L'IRCOCERVO
PRIMA RIVISTA ELETTRONICA ITALIANA DI METODOLOGIA GIURIDICA - TEORIA GENERALE DEL DIRITTO E DOTTRINA DELLO STATO
FIRST ITALIAN DIGITAL JOURNAL OF LEGAL METHODOLOGY - GENERAL THEORY OF LAW AND DOCTRINE OF THE STATE

Algorithmic Recommendation ed *Artificial Intelligence* nell'esperienza statunitense ed europea fra esigenze strategiche e tutela dei diritti fondamentali*

Laura Fabiano

Università degli Studi di Bari Aldo Moro

Abstract: **Algorithmic Recommendation and Artificial Intelligence in the United States and European Union: Balancing Strategic Goals and Fundamental Rights**
The regulatory approaches taken by the US and Europe in the field of digital law frequently differ. However, there seems to have been a recent convergence on the topic of artificial intelligence. In actuality, the priorities still differ.
This disparity reflects the economic structures of the two regions. The United States must maintain its lead in the digital market. Europe still records a partial technological delay.
The difference also lies in the cultural diversity between Europe and the United States: while the United States typically prioritizes the nation's economic growth, Europe has historically paid more attention to the guarantee of fundamental rights.
The United States has recently been forced to pay attention to the issue of defending the rights of the American people in part due to the growth of Chinese competition.

Keywords: Algorithmic Recommendation, Artificial Intelligence, Commercial Competition, Fundamental Rights, National Security.

Sommario: 1. Condizionamento algoritmico e intelligenza artificiale nell'evoluzione normativa del digitale in Europa e Stati Uniti d'America: osservazioni preliminari – 2. L'impianto *rights-based* e di "regolazione sociale" nella disciplina sull'AI in ambito europeo – 3. La normativa e la giurisprudenza sull'AI e sulla raccomandazione algoritmica nell'esperienza USA fra strategie di tutela della *leadership* nel mercato e problemi di sicurezza internazionale – 4. La parabola cinese e il possibile ravvicinamento della strategia statunitense all'impostazione strategica europea.

1. Condizionamento algoritmico e intelligenza artificiale nell'evoluzione normativa del digitale in Europa e Stati Uniti d'America: osservazioni preliminari

* Il presente contributo si inquadra in una linea di ricerca del progetto competitivo *Horizon Europe Seeds* finanziato dall'Università degli Studi di Bari Aldo Moro, su "Libertà di opinione, nuove tecnologie e formazione del consenso".

Il presente contributo intende indagare il tema dell'evoluzione normativa in materia di ecosistema digitale (con particolare riguardo alle questioni concernenti il condizionamento algoritmico e l'intelligenza artificiale) nelle esperienze europea e statunitense individuando eventuali similitudini e differenze. Obiettivo finale dello scritto è valutare come alla base di alcune scelte normative assunte in tali contesti ordinamentali vi sia tanto una differenza culturale di fondo quanto ragioni economiche e politico-strategiche collegate, non ultimo, alla concorrenza sui mercati internazionali di altri colossi mondiali quali la Cina.

Sia nell'esperienza statunitense sia nel contesto europeo l'approccio iniziale alla disciplina dell'ecosistema digitale si è proposto con tratti tendenzialmente liberistici in quanto la finalità normativa maggiormente sentita era favorire la libera circolazione delle comunicazioni e la promozione dei servizi della società dell'informazione eliminando gli ostacoli allo sviluppo del commercio elettronico.

Tale orientamento risulta certamente collegato ad un'iniziale aspettativa nutrita nei confronti delle tecnologie informatiche che si andavano affermando connessa all'idea che i media collegati alla tecnologia della rete Internet fossero dotati di un importante potenziale migliorativo della vita individuale e collettiva umana venendo interpretati come un possibile strumento funzionale all'incremento della qualità democratica mondiale e di maggiore possibilità di espressione del pensiero individuale[1] oltre che di sviluppo economico globale.

Tale connotazione si rintraccia, guardando all'esperienza statunitense, nell'adozione da parte del Congresso, nel 1996, della notissima sezione 230 del *Title 47* dello *Us Code* (*Communication Decency Act*) la quale sanciva la completa deresponsabilizzazione degli *Internet provider* per i contenuti caricati da terzi attraverso la previsione della c.d. clausola del buon samaritano[2]. Altresì, un impianto normativo non molto dissimile è rinvenibile nella parallela esperienza europea: in tale ambito la disciplina di riferimento è stata per anni la direttiva n. 2000/31/Ce[3] (la c.d. direttiva *e-commerce*) la quale, anch'essa, sanciva sostanzialmente il c.d. dogma della irresponsabilità degli intermediari digitali.

[1] Ancora nel 2010 Larry Diamond, professore di sociologia di Stanford, in un articolo intitolato "Liberation Tecnology", in *Journal of Democracy*, 21 (2010), n. 3, pp. 69-83 (consultabile all'url www.journalofdemocracy.org/articles/liberation-technology/) sosteneva con energia le virtù socializzanti del *web* (anche in termini politici). Sul tema in generale si rinvia G. Gometz, *Democrazia elettronica. Teoria e tecniche*, Edizioni ETS, Pisa, 2017.

[2] La tendenza a garantire l'irresponsabilità del *provider* per contenuti caricati da terzi è ribadita anche dal *Digital Millennium Copyright Act* del 1996. Sul tema cfr. ampiamente M. Bassini, *Internet e libertà di espressione*, Aracne, Roma, 2019; R. Imperadori, "La responsabilità dell'Internet Service Provider per violazione del diritto d'autore: un'analisi comparata", in *Trento Law and Technology group*, (2014), Student paper n. 21 (reperibile all'url: www.lawtech.jus.unitn.it).

[3] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico").

Nondimeno, con la progressiva evidenziazione delle peculiarità tecniche connesse al contesto informatico, con riguardo in particolare alle tecnologie informatiche delle telecomunicazioni (ICT), e alle loro potenzialità predittive e manipolative[4], si è rivelato necessario nel tempo normare con maggiore rigore l'attività algoritmica: l'attenzione del decisore politico si è dunque gradualmente spostata dalla mera garanzia della libertà di azione *on line* alla predisposizione di norme a tutela dell'utente digitale con particolare riferimento alla manipolazione della sua identità e più in generale con riguardo alla c.d. coercizione algoritmica.

Nell'approcciarsi a tali tematiche le scelte europee e statunitensi non hanno seguito tuttavia le medesime strade. Ciò è accaduto certamente, in primo luogo, in considerazione di una diversa tradizione storica che caratterizza tali ambienti giuridici: l'impianto culturale statunitense nasce difatti connotato da forti tratti liberisti e, pur evolvendo in senso democratico, non abbandona mai del tutto la propria origine culturale[5]; in Europa, invece, anche a causa delle traumatiche esperienze storiche del Novecento[6], l'orientamento normativo alla tutela delle garanzie fondamentali individuali è un connotato particolarmente sentito e oramai irretrattabile.

