157. Il «*Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act*», (conosciuto come TAKE IT DOWN Act) è una legge federale approvata dal 119° Congresso [119th Congress Public Law 12] e firmata dal Presidente Trump il 19 maggio 2025. In dottrina, J. C. Ginsburg, G. W. Austin, *Regulating Deepfakes at Home and Abroad*, in *Columbia Journal of Law & the Arts*, 48, 2025 (forthcoming); A. Mitton, *Deep Fakes, Deeper Consequences: Combating AI Child Pornography by Mandating Sex Offender Registration*, in *International Journal of Law, Ethics and Technology*, 2, 2025; J. Grimmelmann, *Deconstructing the Take It Down Act*, in *Communications of the ACM*, vol. 68, 8, 2025, pp. 28-30.
158. W. Hawkins, B. Mittelstadt, C. Russell, *Deepfakes on Demand: The Rise of Accessible Non-Consensual Deepfake Image Generators*, in *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency*, 2025, pp. 1602-1614.
159. *United States District Court for the District of South Carolina, Spartanburg Division, Does*

- 1-9 v. *Murphy et al*, No. 7:2020cv00947 - Document 288 (D.S.C. 2023). Il fatto riguardava individui non identificati che avevano diffuso video manipolati su vari siti di contenuti per adulti, tra cui Pornhub (Mindgeek) e xHamster (Hammy). Entrambi i siti hanno rimosso i video dopo averne ricevuto notifica, tuttavia, le immagini dei video si sono diffuse su 4Chan e altri siti. Questa sentenza riguarda l'istanza di un preliminary injunction presentata da Pornhub, xHamster e alcuni dei loro fornitori di servizi. Nel processo si dimostra che i video provengono da terzi e che né MindGeek né Hammy siano stati coinvolti nella creazione o nello sviluppo iniziale dei video. <https://law.justia.com/cases/federal/district-courts/south-carolina/scdce/7:2020cv00947/256074/288>.
160. La Corte osserva che l'attività dei siti di condivisione è oggi molto diversa rispetto all'adozione della Sect. 230 e suggerisce che spetti al Congresso rivalutare doveri e responsabilità di tali piattaforme. Tuttavia la Corte incorre in un errore sorprendente poiché il Congresso è già intervenuto e il 19 maggio 2025 il Presidente Trump ha firmato il *Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act*, conosciuto come TAKE IT DOWN Act, neppure citato da questo provvedimento emanato il 3 settembre 2025.
161. S. A. Saltzburg, *Circumstantial Authentication of Video Evidence*, in *Criminal Justice*, vol. 40, 1), 2025, pp. 56-58.
162. K. Kasali, *Optimizing Workforce Efficiency in the United States (U.S.) Federal Sector: The Role of Predictive Analytics and AI in Human Resource (HR) Decision-Making*, in *International Journal of Research and Scientific Innovation*, 2025, <https://doi.org/10.51244/ijrsi.2025.12030082>.
163. D. Vidhate, K. Raut, M. Ahuchogu, D. Vinod, M., P. Thodkar, S. Daida, *Exploring the Role of Generative AI in Procurement, Contract Lifecycle Management, Supplier Risk Assessment, and Supply Chain Planning*, in *Power System Technology*, 1, 2025, <https://doi.org/10.52783/pst.1648>.
164. AIAP, *cit.* pp. 14-15.
165. L. Xin, *open-source Marketing Strategy of AI Companies from the Perspective of the Knowledge Gap Hypothesis Research – On the Case of DeepSeek*, in *Advances in Economics, Management and Political Sciences*, 2025, <https://doi.org/10.54254/2754-1169/2025.22109>; D. R. Russel, E. Ratté, *Defense or Diffusion? open-source AI*, in *US-China Competition*, 2025.
166. Emanato dal Presidente Trump in ossequio degli adempimenti posti dalla sentenza della Corte Suprema "TikTok v. Garland". In dottrina, S. Raman, J. Jaffer, C. Newman, K. Ruane, *TikTok Takedown: National Security & Speech Implications of Social Media*, in *National Security Law Journal*, 12, 2024, p. 129.
167. Si consenta il rinvio a E. Falletti, *Sovranità digitale, tutela della sicurezza nazionale e libertà di manifestazione del pensiero*, *cit.* In dottrina, M. Juned, S. Maryam, S. Salam, R. A. A. Utami, *TikTok's conflict of interest with the US government: between big data security and economics (2017-2023)* in *European Journal of Communication and Media Studies*,

- vol. 2, 4, 2023, pp. 1-8; A. Chander, P. Schwartz, *The President's Authority Over Cross-Border Data Flows*, in *172 U. Pa. L. Rev.*, 7, 2024, p. 1989 ss.
