Il liberal-protezionismo digitale statunitense fra difesa della *leadership* nel mercato tecnologico e sicurezza nazionale[1*]

di Laura Fabiano

Abstract: *US liberal digital protectionism between defense of technological market leadership and national security* - In both the United States and European contexts, the digital agora discipline has been historically characterized by a long initial period characterized by tendentially liberal traits.
However, the particularities of the IT environment have led over time to assess the need to modify this guideline and to more strictly regulate issues relating to provider responsibility and algorithmic activity.
In addressing this problem, European and US action are divided. This occurs due to a different historical tradition that recognizes these contexts and geopolitical considerations.
The present work aims to analyze the US experience in the field of digital ecosystem in order to evaluate in it the existence of a sort of ambivalence between liberalism and protectionism.

Keywords: Us IT Environment; Artificial Intelligence; National Security; Digital Market; recommendation algorithm.

1. Europa e Stati Uniti nell'evoluzione della disciplina della tecnologia digitale

Tanto negli Stati Uniti quanto nel contesto europeo la disciplina concernente l'*agorà* digitale si caratterizza storicamente per una prima lunga fase storica connotata da tratti tendenzialmente liberistici ove il tema maggiormente sentito era favorire la libera circolazione e la promozione dei servizi della società dell'informazione eliminando gli ostacoli allo sviluppo del commercio elettronico. Tale impianto segue al copioso dibattito fra gli studiosi del tema attinente alla considerazione dello spazio digitale quale (non)luogo anarchico o al più autogestito[2].

[1*] 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".

[2] La dottrina giuridica si è interrogata, inizialmente, e per lungo tempo, sulla stessa praticabilità dell'estensione al mondo telematico del diritto territoriale vigente nel mondo reale e, dunque, sul c.d. "statuto costituzionale di Internet". Tale questione dottrinale ha subito un'evoluzione storica, oramai ventennale, nel corso della quale da un primo approccio improntato all'idea della completa autonomia di Internet rispetto al mondo reale, si è approdati -grazie probabilmente al contributo rilevante della

Negli Stati Uniti, nel 1996, il Congresso adotta difatti la notissima sezione 230 del *Title 47* dello *Us Code* (*Communication Decency Act*) che sanciva la completa deresponsabilizzazione degli *Internet provider* per i contenuti caricati da terzi attraverso la previsione della c.d. clausola del buon samaritano[3]; in ambito europeo, d'altra parte, sino alla più recente adozione

giurisprudenza di alcune Corti-, alla concezione piena della vigenza del diritto territoriale anche nel contesto telematico. Fra gli studiosi patrocinanti della concezione autonoma e anarchica del mondo digitale si richiama innanzitutto John Perry Barlow il quale con la sua *Declaration of Independence of the Cyberspace* del 1996 (in www.eff.org, 8 febbraio 1996) incarnava, sotto un profilo dottrinale, quelle posizioni ultralibertarie che si sono imposte nei primi anni di affermazione della rete *web* per le quali lo spazio digitale era, e doveva rimanere ad ogni costo, un (non) luogo di assoluta sfrenata libertà individuale. Fra i sostenitori della *self regulation* del mondo digitale, «*lex specialis* convenzionale pensata per internet e partorita da internet» (M. Bassini, *Internet e libertà di espressione*, Prospettive Costituzionali e Sovranazionali, Roma, 2019, 46) figurano David Johnson e David Post i quali, in diversi scritti, (il più noto è: *Law and Borders. The Rise of Law in Cyberspace*, in *Stanford Law Review*, vol. 48, n. 5, 1996, 1367 ss.) contestano la possibilità di regolazione statuale per il mondo digitale e sostengono l'autosufficienza regolatoria delle comunità digitali.
Parallelamente a tale tipologia di dibattito, la dottrina ha sviluppato un secondo filone di dissertazione concernente la sussistenza o meno di una dignità scientifica da riconoscersi allo studio delle dinamiche di *governance* e delle relazioni che si sviluppano nella rete *web*. Ciò a partire dalla provocazione di Frank Easterbrook (allora giudice della Corte di Appello degli Stati Uniti per il Settimo Circuito) il quale, nel 1996, in una conferenza sul tema *Law of Cyberspace* organizzata dall'Università di Chicago, contestò l'idea che il diritto digitale possedesse una sua intrinseca autonomia sostenendo che i suoi fenomeni dovessero essere studiati e analizzati attraverso il prisma delle regole generali. Sul fronte opposto si schierò con decisione Lawrence Lessing al quale, dunque, fa capo quel filone di pensiero che, riconoscendo alla dimensione digitale delle specificità irriducibili, riteneva che le caratteristiche del *web* impongano una seria valutazione circa la possibilità delle categorie giuridiche tradizionali di permearne i confini e quindi di soddisfare pienamente le esigenze di regolazione e tutela che anche da tale (non)luogo promanano. Sul punto cfr. S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma, 1997; V. Zeno-Zencovich, *Informatica ed evoluzione del diritto*, in *Diritto dell'informazione e dell'informatica*, n. 1, 2003; M. Bassini, *Internet e libertà di espressione*, Canterano (RM), 2019; P. Costanzo, *Il fattore tecnologico e le sue conseguenze*, in *Rassegna parlamentare*, n. 4, 2012, 811 ss.; T.E. Frosini, *Tecnologie e libertà costituzionali*, in *Diritto dell'informazione e dell'informatica*, n. 3, 2003, 487 ss.; T.E. Frosini, O. Pollicino, E. Apa, M. Bassini (a cura di), *Diritti e libertà in Internet*, Firenze, 2017; M. Olivetti, *Diritti fondamentali e nuove tecnologie. Una mappa del dibattito italiano*, in *Revista Estudos Institucionais*, vol. 6, n. 2, maio/ago, 2020, 395-430. Sul tema dell'impatto dell'evoluzione tecnologica informatica sul diritto pubblico e sulla tenuta delle garanzie costituzionali si rinvia, inoltre, in generale, ai numerosi interessanti contributi presenti nel vol. 1 del *Liber Amicorum* per Pasquale Costanzo dedicato a *Costituzionalismo, Reti e Intelligenza Artificiale*, in *ConsultaOnLine*, 2020.