Un secondo ordine di ragioni alla base di tale divergenza riposa in considerazioni di tipo maggiormente geopolitico[7]: difatti, giacché nella lista delle prime dieci società del mondo per capitalizzazione (nel 2023), 7 afferiscono al comparto tecnologico e sono tutte statunitensi (Apple, Microsoft, Alphabet, Amazon, Nvidia, Meta, Tesla)[8], risulta intuitivo comprendere le motivazioni per cui "gli USA hanno una posizione di antica primazia tecnologica da difendere, […] mentre l'Europa ha tuttora un notevole problema di autonomia e sovranità tecnologica, aggravato dall'uscita del Regno Unito dall'Unione"[9].

Tale posizione di primazia, per quanto riguarda gli Stati Uniti, si gioca peraltro nella particolare competizione con la Cina, Paese che si propone come

[4] La raccomandazione algoritmica produce nelle odierne ICT capacità predittive e manipolative: predittive in quanto gli algoritmi, grazie al trattamento di una gran massa di dati (*Big Data*) sono capaci di rivelare relazioni tra scelte, comportamenti, gusti, azioni e, sulla base di tali informazioni, sono in grado di costruire dei modelli di comportamento individuali e collettivi; manipolativi, perché la profilazione algoritmica contribuisce a selezionare i contenuti determinanti per la formazione dell'opinione pubblica. Sul punto cfr. L. Fabiano, "Le potenzialità manipolative della democrazia digitale fra interessi pubblici e poteri privati", in *Diritto dell'Informazione e dell'Informatica*, (2023) n. 4-5, pp. 597 ss.

[5] Sul punto cfr. G. Bognetti, *Lo spirito del costituzionalismo americano*, vol. I, *La Costituzione liberale*, Giappichelli, Torino, 1998; Vol. II, *La Costituzione democratica*, Giappichelli, Torino, 2000.

[6] Cfr. sul tema R. Tarchi, *Patrimonio costituzionale europeo e tutela dei diritti fondamentali*, Giappichelli, Torino, 2015.

[7] Su cui cfr. G. Resta, "Cosa c'è di europeo nella proposta di regolamento Ue sull'Intelligenza artificiale?", in *Diritto dell'Informazione e dell'informatica*, (2022), n. 2, pp. 323 ss.

[8] https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/.

[9] G. Resta, "Cosa c'è di europeo nella proposta di regolamento Ue sull'Intelligenza artificiale?", cit., p. 325.

l'ordinamento che più fortemente concorre per la *leadership* globale in tale ambito.

La crescita tecnologica cinese nel periodo più recente ha subito una battuta d'arresto[10] collegata al contesto non democratico che caratterizza il Paese (nella misura in cui il colosso orientale si è confrontato con difficoltà con la dimensione generativa della tecnologia AI)[11] e tuttavia la concorrenza in ambito informatico digitale della Cina rappresenta per gli Stati Uniti una minaccia non solo in termini commerciali ma anche in relazione ai temi della sicurezza interna.

Ci si riferisce, ad esempio, alla crisi innescatasi negli Stati Uniti in relazione alle tensioni provocate dalla estrema diffusione sul territorio USA della *app* di *social media* conosciuta come TikTok. Questo *social*, che sostanzialmente ospita video in formato breve e offrendoli agli utenti tramite algoritmo, è di proprietà della società tecnologica cinese ByteDance e la sua crescente popolarità tra adolescenti e giovani adulti in America ha suscitato preoccupazioni in relazione alla possibilità che lo stesso possa essere utilizzato per la raccolta di dati e di informazioni degli americani iscritti a tale *social* e, dunque, utilizzato per operazioni di influenza straniera sul territorio statunitense. Ciò in quanto la detta società madre di TikTok, ByteDance, avendo sede in Cina, è soggetta alla legge cinese sull'*intelligence* nazionale (adottata nel 2017) in base alla quale le autorità statali cinesi possono richiedere ai propri cittadini ed alle aziende di fornire dati rilevanti per il loro lavoro di *intelligence*[12].

[10] Il sorpasso statunitense rispetto alla Cina in tema di tecnologia può essere apprezzato già considerando che con riguardo alla medesima statistica appena citata in relazione ai dati del 2022 nella lista delle prime dieci società del mondo per capitalizzazione, 8 appartenevano al comparto tecnologico e di queste 6 erano statunitensi (Apple, Microsoft, Amazon, Alphabet, Facebook, Tesla) e 2 cinesi (Tencent, Alibaba). Cfr. https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/

[11] Ad aprile 2023 la *Cyberspace Administration of China* (Cac), l'ente regolatore della sfera digitale in Cina, ha pubblicato una bozza di legge dal titolo "Misure Amministrative per i Servizi di Intelligenza Artificiale" (il documento originale è reperibile al seguente link: https://www.cac.gov.cn/2023-04/11/c_1682854275475410.htm. Si tratta di una bozza normativa in tema di intelligenza artificiale che, per molti aspetti, ricalca la precedente normativa del 2022 sulla raccomandazione algoritmica ove una delle finalità principali perseguite dal regime cinese si percepiva essere il controllo governativo sui sistemi e la loro eventuale utilizzabilità a fini strategici da parte del partito. Altresì, l'11 ottobre 2023, il *National Information Security Standardization Technical Committee* (un'organizzazione governativa cinese) ha pubblicato una bozza di documento che propone regole dettagliate per determinare se un modello di IA generativa è da considerarsi problematico. Spesso abbreviato in TC260, il detto Comitato agisce consultando i rappresentanti delle aziende, gli accademici e le autorità di regolamentazione per definire le regole del settore tecnologico su questioni che vanno dalla cybersicurezza alla *privacy*, all'infrastruttura informatica. Sul tema cfr. B. Calderini, "La Cina corre al primato nell'AI: ecco le strategie", in *Agenda Digitale*, 10/11/2023. Cfr. altresì l'articolo M. Koetse, "In the race for AI supremacy, China and the US are travelling on entirely different tracks", in *The Guardian*, 09/01/2024.

[12] Sulla vicenda TikTok si rinvia a L. Fabiano, "Le potenzialità manipolative della democrazia digitale fra interessi pubblici e poteri privati", cit.; Id., "Il liberal protezionismo digitale statunitense

Queste divergenze si riversano inevitabilmente sul piano degli obiettivi strategici che le politiche adottate da questi Paesi perseguono per cui tendenzialmente Stati Uniti d'America accentuano il profilo delle opportunità offerte dalla raccomandazione algoritmica e, più in generale, dall'intelligenza artificiale (AI)[13] e conferiscono un'importanza significativa all'obiettivo di mantenere una *leadership* globale nello sviluppo e nell'impiego delle stesse, quale presupposto per la crescita economica e la supremazia militare. Diversamente, l'Unione Europea sembra orientata a definire "un *gold standard* globale per l'uso etico delle applicazioni di AI"[14] evidenziando un approccio maggiormente orientato alla precauzione[15].