168. Executive Order n. 14352. Da un lato, l'accordo prevede che le operazioni di trattamento effettuate all'estero dei dati dei cittadini statunitensi da Tiktok, cioè un avversario straniero, cessino. Secondo gli osservatori, l'accordo presenta criticità importanti ma pure rilevanti benefici. Tra i primi va segnalata la difficoltà di eliminare completamente le influenze ovvero il flusso dei dati verso la precedente società madre, cioè una compagnia avversaria straniera, indipendentemente dalla percentuale della proprietà della piattaforma in mani americane. La ristrutturazione concordata presenta aspetti critici, in particolare la separazione degli algoritmi e il loro nuovo settaggio, che potrebbero interrompere la fruizione del servizio. Da un punto di vista più strettamente costituzionale sembra essere problematico il riconoscimento esclusivo in capo alla Presidenza dell'applicazione della normativa, impedendo quindi iniziative legali statali ovvero private. Dall'altro lato, si stabilisce che il controllo e la proprietà della piattaforma sia trasferita a una joint venture la cui maggioranza sia in mano americana. Inoltre, siffatto accordo prevede meccanismi di tutela della sicurezza nazionale (statunitense), tra cui l'archiviazione dei dati in un'infrastruttura cloud gestita negli Stati Uniti, il divieto di rapporti operativi come accordi di condivisione dei dati e l'obbligo di monitoraggio degli algoritmi da parte di partner di sicurezza fidati. Siffatto accordo raggiungerebbe un equilibrio che consentirebbe agli utenti americani, tanto i singoli "content creator", quanto le imprese, di mantenere le loro attività, bilanciando questi interessi economici con la tutela della sicurezza nazionale. Le parti hanno 120 giorni di tempo per effettuare la cessione qualificata, mantenendo però la piena autorità presidenziale sull'applicazione dell'accordo stesso.
169. S. Bennett, A. Fernandez Pales et al., *The State of Energy Innovation*, International Energy Agency, Paris, 2025, p. 151 ss.
170. Y. Malkova, *Artificial Intelligence and Sustainable Power*, in *The Sustainable Power Grid*, Elsevier, 2025, pp. 43-58; I. Satpathy, D. Chakravarty, V. Jain, B. C. M. Patnaik, *Towards Sustainable Intelligence: Enhancing Cloud Infrastructure Through Green Computing and AI-Driven Engineering*, in K. Kishor, S. Kadry *Advancements in Cloud-Based Intelligent Informative Engineering*, IGI Global Scientific Publishing, 2025, pp. 203-228;
171. In prospettiva generale, si veda: A. Coll, *Redefining Efficiency in the Doge Era: The Value of Evidence-Based Policymaking in Federal Agencies*, n. 5433877, 8 maggio 2025, disponibile su SSRN.
172. D. Riesel, *Environmental Enforcement: Civil and Criminal*, Law Journal Press, 2025; H. Besse, D. Rojas-Rueda, *Environmental Justice Mapping Tools in the United States: A Review of National and State Tools*, in *Science of The Total Environment*, vol. 962, 2025, p. 178449.
173. Pertanto, secondo l'AIAP, occorrerebbe semplificare i processi autorizzativi, senza comprometterne la sicurezza, e proteggere le infrastrutture da tecnologie straniere potenzialmente ostili. Le azioni raccomandate riguardano l'introduzione nuove eccezioni

- per i data center a basso impatto ambientale, estendere il processo previsto dal *Fixing America's Surface Transportation Act 2015* a tutti i modelli energetici e di data center idonei. Valutare un permesso nazionale, ai sensi della *Clean Water Act Section 404*, semplificato e proporzionato ai moderni data center di AI. Accelerare i permessi riducendo le complessità previste da leggi come *Clean Air Act* e *Comprehensive Environmental Response Act*. Rendere disponibili terreni federali per data center e infrastrutture energetiche, con mappatura dei siti adatti a grandi sviluppi. Rafforzare la sicurezza, imponendo che lo stack computazionale dell'IA nazionale si basi su prodotti americani e infrastrutture ICT prive di tecnologie di avversari esteri (AIAP, cit. p. 14 ss.).
174. A. Madaan, N. Tandon, P. Gupta, S. Hallinan, L. Gao, S. Wiegrefe, ... P. Clark, *Self-Refine: Iterative Refinement with Self-Feedback*, in *Advances in Neural Information Processing Systems*, 36, 2023, pp. 46534-46594; E. Carson, N. J. Higham, *A New Analysis of Iterative Refinement and Its Application to Accurate Solution of Ill-Conditioned Sparse Linear Systems*, in *SIAM Journal on Scientific Computing*, vol. 39, 6, 2017, pp. A2834-A2856.