[3] 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*, cit. e R. Imperadori, *La responsabilità dell'Internet Service Provider per violazione del diritto d'autore: un'analisi comparata, Trento Law and Technology group, Student paper n. 21*, reperibile all'url: www.lawtech.jus.unitn.it .

DPCE online
ISSN: 2037-6677

del *Digital Services Act*[4] e del *Digital Market Act*[5], la disciplina di riferimento è stata rappresentata dalla Direttiva n. 2000/31/Ce[6] (la c.d. direttiva *e-commerce*) la quale, anch'essa, sanciva sostanzialmente il c.d. dogma della irresponsabilità degli intermediari digitali[7].

La progressiva evidenza delle peculiarità tecniche connesse al contesto informatico hanno tuttavia spinto a (ri)valutare la necessità di normare la dimensione tecnica del mezzo digitale e, dunque, a considerare l'esigenza di disciplinare con maggior rigore le questioni attinenti la responsabilità del *provider* e l'attività algoritmica. Le odierne ICT evidenziano infatti al medesimo tempo, capacità sia predittive sia manipolative: predittive, in quanto gli algoritmi, grazie al trattamento di una gran massa di dati (*Big Data*) sono capaci di rivelare relazioni (*correlation insights*) tra scelte, comportamenti, gusti, azioni e sulla base di tali informazioni sono in grado di costruire, dei modelli di comportamento individuali e collettivi; manipolative, perché la profilazione algoritmica contribuisce a selezionare i contenuti determinanti per la formazione dell'opinione pubblica. L'algoritmo difatti è in grado di definire gli utenti a partire dai dati che li riguarda - e che essi stessi consapevolmente o inconsapevolmente forniscono - (*profiling*) ed offre loro informazioni selezionate (*targeting*)[8]. Ciò conduce al paradosso per il quale, in un contesto come quello della rete *web*, ove circolano continuamente milioni di dati e di informazioni, i singoli individui vengono sostanzialmente chiusi in una bolla informativa realizzata dal filtro algoritmico (*filter bubble*)[9]. Si tratta di una "esposizione selettiva" per la quale, privati di fatto della possibilità di un'informazione libera e completa[10] gli

[4] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (Regolamento sui servizi digitali). https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R2065&from=EN

[5] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (Regolamento sui mercati digitali). Reperibile all'URL https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R1925&from=EN. Su regolamenti detti cfr. F. Zorzi Giustiniani, *L'Unione Europea e la regolamentazione del digitale: il Digital Services Packages e il codice di buone pratiche sulla disinformazione*, in *Nomos. Le Attualità nel Diritto*, n. 2, 2022.

[6] 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").

[7] La bibliografia sulla direttiva *e-commerce* è sterminata. Si rinvia esemplificativamente a M. Bassini, *Internet e diritto*, cit. ed alla bibliografia ivi citata.

[8] A. Perrini, *Microtargeting: cos'è e quali sono gli impatti per la protezione dei dati personali*, consultabile all'url: https://www.agendadigitale.eu/sicurezza/privacy/microtargeting-cose-e-quali-sono-gli-impatti-per-la-protezione-dei-dati-personali/ (23 marzo 2020).