2. L'impianto *rights-based* e di "regolazione sociale" nella disciplina sull'AI in ambito europeo

Per le ragioni brevemente esposte in premessa non sorprende dunque riscontrare nel contesto europeo scelte di disciplina sull'AI orientate in primo luogo alla garanzia dei diritti fondamentali.

Ciò si riscontra sin dal 2016 quando, con l'adozione del Regolamento generale della protezione dei dati (GDPR n. 2016/679)[16], l'UE si propone di affrontare il tema della protezione dei dati personali processati algoritmicamente e, dunque, se pur il GDPR non si presenta quale atto normativo volto a disciplinare specificamente l'AI esso, tuttavia, pone numerosi principi che possono rappresentare un utile argine ad un utilizzo sconsiderato della stessa.

A partire dal 2016 a livello europeo vengono pertanto introdotti e sviluppati concetti fondamentali e principi cardine quali: il diritto di contestare la decisione

fra difesa della leadership nel mercato tecnologico e sicurezza nazionale", in *Dpce online*, 60 (2023), n. 3; sul Cyberspionaggio cinese cfr. G. Iuvinale, N. Iuvinale, "Sicurezza. Così il governo cinese penetra nella tecnologia USA", in *Agenda Digitale*, 20/04/2023.

[13] Sulla raccomandazione algoritmica come tipologia di AI cfr. P. Casagranda, S. Metta, *Sistemi di Raccomandazione: Intelligenza Artificiale, Deep Learning e personalizzazione dei contenuti*, in *Elettronica e comunicazioni*, (2020), n. 1, pp. 101 ss.

[14] Cfr. ancora G. Resta, "Cosa c'è di europeo nella proposta di regolamento Ue sull'Intelligenza artificiale?", cit., p. 326.

[15] Sul punto ancora G. Resta, "Cosa c'è di europeo nella proposta di regolamento Ue sull'Intelligenza artificiale?", cit. Cfr. anche E. Chiti, B. Marchetti, "Divergenti? Le strategie di Unione Europea e Stati Uniti in materia di intelligenza artificiale", in *Riv. Regolazione mercati*, (2020), n. 2, pp. 29-50; L. Floridi, "The European Legislation on AI: a Brief Analysis of its Philosophical Approach", in *Philosophy & Technology*, 34 (2021), n. 3, pp. 215 ss.

[16] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 avente a oggetto la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Il Regolamento è entrato in vigore nel maggio 2018.

automatizzata[17], il principio di non discriminazione algoritmica[18], il principio di non esclusività[19], il diritto ad accedere alla logica impiegata dall'algoritmo[20].

L'introduzione di tali principi riflette la finalità di "regolazione sociale" prescelta dall'Unione Europea in tale ambito e segnala l'esigenza insita in tale intervento normativo di realizzazione di "alcune esigenze sociali che è un mercato dominato dall'intelligenza artificiale è lasciato a se stesso non garantirebbe: la tutela dei dati personali, la tutela del consumatore, ma anche la tutela ambientale insieme alla grande questione dell'energia necessaria per alimentare l'uso dell'intelligenza artificiale"[21]

In materia di trattamento automatizzato dei dati personali nel 2016 viene altresì adottata la Direttiva UE 680-2016[22] concernente il trattamento interamente o parzialmente automatizzato dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali. La detta Direttiva ribadisce in più passaggi il Regolamento 2016/679: l'art. 11 comma 1 riproduce ad esempio il contenuto dell'art. 22 GPDR in materia di decisione basata unicamente su un trattamento automatizzato, stabilendo che "una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici negativi o incida significativamente sull'interessato sia vietata, salvo che sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che preveda garanzie adeguate per i diritti e le libertà dell'interessato" tra cui almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento. La previsione è rafforzata dal Considerando 38, in virtù del quale l'interessato "dovrebbe avere il diritto di non essere oggetto di una decisione che valuta aspetti personali che lo concernono basata esclusivamente su un trattamento automatizzato e che produca effetti giuridici negativi nei suoi confronti o incida significativamente sulla sua persona"; devono essere in ogni caso fornite garanzie adeguate tra cui il diritto a ottenere l'intervento umano, il diritto di esprimere la propria opinione, di ottenere una spiegazione della decisione raggiunta dopo tale valutazione e di impugnare la decisione. Viene previsto altresì che la discriminazione di persone

[17] Artt.13, comma 2, lett. f); 14 comma 2, lett. g) Reg. (UE) 2016/679.

[18] Cons. 71 Reg. (UE) 2016/679 secondo cui le procedure matematiche e statistiche utilizzate devono essere appropriate e sottoposte a controllo per evitare inesattezze o errori, al fine di impedire "effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero un trattamento che comporti misure aventi tali effetti".

[19] Art. 22 Reg. (UE) 2016/679.

[20] Art. 15, comma 1, lett. h) Reg. (UE) 2016/679.

[21] E. Chiti, B. Marchetti, *Divergenti? Le strategie di Unione europea e Stati Uniti in materia di intelligenza artificiale*, cit., spec. p. 32. Cfr. sul tema anche G. Resta, "Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di eguaglianza", in *Politica del Diritto*, (2019), p. 199 ss.

[22] Adottata il 27 aprile 2016 dal Parlamento e dal Consiglio europeo; Direttiva recepita dall'ordinamento italiano con il Decreto Legislativo 21/05/2018 n. 51.

fisiche sulla base di dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dovrebbe essere vietata. Infine, l'art. 29 comma 2 dispone che il titolare del trattamento attui una serie di misure volte ad impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati (lett. d), a garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione d'accesso (lett. e) ed infine a garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata ("controllo dell'introduzione") (lett. g).

Il tema dell'AI è attualmente oggetto del Regolamento europeo sull'Intelligenza Artificiale (l'*AI Act*) approvato dal Parlamento Ue il 13 marzo 2024 e dal Consiglio Europeo il 21 maggio 2024[23]. Avendo ottenuto il via libera all'unanimità dagli Stati, la detta normativa entra in vigore venti giorni dopo la sua pubblicazione nella Gazzetta Ufficiale dell'Ue e diverrà pienamente applicabile due anni dopo la sua entrata in vigore, secondo il seguente approccio graduale: sei mesi dopo l'entrata in vigore, gli Stati membri dovranno eliminare gradualmente i sistemi vietati; dodici mesi dopo, diventeranno applicabili gli obblighi relativi alla governance dell'IA per finalità generali; ventiquattro mesi dopo, diverranno applicabili tutte le regole della legge sull'IA, compresi gli obblighi per i sistemi ad alto rischio definiti nell'allegato III (elenco dei casi d'uso ad alto rischio); trentasei mesi dopo, si applicheranno gli obblighi per i sistemi ad alto rischio definiti nell'allegato II (elenco della normativa di armonizzazione dell'Unione) [24].