 175. *Supra*, §3. A. M. Leventi-Peetz, N. Zacharis, *Hallucinations*, cit.; J. Fredrikzon, *Rethinking Error*, cit.; N. Chakraborty, M. Ornik, K. Driggs-Campbell, *Hallucination Detection in Foundation Models for Decision-Making: A Flexible Definition and Review of the State of the Art*, in *ACM Computing Surveys*, vol. 57, 7, 2025, pp. 1-35.
 176. C. Rathkopf, *Hallucination, Reliability, and the Role of Generative AI in Science*, 1, 2025, p. 8526; Y. Song, J. Sohl-Dickstein, D. P. Kingma, A. Kumar, S. Ermon, B. Poole, *Score-Based Generative Modeling Through Stochastic Differential Equations*, in *Proceedings of the International Conference on Learning Representations*, (ICLR), 2021.
 177. I VAE si basano su un framework probabilistico flessibile, robusto in caso di scarsità di dati e compatibile con altri modelli basati sul deep learning per la gestione di dati multimodali. La struttura generativa profonda dei VAE aiuta a eseguire l'inferenza bayesiana in modo efficiente (S. Liang, Z. Pan, W. Liu, J. Yin, M. De Rijke, *A Survey on Variational Autoencoders in Recommender Systems*, in *ACM Computing Surveys*, 56, 2024, pp. 1-40, <https://doi.org/10.1145/3663364>).
 178. Le reti generative avversarie (GAN) sono un tipo di tecniche di deep learning che generano immagini, video e altri tipi di contenuti realistici (J. Gui, Z. Sun, Y. Wen, D. Tao, J. Ye, *A Review on Generative Adversarial Networks: Algorithms, Theory, and Applications*, in *IEEE Transactions on Knowledge and Data Engineering*, 35, 2020, pp. 3313-3332, <https://doi.org/10.1109/TKDE.2021.3130191>).
 179. A questo proposito, *l'ALAP raccomanda di creare nuovi standard tecnici per i data center ad alta sicurezza, guidati dal Department of Defence (DoD), Intelligence Community (IC), National Security Council (NSC) e NIST del Dipartimento del Commercio, in collaborazione con industria e centri di ricerca federali. Le agenzie dovrebbero adottare ambienti di calcolo classificati, capaci di gestire carichi di lavoro IA scalabili, proteggendo i dati sensibili e garantendo affidabilità operativa.*
 180. *Executive Order 14306 del 6 giugno 2025, Sustaining Select Efforts To Strengthen the*

- Nation's Cybersecurity and Amending Executive Order 13694 e Executive Order 14144.*
181. M. Lévesque, *Full-Stack AI Governance*, disponibile su SSRN, 2025, n. 5270641.
 182. A. Taivalsaari, T. Mikkonen, C. Pautasso, K. Systä, *Full Stack Is Not What It Used to Be*, in *International Conference on Web Engineering*, Cham: Springer International Publishing, maggio 2021, pp. 363-371.
 183. In tale ottica, si propone l'istituzione, presso il Dipartimento del Commercio (Department of Commerce, DOC), di un programma di raccolta e selezione di progetti industriali volti alla realizzazione di pacchetti integrati di tecnologie IA da esportare sotto la supervisione congiunta del DOC, del Dipartimento di Stato (DOS), della U.S. Trade and Development Agency, della Export-Import Bank e della International Development Finance Corporation. Tale coordinamento interistituzionale mira ad assicurare la piena conformità di ogni esportazione agli standard di sicurezza e controllo propri della legislazione federale in materia di commercio internazionale e difesa nazionale (AIAP, *cit.* p. 20).
 184. H. Roberts, J. Cows, E. Hine, F. Mazzi, A. Tsamados, M. Taddeo, L. Floridi, *Achieving a "Good AI Society": Comparing the Aims and Progress of the EU and the US*, in *Science and Engineering Ethics*, 27, 2021, p. 67 ss., doi: 10.1007/s11948-021-00340-7; V. Birchfield, *From Roadmap to Regulation: Will There Be a Transatlantic Approach to Governing Artificial Intelligence?*, in *Journal of European Integration*, vol. 46, 2024, pp. 1053-1071, doi: 10.1080/07036337.2024.2407571; M. Ebers, *Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU's AI Act*, 19 giugno 2024, disponibile in SSRN, doi: 10.1017/err.2024.78.