[9] E. Pariser, *Il filtro. Quello che Internet ci nasconde*, Milano, 2012; Cfr. sul tema E. Longo, *Dai big data alle "bolle filtro": nuovi rischi per i sistemi democratici*, in *Percorsi costituzionali*, n. 1, 2019, 29-44; M. Bianca, *La filter bubble e il problema dell'identità digitale*, in *MediaLaws – Rivista di diritto dei media*, n. 2, 2019, 39 ss.

[10] Afferma efficacemente Sunstein a tal proposito che «se alle persone viene negato l'accesso a pareri contrastanti su argomenti di interesse pubblico e se, da parte loro, c'è

individui tendono ad estremizzare le proprie opinioni con un generale effetto polarizzante[11] che riguarda l'intera collettività[12]. In questo contesto il ruolo svolto dalle grandi aziende tecnologiche è cruciale in quanto esse «dietro l'apparente gratuità dei propri servizi, richiedono all'utente, quale contropartita […] la cessione (in varia misura e a vario titolo) di dati di eterogenea natura (riguardanti sia la sfera personale sia, più in generale, inclinazioni, gusti e preferenze)»[13] al fine tanto di potenziare la loro capacità pubblicitaria sul mercato quanto per rivendere questi dati a soggetti terzi[14].

L'attenzione del decisore politico si è dunque gradualmente spostata dalla mera garanzia della libertà di azione in Internet alla normazione di tutela dell'utente digitale dalla manipolazione della sua identità e dalla c.d. coercizione algoritmica.

Nell'approccio a tale tema l'azione europea e statunitense diverge. Ciò accade in relazione sia ad una diversa tradizione storica che connota tali contesti (liberista negli Usa e orientata al garantismo in Europa) sia in ragione di considerazioni dal sapore maggiormente geopolitico[15]: difatti, giacché nella lista delle prime dieci società del mondo per capitalizzazione, 7 afferiscono al comparto tecnologico e sono tutte statunitensi (Apple, Microsoft, Alphabet, Amazon, Nvidia, Meta, Tesla)[16], risulta intuitivo comprendere le ragioni per cui «gli USA hanno una posizione di antica primazia tecnologica da difendere, … mentre l'Europa ha tuttora un

come risultato una mancanza di interesse per questi punti di vista, si verifica una mancanza di libertà, qualunque sia la natura delle loro preferenze e scelte», *Republic.com. Cittadini informati o consumatori di informazioni?*, cit., 126.

[11] L'Agcom, in uno studio pubblicato a novembre 2018 (Agcom, *Rapporto Tecnico. Le strategie di disinformazione online e la filiera dei contenuti fake*, 9 novembre 2018. Il documento è disponibile a seguente link: https://www.agcom.it/documents/10179/12791484/Documento+generico+09-11-2018+1541763433144/e561edf2-a138- 443e-9937-303f68d92cc3?version=1.0.) ha rilevato come sussista un rapporto direttamente proporzionale fra la polarizzazione ideologica degli utenti dei *social network* e l'intensità e la frequenza delle loro attività in rete. Accade dunque che gli individui più schierati dal punto di vista ideologico ricorrono ad Internet come mezzo di comunicazione per informarsi sulle scelte politico-elettorali assai più ampiamente rispetto alle persone con scarso livello di polarizzazione ideologica. Sul punto cfr. M.R. Allegri, *Oltre la Par Condicio, comunicazione politico elettorale nei social media, fra diritto e autodisciplina*, Milano, 2020; G. Origgi, *La democrazia può sopravvivere a Facebook?*, cit. il quale efficacemente definisce tale condizione "vulnerabilità cognitiva" (447); O. Grandinetti, *La par condicio al tempo dei social, tra problemi "vecchi" e "nuovi" ma, per ora, tutti attuali*, in *MediaLaws – Rivista di diritto dei media*, n. 3, 2019, 92 ss.

[12] Cfr. sul tema E. Longo, *Dai big data alle "bolle filtro": nuovi rischi per i sistemi democratici*, cit.

[13] B. Rabai, *I Big Data nell'ecosistema digitale: tra libertà economiche e tutela dei diritti fondamentali*, in *Amministrare*, n. 3, 2017, 407.

[14] Sul tema cfr. la sezione monografica curata da E. Longo e A. Pin, *Oltre il Costituzionalismo? (parte II)*, in *Diritto Pubblico Comparato ed Europeo*, n. 1, 2023, 103 ss. nella quale figurano numerosi interessanti interventi dedicati alla tutela dei diritti e all'evoluzione del costituzionalismo contemporaneo a fronte del progresso digitale.