L'*AI Act*, analogamente al GDPR, segue un approccio regolatorio orizzontale e non per singoli settori (o problemi) oggetto di disciplina. Oltre ad elencare tassativamente alcune pratiche di AI del tutto vietate[25] la proposta di Regolamento

[23] Il testo armonizzato del Regolamento europeo sull'intelligenza artificiale è reperibile al seguente url: https://data.consilium.europa.eu/doc/document/PE-24-2024-INIT/it/pdf.

[24] Per facilitare il passaggio verso in nuovo quadro normativo la Commissione ha promosso il c.d. Patto sull'AI sollecitando i soggetti destinatari della normativa ad anticipare, con impegno volontario, l'attuazione della detta disciplina. Sul punto cfr. https://digital-strategy.ec.europa.eu/en/policies/ai-pact.

[25] Le pratiche di AI espressamente vietate sono collegate all'utilizzo di tecniche subliminali che possano in maniera estranea alla consapevolezza della persona coinvolta al fine di distorcerne il comportamento in modo da provocare ad essa o ad altri un danno fisico o psicologico; allo sfruttamento della vulnerabilità di uno specifico gruppo di persone, dovute all'età o ad una disabilità fisica o mentale, al fine di distorcerne il comportamento di una di esse in modo da arrecare ad essa o ad altri un danno fisico o psicologico; a consentire alle autorità pubbliche di valutare o classificare l'affidabilità delle persone fisiche per un determinato periodo di tempo, sulla base del loro comportamento, delle loro caratteristiche personali o delle loro personalità, attribuendo loro un punteggio che, se particolarmente sfavorevole, dia luogo ad una serie di scenari arbitrariamente pregiudizievoli; all'uso di sistemi di identificazione biometrica remota in tempo reale, ai fini di attività di contrasto. Queste pratiche sarebbero consentite solo nella misura in cui fossero finalizzate alla ricerca di potenziali vittime o minori scomparsi, a prevenire minacce specifiche per la vita delle

è caratterizzata da un approccio *risk based* individuando IA che generino rischi: A) Inaccettabili; B) Alti; C) Bassi o minimi.

I sistemi di IA qualificati come di "rischio inaccettabile" saranno del tutto vietati. In questa categoria rientrano i sistemi che sono in grado di manipolare il comportamento umano ovvero quelli che consentono di attribuire un "punteggio sociale" (*social scoring*), per finalità pubbliche e private, classificando le persone in base al loro comportamento sociale o alle loro caratteristiche personali. Sono incluse in questa categoria anche determinate applicazioni di polizia predittiva. In particolare saranno vietati: a) i sistemi di sfruttamento delle vulnerabilità delle persone e di utilizzo di tecniche subliminali ovvero deliberatamente manipolative o ingannevoli; b) i sistemi di categorizzazione biometrica delle persone fisiche sulla base di dati biometrici per dedurne o desumerne la razza, le opinioni politiche, l'appartenenza sindacale, le convinzioni religiose o filosofiche, la vita sessuale o l'orientamento sessuale (sarà ancora possibile filtrare set di dati basandosi su dati biometrici nel settore delle attività di contrasto); c) i sistemi di identificazione biometrica in tempo reale in spazi accessibili al pubblico (ossia il riconoscimento facciale mediante telecamere a circuito chiuso) da parte delle autorità di contrasto (con limitate eccezioni); d) i sistemi di riconoscimento delle emozioni utilizzati sul luogo di lavoro e negli istituti scolastici, eccetto per motivi medici o di sicurezza (ad esempio il monitoraggio dei livelli di stanchezza di un pilota); e) l'estrazione non mirata (*scraping*) di immagini facciali da internet o telecamere a circuito chiuso per la creazione o l'espansione di banche dati; f) i sistemi che consentono di attribuire un "punteggio sociale" (*social scoring*), classificando o valutando le persone in base al loro comportamento sociale o alle loro caratteristiche personali.

Nell'allegato III al Regolamento sono invece elencati i sistemi di AI considerati ad "alto rischio"[26] e dunque non vietati ma sottoposti ad una stringente normativa concernente la loro valutazione di conformità in particolare nell'impatto sui diritti fondamentali[27]

persone o collegate ad attacchi terroristici, oppure ad individuare, localizzare, identificare e/o perseguire un autore, o sospettato tale, di un reato di particolare gravità.

[26] L'allegato III qualifica i sistemi di IA ad alto rischio a norma dell'articolo 6, paragrafo 2, gli algoritmi operanti nei seguenti contesti: 1. Identificazione e categorizzazione biometrica delle persone fisiche. 2. Gestione e funzionamento delle infrastrutture critiche. 3. Istruzione e formazione professionale. 4. Occupazione, gestione dei lavoratori e accesso al lavoro autonomo. 5. Accesso a prestazioni e servizi pubblici e a servizi privati essenziali e fruizione degli stessi. 6. Attività di contrasto. 7. Gestione della migrazione, dell'asilo e del controllo delle frontiere. 8. Amministrazione della giustizia e processi democratici.

[27] La valutazione deve consistere in una descrizione dei processi dell'operatore in cui il sistema di IA ad alto rischio sarà utilizzato, del periodo di tempo e della frequenza in cui il sistema di IA ad alto rischio è destinato a essere utilizzato, delle categorie di persone fisiche e dei gruppi che possono essere interessati dal suo uso nel contesto specifico, dei rischi specifici di danno che possono incidere sulle categorie di persone o sui gruppi di persone interessati, e in una descrizione dell'attuazione delle misure di sorveglianza umana e delle misure da adottare in caso di concretizzazione dei rischi. Per un approfondimento cfr. Camera dei deputati, XIX legislatura, "Documentazioni per le

Il regolamento sull'AI, oltre a porre una serie di norme tecniche e di sorveglianza destinate ai produttori ed ai distributori di tali tecnologie sancisce, all'art. 29, anche degli obblighi in capo agli utenti della medesima AI classificata ad alto rischio quali ad esempio il corretto uso della stessa ed il monitoraggio e l'impegno alla segnalazione immediata in caso di incidenti o malfunzionamenti.

Il medesimo regolamento pone inoltre in essere delle misure a sostegno dell'innovazione e della ricerca sull'AI[28] e definisce altresì un'architettura della governance in tema di sorveglianza sul rispetto del medesimo Regolamento stabilendo che le autorità nazionali competenti per la vigilanza del mercato sorveglieranno l'attuazione delle nuove norme a livello nazionale, mentre un Ufficio europeo per l'IA, costituito presso la Commissione europea, garantirà il coordinamento a livello europeo. Ciascuno Stato membro designerà una o più autorità nazionali competenti, incaricate di supervisionarne l'applicazione e l'attuazione, nonché di svolgere attività di vigilanza del mercato. Un comitato scientifico di esperti indipendenti avrà il compito di segnalare i rischi sistemici e contribuire alla classificazione e alla sperimentazione dei modelli. Un comitato europeo per l'IA, composto dai rappresentanti degli Stati membri, svolgerà il ruolo di piattaforma di coordinamento e di organo consultivo per la Commissione europea. Il Garante europeo della protezione dei dati parteciperà come osservatore. È prevista inoltre l'istituzione di un forum consultivo per i portatori di interessi, come i rappresentanti dell'industria, le PMI, le start-up, la società civile e il mondo accademico.