 185. In particolare presso l'International Telecommunication Union (ITU) e l'Internet Corporation for Assigned Names and Numbers (ICANN) attraverso una più incisiva partecipazione diplomatica e tecnica, il governo statunitense intende promuovere modelli regolatori ispirati ai principi di apertura, innovazione e tutela delle libertà fondamentali, in opposizione a paradigmi restrittivi o di matrice autoritaria. Tale impostazione riflette una visione giuridico-istituzionale dell'IA quale infrastruttura globale soggetta a regole comuni, in cui la legittimazione degli standard tecnici diviene veicolo di influenza normativa e strumento di soft power. (AIAP, *cit.*, p. 20). In dottrina, in senso critico, M. L. Mueller, *Declaring Independence in Cyberspace: Internet Self-Governance and the End of US Control of ICANN*, MIT Press, Cambridge, 2025, *passim*.
 186. Sul punto, l'AIAP dispone che il Dipartimento del Commercio, di concerto con l'*Office of Science and Technology Policy (OSTP)*, il *National Security Council (NSC)* e l'industria privata, sia chiamato a implementare sistemi di tracciabilità e verifica dei chip e dei sottosistemi tecnologici, al fine di impedire la deviazione di componenti sensibili verso Paesi o attori non autorizzati (AIAP, *cit.*, p. 21).
 187. In dottrina, A. King, *AI, Automation, and War: The Rise of a Military-Tech Complex*, Princeton University Press, 2025, pp. 60 ss.
 188. Sotto la direzione del Dipartimento di Stato, in coordinamento con DOC, Dipartimento della Difesa (DOD) e Dipartimento dell'Energia (DOE), è previsto lo sviluppo di un piano strategico volto a consolidare un'alleanza globale per la sicurezza dell'IA, che includa

- controlli comuni sulle esportazioni, standard condivisi e regole di interoperabilità (AIAP, *cit.*, p. 21).
189. Il governo federale, tramite il Chief Artificial Intelligence and Security Initiative (CAISI) istituito presso il DOC, è tenuto a condurre analisi periodiche dei sistemi di frontiera per identificare eventuali vulnerabilità suscettibili di compromettere la sicurezza nazionale, comprese le minacce cibernetiche e i rischi connessi alle tecnologie CBRNE (chimiche, biologiche, radiologiche, nucleari ed esplosive) (AIAP, *cit.*, p. 22).
190. A. Iliadis, A. Acker, *The seer and the seen: Surveying Palantir's surveillance platform*, in *The Information Society*, vol. 38, 5, 2022,, pp. 334-363; B. Wright, J. Payne, M. Steckman, S. Stevson, *Palantir: A visualization platform for real-world analysis*, in *2009 IEEE Symposium on Visual Analytics Science and Technology*, 2009, pp. 249-250.
191. Bundesverfassungsgericht, Erster Senat, (Germania) 16.2.2023, 1 BvR 1547/19, 1 BvR 2634/20, Pres. Harbarth.
192. L. Algeri, *Intelligenza artificiale e polizia predittiva*, in *Diritto penale e processo*, 6, 2021, pp. 724-734; S. Egbert, E. Esposito, *Algorithmic crime prevention. From abstract police to precision policing*, in *Policing and Society*, vol. 34, 6, 2024, pp. 521-534; K. Blount, *Using artificial intelligence to prevent crime: implications for due process and criminal justice*, in *AI & Society*, vol. 39, 1, 2024, pp. 359-368; R. Favino, N. Conte, M. A. De, M. E. Garcia, E. Montanari, A. Paganini, ... e C. E. Sfalagkiaris, *Emerging risks and opportunities for EU internal security stemming from new technologies*, Researchgate, 2025.
193. H. Haddad, *Redefining Biological Weapons in the Evolving AI, CRISPR, and Biotbreath Landscape*, in *Ethics, Medicine and Public Health*, vol. 33, 2025, p. 101176.
194. L'OSTP è incaricato di promuovere la creazione di una piattaforma di condivisione dei dati tra istituzioni pubbliche e private, finalizzata a prevenire abusi e individuare tempestivamente comportamenti fraudolenti (AIAP, *cit.* p. 23).
195. A. Chelikavada, C. C. Bennett, *Examining the Relationship between Scientific Publishing Activity and Hype-Driven Financial Bubbles: A Comparison of the Dot-Com and AI Eras*, arXiv preprint arXiv:2509.11982, 2025; H. Taherdoost, *From hype to bubble: a historical analysis of technology trends and the case for artificial intelligence*, in *Future Digital Technologies and Artificial Intelligence*, 1, 2025; A. S. George, *The Algorithmic Boom: Comparing AI's Trajectory to the Dot-Com Revolution and Its Divergent Future*, in *Partners Universal Innovative Research Publication*, vol., 3, 3, 2025, pp. 58-73.