[15] 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*, n. 2, 2022, 323 ss.

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

DPCE online
ISSN: 2037-6677

notevole problema di autonomia e sovranità tecnologica, aggravato dall'uscita del Regno Unito dall'Unione»[17].

Queste divergenze si riversano inevitabilmente sul piano degli obiettivi strategici delle politiche dei detti Paesi in relazione ai quali, tendenzialmente, gli Stati Uniti d'America accentuano il profilo delle opportunità offerte dall'innovazione tecnologica digitale e conferiscono un'importanza significativa all'obiettivo di mantenere una *leadership* globale nello sviluppo e nell'impiego della stessa (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»[18] tecnologiche evidenziando un approccio maggiormente orientato alla precauzione[19].

A tutto ciò si aggiunge la concorrenza rappresentata da alcune potenze orientali (Taiwan, Cina e Giappone) fra le quali la Cina, peraltro, rappresenta un'alternativa ideologica del tutto antitetica agli Stati Uniti. La competizione con la Cina sembra atteggiarsi, dunque, come un inestricabile intreccio di antagonismo commerciale e ideologico che ha condotto gli Stati Uniti ad azioni politiche caratterizzate da un altrettanto peculiare commistione fra scelte alternativamente liberiste o protezionistiche in relazione alle quali non è sempre agevole distinguere se l'obiettivo perseguito è, genuinamente, la tutela dell'interesse nazionale alla sicurezza o (anche) la garanzia della *leadership* di mercato statunitense.

Difatti, l'orientamento normativo e giurisprudenziale statunitense in tema di disciplina del digitale prende le mosse da una tradizione liberista che connota il medesimo ordinamento con riguardo alla normativa ed alle garanzie della libertà di espressione tutelate dal I emendamento[20]. Il decisore politico e la giurisprudenza ne offrono peraltro un'interpretazione particolarmente ampia collegata, a ben vedere, alla volontà di tutelare le possibilità di espansione di un mercato digitale dominato dalla tecnologia statunitense e dunque, probabilmente, anche strumento di esportazione della stessa cultura americana nel mondo. Nondimeno, giacché nello scorrere del tempo, anche in tale esperienza non sono mancate le problematiche con cui confrontarsi concernenti i temi, di volta in volta, della difesa della dignità umana *on line* e della sicurezza nazionale, le reazioni a tali sfide sembrano evidenziare un'evoluzione protezionistica nell'azione politica statunitense che non costituisce un cambiamento di rotta, quanto il naturale prodotto delle reali ragioni alla base dell'iniziale scelta statunitense: solo apparentemente del tutto fautrice del libero mercato ma in realtà, sin dall'inizio, finalizzata a massimizzare il vantaggio tecnologico detenuto.

Il presente lavoro si prefigge pertanto di analizzare l'esperienza statunitense in tema di ecosistema digitale al fine di valutare questa

[17] G. Resta, *Cosa c'è di europeo nella proposta di regolamento Ue*, 325
[18] Cfr. ancora G. Resta, *Cosa c'è di europeo nella proposta di regolamento Ue*, 326.
[19] Sul punto ancora G. Resta, *Cosa c'è di europeo nella proposta di regolamento Ue*. 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, 29-50; L. Floridi, *The European Legislation on AI: a Brief Analysis of its Philosophical Approach*, in *Philosophy & Technology*, vol. 34, 2021, 215 ss.
[20] Cfr. F. Abrams, *The Soul of First Amendment*, New Haven, 2017.

ambivalenza fra liberismo e protezionismo nelle scelte politiche USA sul tema e di valutarne le ragioni politiche ed economiche.

2. I Emendamento e strumenti di comunicazione di massa: la giurisprudenza della Corte suprema federale

Negli Stati Uniti la Corte suprema federale ha affermato con chiarezza il principio per il quale il mezzo di comunicazione costituisce un elemento di cui tenere conto per valutare il regime più o meno restrittivo di applicazione del I emendamento[21]; ciò non ha condotto, tuttavia, come ben noto, ad una modulazione in termini restrittivi dell'interpretazione del I emendamento in ambito digitale.