L'assetto normativo del Regolamento evidenzia la logica di cooperazione fra soggetti coinvolti nella tecnologia sottoposta a normativa che caratterizza tale disciplina[29] sottolineando, per certi versi, la fluidità dell'oggetto disciplinato e la necessità che ad esso, al di là delle regole imposte, ci si approcci con responsabilità.

Con risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'AI, sono state infine proposte delle raccomandazioni dettagliate per l'elaborazione di un Regolamento europeo sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale[30]. La proposta di Regolamento impone agli operatori di sistemi di AI ad alto rischio, di attivare un'apposita polizza assicurativa per la responsabilità civile (per danni materiali ed immateriali) adeguata agli importi e all'entità del risarcimento stabiliti anch'essi dal regolamento. La proposta opera una

Commissioni, Attività dell'Unione Europea, Il Regolamento UE in materia di Intelligenza Artificiale", paper n. 26, 5 febbraio 2024.

[28] In particolare, consente la creazione di spazi di sperimentazione normativa per l'IA (*sandbox* normativi) e di prova in condizioni reali, che forniscono un ambiente controllato per testare tecnologie innovative per un periodo di tempo limitato, promuovendo in tal modo l'innovazione da parte delle imprese, delle PMI e delle *start-up*. Gli Stati membri dovranno istituire almeno un *sandbox* normativo sull'IA a livello nazionale. Potrà anche essere istituito congiuntamente tra più Stati membri.

[29] L'osservazione è di L. Milano, *op. cit.*

[30] Proposta di Regolamento A9-178/2020.

differenziazione tra i sistemi di AI ad alto rischio, individuati da un apposito elenco allegato al regolamento, per i quali la responsabilità è oggettiva in causa di danni o pregiudizi, rispetto agli altri sistemi di AI (art. 8) dove la responsabilità assume il grado di colpa, sino a potere essere esclusa in caso di dimostrazione della non imputabilità in presenza di alcuni motivi individuati[31].

3. La normativa e la giurisprudenza sull'AI e sulla raccomandazione algoritmica nell'esperienza USA fra strategie di tutela della *leadership* nel mercato e problemi di sicurezza internazionale

Rispetto all'importanza che nel contesto europeo è attribuita alla dimensione cautelativa e di garanzia dei diritti degli utenti, l'approccio statunitense alla disciplina dell'AI è maggiormente orientato alla promozione della *leadership* economica del paese. Tale divergenza si evince sin dalla lettura dell'*Executive Order* n. 13859/2019, *Mantaining American Leadership in AI*, adottato dal Presidente Trump l'11 febbraio del 2019 sulla scorta del *White House Summit on AI for American Industry* del 2018[32]. L'*executive Order* 13859, sottolineando il ruolo dell'America come *leader* globale nella tecnologia dell'intelligenza artificiale si compone di cinque direttive principali: 1. Investimenti federali intesi come una priorità delle agenzie federali che dovrebbero sviluppare i propri *budget* in funzione del sostegno alla ricerca e allo sviluppo tecnologico AI oltre che esplorare opportunità di collaborazione con il mondo accademico ed il settore privato; 2. Risorse federali: ovvero l'organizzazione delle risorse già in essere orientate alla valorizzazione dell'AI di conio statunitense; 3. Linee guida per la regolamentazione; 4. Investimenti nell'*expertise*; 5. Protezione dell'AI americana.

In diretta correlazione con quanto accade nel coevo periodo in Cina, ove nel 2017 il governo afferma ambiziosamente di voler diventare il *leader* mondiale nell'IA entro il 2030[33], la presidenza Trump reagisce con vigore inaugurando una strategia regolatoria fortemente promozionale e allo stesso tempo di protezione del mercato statunitense in ambito tecnologico e specificatamente sull'AI. Tale strategia, orientata dunque non alla considerazione delle problematiche connesse alla tutela dei diritti individuali nell'interazione umana con l'intelligenza artificiale, quanto volta a garantire la supremazia tecnologica americana e la sicurezza

[31] La proposta è commentata da A. Mastromatteo, B. Santacroce, *Responsabilità civile per i danni dell'intelligenza artificiale: la proposta del Parlamento Ue*, 05/01/2021, reperibile all'url www.agendadigitale.eu/cultura-digitale/la-responsabilita-civile-per-lintelligenza-artificiale-le-proposte-europee/, [Data di consultazione: 22/03/2024].

[32] Su cui cfr. https://trumpwhitehouse.archives.gov/ai/.

[33] *State Council: New Generation of Artificial Intelligence Development Plan. State Council Document №. 35 (2017)*. Cfr. M.S. Reshetnikova, "Future China: AI Leader in 2030?", in *Conference: Research and Innovation Forum, Rii Forum 2021*. Reperibile all'url www.researchgate.net/publication/357737833_Future_China_AI_Leader_in_2030, [Data di consultazione: 22/03/2024].

nazionale si evidenzia anche in alcune scelte del Congresso statunitense assunte nel medesimo periodo: il 13 agosto 2018 la sezione 1051 del *John S. McCain National Defense Authorization Act for Fiscal Year* 2019[34] ha istituito la *National Security Commission* quale Commissione indipendente con l'obiettivo di "considerare i metodi e i mezzi necessari per avanzare lo sviluppo dell'intelligenza artificiale dell'apprendimento automatico e delle tecnologie associate per affrontare in modo completo le esigenze di sicurezza e difesa nazionale degli Stati Uniti"; nel 2020 viene altresì proposto il *National AI Initiative Act*[35], atto normativo di pianificazione delle attività federali a sostegno della ricerca sull'AI statunitense.

Il Congresso ha dunque scelto di confermare l'approccio politico all'AI impresso dalla Presidenza Trump mentre altre prospettive maggiormente orientate a considerare i rischi che tali tecnologie rappresentano per gli utenti che le utilizzano e della responsabilità delle grandi aziende *Tech* in relazione all'attività di *algorithmic recommendation*, pur riscuotendo un consenso *bipartisan*, non sono riusciti a concretizzarsi nell'emanazione di atti normativi[36].

Il tema della responsabilità del *provider* collegato alla raccomandazione algoritmica è stato affrontato nell'esperienza statunitense anche nelle aule giudiziarie ove, nondimeno, sembra essersi esaurito nel maggio del 2023 in una decisione assunta dalla Corte suprema federale.

La vicenda giurisprudenziale da cui il dibattito sul tema ha preso le mosse è il caso *Force v. Facebook, Inc.*[37], una decisione del Secondo Circuito, in cui la Corte, richiamandosi e ribadendo la nota differenziazione fra *content* e *service provider* ha stabilito che la sez. 230 garantisce un *social network* dai ricorsi per risarcimento civile in relazione a vicende che riguardano il sostegno materiale al terrorismo. Ciò veniva deciso nonostante quanto affermato dai ricorrenti i quali sostenevano che la decisione algoritmica costituisse un elemento da prendere in considerazione per valutare se un *provider* apparentemente neutro non fosse, in effetti, un reale produttore di contenuti[38]. Nella decisione ha tuttavia dissentito il giudice Robert Katzman il quale ha posto in evidenza come, allo stato attuale dell'evoluzione tecnologica, la decisione algoritmica ed i suoi effetti hanno

[34] PL 115-232.
[35] In vigore dal primo gennaio 2021.
[36] Fra le proposte figura, ad esempio, l'*Algorithmic Accountability Act* (S. 3572). La proposta di legge era finalizzata ad attribuire alla *Federal Trade Commission* il potere di effettuare delle valutazioni sugli algoritmi usati dalle grandi aziende *Tech*. Al Congresso peraltro sono stati presentati anche altri progetti normativi sul medesimo tema (l'*Algorithmic Justice and Online Trasparency Act*, S. 1896; il *Protecting Americans from Dangerous Algorithmic Act*, H.R. 2154).
[37] *Force v. Facebook, Inc.*, 934 F.3d 53 (2nd Cir. 2019).
[38] "*The algorithms take the information provided by Facebook users and 'match' it to other users—again, materially unaltered—based on objective factors applicable to any content, whether it concerns soccer, Picasso, or plumbers. Merely arranging and displaying others' content to users of Facebook through such algorithms—even if the content is not actively sought by those users—is not enough to hold Facebook responsible as the 'develop[er]' or 'creat[or]' of that content*", *Force v. Facebook, Inc.*, 934 F.3d 53, 70 (2d Cir. 2019).

trasformato il ruolo dei *providers* riducendone la neutralità. Il giudice dissenziente ha considerato difatti che fosse necessario, nell'interpretazione e nell'applicazione della sez. 230, distinguere fra la irresponsabilità del *provider*, nonostante l'attività di moderazione, per i contenuti caricati da terzi, rispetto alla responsabilità dello stesso allorché, attraverso l'attività algoritmica, vada a "potenziare" un pensiero diffondendolo e collegandolo ad una rete di sostenitori e dunque creando connessioni fra utenti delle quali è responsabile[39]. La Corte non ha tuttavia condiviso l'opinione del giudice Katzman ritenendo che la neutralità dell'algoritmo nelle sue decisioni di creazione dei rapporti sul *web* ne sani gli effetti.

Il tema della necessità di escludere la decisione algoritmica (determinata, in ultima analisi, dalla programmazione del *provider*) dalle garanzie della sez. 230 è ripreso nello *statement* del giudice Clarence Thomas nel diniego al *Writ of certiorari* al caso *Malwarebytes, Inc. v. Enigma Software Group Usa LLC*[40], una vicenda giudiziaria nella quale figuravano come controparti due aziende produttrici di *software* per l'esclusione di materiale indesiderato: la *Malwarebytes* aveva perfezionato il suo programma per impedire che ai propri utenti pervenissero prodotti della società concorrente *Enigma* qualificandoli, nella definizione algoritmica, come prodotti indesiderati. Pur condividendo il diniego del *certiorari* disposto dalla Corte suprema, il giudice Thomas ha tratto spunto da tale vicenda per evidenziare come la portata della sez. 230 necessiti di essere rivista ed ha richiamato, nella sua argomentazione sul punto, anche l'opinione in dissenso del giudice Katzman nel caso *Force v. Facebook.*

Il tema della responsabilità del *provider* in relazione alla decisione algoritmica, oggetto di diverse decisioni delle Corti federali di distretto o di circuito[41], è stato oggetto di un recente ricorso alla Corte suprema e la relativa

[39] Nelle parole del giudice: "*we today extend a provision that was designed to encourage computer service providers to shield minors from obscene material so that it now immunizes those same providers for allegedly connecting terrorists to one another. Neither the impetus for nor the text of § 230(c)(1) requires such a result. When a plaintiff brings a claim that is based not on the content of the information shown but rather on the connections Facebook's algorithms make between individuals, the CDA does not and should not bar relief*". *Marshall's Locksmith Service v. Google*, 925 F.3d 1263. In un passo successivo il giudice aggiunge: "*in part through its use of friend, group, and event suggestions, Facebook is doing more than just publishing content: it is proactively creating networks of people. Its algorithms forge real-world (if digital) connections through friend and group suggestions, and they attempt to create similar connections in the physical world through event suggestions. The cumulative effect of recommending several friends, or several groups or events, has an impact greater than the sum of each suggestion. It envelops the user, immersing her in an entire universe filled with people, ideas, and events she may never have discovered on her own*", *Force v. Facebook, Inc.*, 934 F.3d 53, 83 (2d Cir. 2019).

[40] *Malwarebytes, Inc. v. Enigma Software Group Usa LLC*, Docket n. 19-1284, decided, October 13, 2020. *Statement of Justice Thomas* - 592 U. S. ____ (2020).

[41] Fra i casi più noti figura la sentenza *Dyroff v. Ultimate Software Grp., Inc.*, 934 F.3d 1093 (9th Cir. 2019) ove il Nono Circuito ha considerato la sez. 230 sufficientemente ampia da garantire un sito circa un dibattito anonimo su tematiche varie ("*Experience Project*"). Il *provider* era accusato di aver favorito attraverso il suo sistema di segnalazione algoritmica l'incontro materiale fra un tossicodipendente ed uno spacciatore.

decisione era attesa quale possibile momento di importante svolta nel regime di responsabilità delle aziende e dei portali digitali. Ciò nella pratica non è avvenuto giacché nella decisione *Gonzales v. Google*[42], assunta *per curiam* il 18 maggio 2023, e vergata materialmente dal giudice Thomas, la Corte suprema ha in effetti annullato e rinviato al Nono circuito la decisione facendo riferimento ad un altro caso congiunto *Twitter, Inc. v. Taamneh*[43] ove lo stesso Thomas, per la Corte, ha chiarito come la raccomandazione algoritmica non possa essere considerata attualmente ragione sufficiente per fondare una responsabilità civile del *provider*.

La vicenda sottostante al caso *Gonzales v. Google* riguardava il grave atto terroristico verificatosi a Parigi nel novembre del 2015. In quella circostanza perse la vita (fra i molti) una giovane donna americana la cui famiglia ha intentato una causa civile contro *Google* sostenendo che *Youtube* (società ad essa collegata), attraverso la diffusione algoritmicamente mirata dei suoi video aveva favorito il reclutamento dei terroristi e la costituzione della loro rete[44]. Il tribunale distrettuale si è pronunciato a favore di *Google* facendo perno sulla sez. 230 e tale decisione è stata confermata dal Nono circuito; tuttavia, la Corte suprema ha concesso il *certiorari*, animando il dibattito circa l'idea per la quale le grandi aziende digitali non possano più continuare ad essere considerate figure neutrali ai discorsi che circolano in rete (ed ai legami che in rete si creano grazie alla raccomandazione algoritmica) giacché risulterebbe oramai evidente come le stesse siano guidate dal maggiore vantaggio economico che risiede nell'acquisizione dei dati e nella circolazione stessa di alcune informazioni[45].