La giurisprudenza in relazione alla quale la Corte suprema ha definito il principio per il quale le differenze nelle caratteristiche dei mezzi di informazione giustificano una differenziazione negli *standards* relativi all'applicazione del I Emendamento si è sviluppata, specificatamente con riguardo al mezzo radiotelevisivo, a partire dalla fine degli anni sessanta: nel 1969, nella decisione *Red Lion Broad. Co. v. FCC*[22], la Corte suprema valuta difatti la legittimità della c.d. *Fairness Doctrine*, una *policy* della *Federal Communications Commission* (FCC)[23], introdotta nel 1949, in base alla quale la Commissione, in considerazione della scarsità delle risorse nella diffusione radiofonica e televisiva, subordinava la concessione della licenza a trasmettere all'impegno da parte dei titolari delle relative licenze a fornire un servizio di informazione pubblica orientato al pluralismo e alla correttezza[24].

Il tema della scarsità delle risorse d'accesso al mezzo televisivo viene ripreso anche in altre decisioni successive ove la Corte sancisce la legittimità costituzionale di alcune disposizioni c.d. "*must carry*" finalizzate a garantire il pluralismo delle emittenti radiotelevisive imponendo, ad esempio, che una percentuale delle reti via cavo fosse riservata all'emittenza locale[25].

Tale giurisprudenza della Corte suprema, collegata alla limitazione della libertà di espressione in ambito radiotelevisivo, esonda negli anni seguenti oltre la mera valutazione quantitativa dell'emittenza spingendosi, in alcune limitate circostanze, a pronunciarsi anche sugli stretti contenuti veicolati tramite tali mezzi: nel 1987, nella decisione *FCC v. Pacifica Foundation*[26], la Corte suprema conferma ad esempio il potere della FCC di regolare, in circostanze limitate (stabilendo orari e condizioni di trasmissione), programmi che pur non "osceni" fossero qualificabili come "indecenti". La decisione *Pacifica*, in termini argomentativi risulta peraltro particolarmente significativa in quanto a fianco della motivazione concernente la "scarsità" del bene, uno dei perni in relazione al quale il

[21] *City of Los Angeles v. Preferred Communications, Inc.*, 476 U.S. 488, 496 (1986); *Red Lion Broad. Co. v. FCC*, 395 U.S. 367, 366-91 (1969).
[22] *Red Lion Broad. Co. v. FCC*, 395 U.S. 367 (1969).
[23] La *Fairness Doctrine* è tecnicamente fondata sul *Radio Act* del 1927 e sulla sez. 307 (licenze) del Titolo 47 (radiodiffusione) dello *US Code*.
[24] Sulla *Fairness doctrine* cfr. K.A. Ruane, *Fairness Doctrine, History and Constitutional Issues, CRS Report, July* 13, 2011.
[25] *Turner Broadcasting System v. FCC*, 512 US 622 (1994).
[26] *FCC v. Pacifica Foundation*, 438 U.S. 726 (1978).

DPCE online
ISSN: 2037-6677

relatore per la Corte ritiene di differenziare il regime di applicabilità del I emendamento al mezzo radiotelevisivo è legato alla passività dell'utenza ed alla sua estrema diffusione presso le abitazioni private.

La detta giurisprudenza restrittiva, inaugurata per i *mass media* radiotelevisivi, lascia inalterata tuttavia la disciplina dedicata alla carta stampata (alla quale dunque non si estende). Anche dopo la decisione del 1969 la diffusione del pensiero a mezzo stampa continua difatti a godere, nelle sentenze della Corte suprema federale, di un'ampia libertà: la conferma emblematica di tale differenza di approccio si riscontra nell'adozione, nel 1974, della decisione *Miami Herald publishing v. Tornillo*[27] ove la Corte suprema, in tema di diritto di replica, in una vicenda dai tratti estremamente similari a quelli accaduti nel caso *Red Lion*, senza peraltro citare mai quest'ultima decisione[28], sancisce che imporre alla carta stampata il diritto di replica significa obbligare la stampa a dei contenuti e, dunque, minarne il carattere di libertà.

Ciò che avviene per la carta stampata si reitera, *mutatis mutandis*, con riguardo alla giurisprudenza concernente l'applicabilità di possibili approcci restrittivi alla libertà di espressione *on line*. A partire dalla nota decisione *Reno v. ACLU*[29], del 1997, i precedenti giurisprudenziali definiti per l'emittenza radiotelevisiva vengono difatti considerati dalla Corte suprema come non applicabili operando dunque, in questo caso, un netto *distinguishing*.

Ciò si verifica effettivamente nella stessa sentenza *Reno* che riguardava l'incostituzionalità del *Communication Decency Act* del 1996. In tale decisione difatti il giudice Stevens, relatore per la Corte, affermò che, a differenza dei *mass media* tradizionali, Internet non dovesse essere considerato altrettanto "invasivo" in quanto l'accesso alle informazioni *on line* richiedeva un'attività di ricerca specifica dell'utente che, dunque, non poteva essere qualificato come soggetto passivo[30]. Inoltre la decisione di maggioranza metteva in evidenza il fatto che Internet non fosse caratterizzato da una intrinseca limitatezza delle vie di accesso[31].