Molti dei numerosi *amicus curiae* depositati in attesa della decisione, pur evidenziando la necessità di una rivalutazione dei contorni della sezione 230, hanno rilevato la necessità che la questione della responsabilità del *provider* venga nondimeno affrontata in sede legislativa e non giurisdizionale e tuttavia, come già evidenziato, progetti normativi concernenti tali temi non sono riusciti a superare sino ad ora il vaglio del Congresso[46].

[42] 598 U. S. _ (2023). Docket No. 21–1333; May 18, 2023.
[43] 598 U. S. _ (2023). No. 21–1496. Argued February 22, 2023—Decided May 18, 2023.
[44] Il ricorso era fondato sull'*Anti Terrorism Act* il quale consente ai cittadini statunitensi di esigere un risarcimento per danni sofferti "*by reason of an act of international terrorism*" 18 U.S.C. § 2333(a), e estende la responsabilità ad "*any person who aids and abets, by knowingly providing substantial assistance*" ad una persona che commette un atto di terrorismo internazionale, 18 U.S.C. § 2333(d).
[45] Cfr. M. Barbera, "Discriminazioni algoritmiche e forme di discriminazione", in *Labour and Law Issue*, 7 (2021), n. 1. S. Tommasi, "Algoritmi e nuove forme di discriminazione: uno sguardo al diritto europeo", in *Rev. de Direito Brasileira*, 27 (2020), n. 10, pp. 112 ss.
[46] In effetti nel 2022 è stato presentato un progetto normativo al Congresso: l'*Algorithmic Accountability Act* (S. 3572). La proposta di legge era finalizzata ad attribuire alla *Federal Trade Commission* il potere di effettuare delle valutazioni sugli algoritmi usati dalle grandi aziende *Tech*. Al Congresso peraltro sono stati presentati anche altri progetti normativi sul medesimo tema (l'*Algorithmic Justice and Online Trasparency Act*, S. 1896; il *Protecting Americans from Dangerous Algorithmic Act*, H.R. 2154).

Come già anticipato, il *certiorari* nel caso *Gonzales v. Google* è stato concesso insieme ad un altro caso collegato a fatti terroristici ovvero *Twitter, Inc. v. Taamneh*. La vicenda sottostante a tale decisione riguardava la morte di un cittadino giordano Nawras Alassaf, nel 2017, durante un attacco terroristico ad Istanbul. I parenti statunitensi del ragazzo avevano citato in giudizio Twitter, Google e Facebook sostenendo che le dette compagnie digitali fossero in parte responsabili dell'accaduto. In questa vicenda processuale il parametro di valutazione non era tuttavia la sez. 230 ma l'*Anti-Terrorism Act*[47] in base al quale i cittadini degli Stati Uniti che maturano un danno "a causa di un atto di terrorismo internazionale" possono chiedere il risarcimento citando in giudizio i singoli terroristi e le organizzazioni che hanno effettuato direttamente l'attacco ed anche, in base alla §2333(d)(2), "qualsiasi persona che aiuti e favorisca, fornendo consapevolmente un'assistenza sostanziale, o che cospiri con la persona che ha commesso un tale atto di terrorismo internazionale".

I ricorrenti sostenevano che non attuando un'adeguata sorveglianza sulle informazioni che circolano in rete, le dette grandi aziende avevano finito con il favorire l'azione terroristica.

La Corte suprema, tuttavia, non ha condiviso la tesi dei ricorrenti sostenendo che la raccomandazione algoritmica posta in essere dalle piattaforme imputate fosse "neutrale" ovvero svolgesse una funzione di *matching* fra contenuti associabili uguale per tutti (dunque non favorendo in particolare l'ISIS ed i suoi adepti)[48]. Il giudice Thomas ha peraltro evidenziato come in molti casi qualcuno può sfruttare a fini "terroristici" una tecnologia, ad esempio la rete telefonica, e questo non rende le aziende che forniscono questi servizi responsabili civilmente di tali azioni[49].

[47] 18 USC § 2333.

[48] "*Defendants' recommendation algorithms matched ISIS-related content to users most likely to be interested in that content—again, just like any other content… plaintiffs assert that defendants' 'recommendation' algorithms go beyond passive aid and constitute active, substantial assistance. We disagree. By plaintiffs' own telling, their claim is based on defendants' 'provision of the infrastructure which provides material support to ISIS.' A 53. Viewed properly, defendants' 'recommendation' algorithms are merely part of that infrastructure. All the content on their platforms is filtered through these algorithms, which allegedly sort the content by information and inputs provided by users and found in the content itself. As presented here, the algorithms appear agnostic as to the nature of the content, matching any content (including ISIS' content) with any user who is more likely to view that content. The fact that these algorithms matched some ISIS content with some users thus does not convert defendants' passive assistance into active abetting. Once the platform and sorting-tool algorithms were up and running, defendants at most allegedly stood back and watched; they are not alleged to have taken any further action with respect to ISIS*", Parte IV sez. A, *Justice Thomas Opinion*.

[49] "*The mere creation of those platforms, however, is not culpable. To be sure, it might be that bad actors like ISIS are able to use platforms like defendants' for illegal—and sometimes terrible—ends. But the same could be said of cell phones, email, or the internet generally. Yet, we generally do not think that internet or cell service providers incur culpability merely for providing their services to the public writ large. Nor do we think that such providers would normally be described as aiding and abetting, for example, illegal drug deals brokered over cell phones—even if the provider's*

Con tali decisioni la Corte sembra dunque essersi sostanzialmente tirata indietro dall'imprimere per via giudiziaria una nuova evoluzione al tema della responsabilità del *provider* nel contesto statunitense confermando in parte le numerose sollecitazioni provenienti da diversi *amicus curiae* che pur riconoscendo la problematica collegata alla limitatezza dell'attuale disciplina sulla responsabilità civile delle piattaforme elettroniche, ritiene che il tema debba essere trattato ed eventualmente sottoposto a modifiche da parte del Congresso.

4. La parabola cinese e il possibile ravvicinamento della strategia statunitense all'impostazione strategica europea

Come accennato in apertura, una delle ragioni principali alla base dell'approccio statunitense in tema di disciplina dell'intelligenza artificiale e della raccomandazione algoritmica orientato alla promozione tecnologica piuttosto che alla garanzia dei diritti fondamentali (come più tipicamente si propone l'impianto europeo), risiede nella concorrenza, nel mercato digitale, con il colosso cinese e nella netta scelta politica volta a preservare il perimetro di vantaggio che gli Stati uniti ritengono di detenere.

Tale assetto dei fatti si evidenzia a partire dall'adozione da parte di Trump del citato *Executive order* n. 13859 del 2019 il quale, come osservato, è contemporaneo al momento di maggior ambizione tecnologico vissuto in anni recenti dalla Cina.

La crisi pandemica, tuttavia, innesca alcuni significativi meccanismi nel contesto cinese, di maggior inasprimento della sorveglianza sistemica del regime sulla società civile, i quali si ripropongono anche in altri ambiti, non ultimo quello della disciplina sulla tecnologia informatica conducendo all'adozione di alcune normative cinesi molto significative in termini di controllo governativo della detta tecnologia ed attraverso la stessa[50].

Se già nel 2017 la Cina adottava una legge sull'*intelligence* nazionale[51] (in base alla quale le autorità statali cinesi possono richiedere ai propri cittadini ed alle aziende di fornire dati rilevanti per il loro lavoro di *intelligence*) – normativa che impensierisce gli Stati Uniti con riguardo al possibile rischio che le aziende tecnologiche possano cedere al Partito comunista cinese importanti informazioni

conference-call or video-call features made the sale easier", Cfr. Parte IV sez. A, *Justice Thomas Opinion*.

[50] Sul tema cfr. R. Berti, "Coronavirus, come la Cina lo ha fermato con la tecnologia e cosa può imparare l'Italia", in *Agenda Digitale*, 12/03/2020; D. Todaro, "Tecnologia e azione pubblica in Cina: il codice sanitario individuale e le principali tendenze delle politiche digitali cinesi contemporanee", in *Istituto Affari Internazionali, (iai) papers*, (2020), n. 46. Più in generale sul tema della sorveglianza digitale in epoca pandemica cfr. C. Blengino, "Tecnologie di sorveglianza e contenimento della pandemia", in *Questione giustizia*, (2020), n. 2.

[51] Cfr. sull'argomento G. Iuvinale, N. Iuvinale, "Sicurezza. Così il governo cinese penetra nella tecnologia USA", in *Agenda Digitale*, 20/04/2023.

sul popolo americano via *social* (in particolar modo attraverso la piattaforma tik tok)[52] – la questione esplode nel 2022 con l'adozione di una specifica normativa sulla raccomandazione algoritmica e nel 2023, anno nel corso del quale la Cina pone in essere le basi per una disciplina dedicata all'AI che sia orientata alla tutela degli interessi del Paese (e del regime)[53].

Sono tali cambiamenti nel contesto cinese, oltre che ovviamente una diversa sensibilità politica, i fattori che probabilmente si pongono alla base di una parziale inversione di rotta percepibile nella strategia politica statunitense a partire dall'adozione del più recente *Executive Order* della Presidenza in tema di intelligenza artificiale adottato da Joe Biden il 30 ottobre ed intitolato "*Executive Order in the safe, Secure, and trustworthy development and the use of artificial intelligence*" [54].

In consonanza con un'impostazione maggiormente orientata alla tutela dei diritti individuali[55] il detto *Executive Order* pone una serie di nuovi obiettivi strategici per la normazione dell'AI fra i quali spiccano: 1. Richiedere che gli sviluppatori dei sistemi di intelligenza artificiale più potenti condividano i risultati dei *test* di sicurezza ed altre informazioni critiche con il governo degli Stati Uniti. 2. Sviluppare *standard*, strumenti e *test* per garantire che i sistemi di intelligenza artificiale siano sicuri, protetti e affidabili. 3. Proteggersi dai rischi derivanti dall'utilizzo dell'intelligenza artificiale in merito alla progettazione di materiali biologici pericolosi sviluppando nuovi e forti standard per lo screening della sintesi biologica. 4. Proteggere gli americani dalle frodi e dagli inganni legati all'intelligenza artificiale stabilendo standard e buone pratiche per rilevare i contenuti generati dall'intelligenza artificiale e autenticare i contenuti ufficiali. 5. Stabilire un programma avanzato di sicurezza informatica per sviluppare strumenti di intelligenza artificiale per individuare e correggere la vulnerabilità nel software critico. 6- Ordinare lo sviluppo di un memorandum sulla sicurezza nazionale che diriga ulteriori azioni su intelligenza artificiale e sicurezza.

Altri aspetti cui l'*Executive order* del 2023 dedica particolare importanza concernano i temi della *privacy* degli americani nell'utilizzo dei sistemi AI oltre che la messa a punto di scelte politiche e normative orientate alla promozione dell'equità e dei diritti civili del popolo statunitense con particolare riguardo alla lotta alla discriminazione algoritmica.

È evidente, dunque, un cambio di rotta nell'approccio strategico alla materia.

[52] Sul tema, L. Fabiano, "Le potenzialità manipolative della democrazia digitale fra interessi pubblici e poteri privati", cit.
[53] Cfr. nota 11.
[54] L'*Executive order* citato è reperibile al seguente url: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/, [Data di consultazione: 22/03/2024].
[55] Tale approccio si evince già nel navigare sul sito internet della Presidenza Biden dedicato all'AI ovvero https://ai.gov/.

Se, come osservato, esso risiede in una particolare sensibilità politica della Presidenza democratica, la quale anche solo per segnare un'importante differenza con la precedente amministrazione Trump, sottolinea la propria tensione alla tutela dei diritti fondamentali ciò nondimeno risulta rilevante osservare come tale cambio di rotta interviene alla fine del primo mandato presidenziale Biden in concomitanza con le evoluzioni strategiche e geopolitiche cinesi.

Nonostante l'apparente ravvicinamento delle politiche strategiche delle due aree territoriali analizzate, risulta tuttavia evidente una divaricazione attualmente sussistente fra le priorità perseguite nel contesto statunitense e gli obiettivi preposti alla normazione europea in tema di disciplina della tecnologia AI. Tale divergenza riflette certamente l'assetto economico imprenditoriale nell'ambito di tale tecnologia che caratterizza i due contesti territoriali (una condizione di *leadership* statunitense e di parziale ritardo tecnologico europeo) e tuttavia la medesima differenziazione si iscrive anche in una diversità culturale che connota Stati Uniti ed Europa che viene ribadita anche in tale circostanza: una maggiore attenzione del decisore politico europeo per i diritti individuali e dunque una sorta di antropocentrismo legislativo che sembra invece lontano dall'approccio statunitense maggiormente orientato al rendimento economico del Paese ed alla protezione dei diritti del popolo americano (e non dei diritti fondamentali intesi in senso più ampio), scelta in funzione della quale gli Stati Uniti si caratterizzano in questo campo, come in effetti in tante altre occasioni, per un approccio liberal-protezionista[56].

[56] Su tale *trend* statunitense cfr. L. Fabiano, "Il liberal protezionismo digitale statunitense fra difesa della leadership nel mercato tecnologico e sicurezza nazionale", cit.