[27] *Miami Herald publishing v. Tornillo*, 418 US 241 (1974).
[28] Criticamente sulla decisione *Tornillo* cfr. D.C. Stephenson, *Access to the Printed Media by Political Candidates: Miami Herald Publishing Company v. Tornillo*, in *SMU law Review*, vol.28, n. 5, 1974.
[29] *Reno v. American Civil Liberties Union* , 521 US 844 (1997). Sulla decisione *Reno* la bibliografia è sterminata. Ci si limita a rinviare a R.H. Barrage, *Reno v. American Civil Liberties Union: First Amendment Free Speech Guarantee Extended to the Internet*, in *Mercer Law Review*, vol. 49, 1997-1998, 625 ss.; A. J. Slitt, *The Anonymous Publisher: Defamation on the Internet after Reno v. American Civil Liberties Union and Zeran v. America Online*, in *Connecticut Law Review*, vol. 31, 1998-1999, 389 ss.
[30] «*the Internet is not as "invasive" as radio or television. The District Court specifically found that [c]ommunications over the Internet do not `invade an individual's home or appear on one's computer screen unbidden. Users seldom encounter content by accident*», *Reno, Opinion of the Court, Part V.*
[31] «*Unlike the conditions that prevailed when Congress first authorized regulation of the broadcast spectrum, the Internet can hardly be considered a "scarce"' expressive commodity. It provides relatively unlimited, low-cost capacity for communication of all kinds*», *Reno, Opinion of the Court, Part* V.

3. La sez. 230 del Communication Decency Act: la *content moderation* e le esigenze del liberismo digitale

La decisione *Reno*, adottata nella seconda metà degli anni novanta, riflette il contesto di ampia fiducia nelle prospettive cui Internet apriva, clima cui corrispondeva un atteggiamento tendenzialmente libertario nella normazione del mezzo. Nondimeno, la decisione è stata criticata, sin dalla sua adozione, da parte di chi, già da allora, percepiva quanto la Corte suprema sovrastimasse le capacità attive di autoprotezione degli utenti digitali nella loro possibilità di scelta fra contenuti desiderati ed indesiderati[32]; tale osservazione, probabilmente valida già all'epoca, sembra esserlo tanto più ad oggi considerando che le evidenze attuali (riguardanti le problematiche della trasparenza algoritmica, del *microtargeting* ecc.) sottolineano ancora di più la fragilità di quell'impostazione iniziale.

Risultò da subito peraltro evidente come la decisione *Reno*, di fatto, fosse in linea con l'approccio libertario assunto solo l'anno precedente dal Congresso il quale, con l'adozione della notissima sezione 230 del *Title 47* dello *Us Code* (*Communication Decency Act*), sanciva la completa deresponsabilizzazione degli *Internet provider* per i contenuti caricati da terzi attraverso la previsione della c.d. clausola del buon samaritano[33].

La normativa congressuale, adottata nel 1996, seguiva alcune decisioni in tema di responsabilità del *provider*, pronunciate dai giudici ordinari nel quinquennio precedente in relazione alle quali si era reso evidente che le soluzioni normative concernenti il tema della responsabilità del *provider* aprivano a tante questioni inestricabilmente intrecciate fra loro le quali potevano caratterizzarsi per bilanciamenti molto differenti. Nel 1991, nella decisione *Cubby v. Compuserve*[34], la Corte distrettuale per il *Southern District* dello Stato di New York aveva elaborato un'equiparazione fra una piattaforma ospitante una *newsletter* ed un edicolante, tentando di applicarne il relativo regime di responsabilità; diversamente, nel 1995, nella decisione *Stratton Oakmont v. Prodigy Service Company*[35] la Corte suprema di New York addivenne a conclusioni opposte condannando il gestore di una piattaforma (*Prodigy*) che ospitava una bacheca virtuale ritenendolo responsabile per i contenuti diffamatori pubblicati da terzi; nell'assumere la propria decisione nel caso *Prodigy* la Corte aveva centrato il proprio ragionamento argomentativo sul fatto che la piattaforma svolgeva, in conformità con i termini d'uso, un'attività di moderazione e che, in considerazione di tale esercizio di *content moderation*, lo *standard* applicato nel precedente *Compuserve* non fosse applicabile (in quanto la piattaforma dimostrava di

[32] D. K. Djavaherian, *Reno v. ACLU*, in *Berkeley Technology Law Journal*, vol. 13, 1998, 371 ss., spec. 380.

[33] Sul tema la dottrina è sterminata; si rinvia, a titolo esemplificativo, a P. Ehrilich, *Communication Decency Act, sec.230*, in *Berkeley Technology Law Journal*, vol. 17, n. 1, 2002, 401 ss.; V.C. Brannon, E. N. Holmes, *Section 230: An Overview*, in *Congressional Research Service* (https://crsreports.congress.gov R46751), April 7, 2021; M.G. Leary, *The Indecency and Injustice of Section 230 of the Communications Decency Act*, in *Harvard Journal of Law & Public Policy*, vol. 41, n. 2, 553 ss., 2018.

[34] *Cubby v. Compuserve*, 776 F Supp. 135 (S.D.N.Y. 1991).

[35] *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 23 *Media L. Rep.* 1794 (N.Y. Sup. Ct. 1995).

DPCE online
ISSN: 2037-6677

essere in qualche modo implicata nella selezione dei contenuti esposti). Tali osservazioni portarono la Corte suprema di New York a paragonare i gestori della stessa piattaforma *on line* ad un editore (piuttosto che, come nel caso *Compuserve*, ad un edicolante). La detta impostazione, tuttavia, innescava delle conseguenze problematiche in quanto poteva finire per spingere i gestori delle piattaforme a non praticare alcuna forma di moderazione dei contenuti o, al contrario, poteva condurre a forme di censura *on line* esasperate. Fu dunque in relazione a tale rischio che il Congresso si risolse all'adozione della nota normativa del CDA esonerando i *provider* da ogni responsabilità (salvo alcune limitate eccezioni[36]) per contenuti caricati da terzi sulle loro piattaforme.

La giurisprudenza successiva all'adozione del CDA ne ha confermato e, se possibile ampliato, l'impianto di base. Nel 1997, nel caso *Zeran v. America Online*[37] la Corte d'appello per il Quarto circuito, sancisce ad esempio l'ampiezza della portata della sez. 230 stabilendo che essa garantiva il *provider* anche quando quest'ultimo fosse stato a conoscenza della natura illecita (mediante segnalazione) dei contenuti presenti sulla sua piattaforma. Tale interpretazione finiva per ampliare l'immunità del *provider* al di là dei limiti già estesi stabiliti nel precedente *Compuserve* in quanto in *Zeran* la Corte stabiliva che la sezione 230 non si limitava ad escludere una qualificazione editoriale dei *provider* ma precludeva ad essi anche l'applicabilità del regime di responsabilità del distributore dei contenuti (il famoso edicolante).

[36] 47 USC sez. 230 (e)(5).

[37] 129 F3d 327 (4th cir. 1997). Il ricorrente era stato vittima di minacce di morte e molestie telefoniche per un anno dopo che i suoi recapiti erano stati pubblicati da un utente anonimo su un forum interattivo gestito dal provider *America Online*, in collegamento alla vendita di oggetti satirici sull'attentato terroristico di Oklahoma City. Dunque, il contenuto del post era illecito. Il richiedente aveva ripetutamente chiesto l'eliminazione dal forum dei suoi dati personali, ma l'*America Online* vi aveva proceduto solamente a distanza di parecchio tempo non sufficiente ad impedire, nel frattempo, la comparsa di altri *post* che riportassero i suoi recapiti. Nel processo, il ricorrente aveva asserito la negligenza della *America Online* nella gestione del *post*, argomentando che la *section* 230 non si applicasse a beneficio dell'*America Online*, poiché il ruolo di quest'ultima nella vicenda si configurava alla stregua non di un editore o di un produttore (per riprendere la terminologia impiegata nell'*Act*) bensì di un "distributore", equiparabile ad un'edicola, e pertanto responsabile se al corrente dell'illiceità del contenuto in questione. Ad avviso del ricorrente, *America Online* era consapevole dell'illiceità proprio in conseguenza delle ripetute richieste di cancellazione da lui avanzate. La Corte d'Appello ha stabilito invece che l'immunità era comunque applicabile ad *America Online*, perché ritenere il provider colpevole per aver semplicemente distribuito un dato illecito lo avrebbe equiparato al produttore del contenuto. Una dichiarazione di colpevolezza avrebbe indotto i *providers* ad una censura eccessiva delle comunicazione, per timore di essere chiamati a rispondere ed inoltre, l'assenza di immunità avrebbe comportato, per i *providers*, la necessità di eseguire una verifica circa la sussistenza di estremi per una eventuale diffamazione, con una decisione che avrebbe dovuto essere pressoché istantanea, ciò che è praticamente impossibile data la natura delle comunicazioni su internet. Si è in tal modo superata l'incertezza ingenerata da due casi in cui si erano posti dubbi circa la responsabilità del provider: *Cubby, Inc. v. CompuServe*, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991) e *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

La vasta estensione dei caratteri dell'immunità garantita dalla sezione 230 viene ulteriormente ribadita in successive decisioni statunitensi nelle quali è affermato il principio per il quale essa si estende anche ai casi in cui il terzo, produttore delle asserite diffamazioni, è vincolato al *provider* per mezzo di un contratto di lavoro autonomo[38] o nei quali il terzo abbia commesso un evidente illecito penale[39].

4. La struttura della libertà di espressione nell'arena digitale: i pericoli insiti nella *collateral censorship* e le proposte dottrinali e giurisprudenziali sul tema

La normativa e la giurisprudenza di impronta liberale e liberista che si afferma inizialmente è destinata, nello scorrere del tempo, ad evidenziare importanti criticità[40]. Ciò avviene quando si rende palese che la struttura "triangolare" delle relazioni che caratterizza la libertà di espressione *on line* (ordinamento giuridico, individui/utenti, aziende digitali) presenta caratteristiche tali da non poter essere, in effetti, adeguatamente ordinata sulla base dei criteri prevalentemente utilizzati in precedenza i quali

[38] *Blumenthal v. Drudge and America Online*, Inc., 992 F. Supp. 44 (D.C.C. 1998). Il giornalista (columnist) internet Matthew Drudge aveva esposto affermazioni asseritamente diffamatorie nei confronti di Sidney Blumenthal, noto ex-giornalista e dipendente della Casa Bianca. Drudge riceveva circa 3.000 dollari mensili come corrispettivo dei suoi servizi; nel contratto di lavoro, l'*America Online* si era riservata il diritto di rimuovere qualsiasi contenuto in violazione dei *Terms of Service* della *America Online* stessa, ma la responsabilità ed il controllo editoriale rimanevano interamente del giornalista. *Blumenthal* ha convenuto in giudizio sia Drudge sia la *America Online*, quest'ultima in qualità di creatrice del post che ha scatenato la controversia, data la riserva presente nel contratto. L'immunità conferita dalla *Section* 230 sarebbe dunque venuta meno, secondo Blumenthal, poiché l'informazione non era stata "fornita da un altro fornitore di contenuto informativo". La Corte ha tuttavia respinto la tesi di Blumenthal, sostenendo che Drudge non era né un agente né un dipendente dell'*America Online*, bensì un lavoratore autonomo; pertanto, l'informazione proveniva effettivamente da un fornitore di contenuti diverso e *America Online* poteva godere dell'immunità anche in questo caso

[39] In *Doe v. America Online*, Inc., 1997 WL 374223 *1, aff'd, *Doe v. America Online*, Inc., No. 97-2587, 1998 WL 712764 (Fla. Ct. App. Oct. 14, 1998), la madre di un utente minorenne delle *chat-rooms* gestite da *America Online* aveva denunciato il *provider*, asserendo che un utente avesse ripetutamente richiesto di poter visionare un filmato nel quale l'utente avrebbe compiuto atti sessuali con il figlio. La madre ha sostenuto che *America Online* era stata negligente nel permettere tali richieste. I *Terms of Service* dell'*America Online* contenevano un espresso divieto della distribuzione di materiale "illegale, nocivo, osceno o comunque indesiderabile" per mezzo dei suoi canali telematici, ed il *provider* si era riservato il diritto di eliminare tale contenuto. Nonostante fossero giunte molte e ripetute richieste di bloccare l'attività dell'utente, *America Online* non aveva preso alcun provvedimento nei suoi confronti. La madre aveva da ciò dedotto che la condotta dell'utente, ma anche quella dell'*America Online*, costituissero una violazione delle leggi dello Stato della Florida che sanzionavano la partecipazione nella distribuzione della pedopornografia. La Corte d'Appello dello Stato della Florida ha ripreso la suddetta sentenza *Zeran v. America Online*, per stabilire che un *provider* può godere dell'immunità sia in quanto editore, sia in quanto distributore.

[40] Sul punto cfr. J.M. Balkin, *Old School/New School Speech Regulation*, in *Harvard Law Review*, vol. 127, n. 8, 2014, 2296 ss.

DPCE online
ISSN: 2037-6677

presuppongono, invece, un assetto tendenzialmente diadico o dualista delle relazioni fra individui ed autorità statale[41]; ciò tanto più, peraltro, tenendo conto che, nel tempo, le grandi compagnie *tech* divengono sostanzialmente compartecipi di numerose importanti scelte afferenti ad alcune questioni che attengono la struttura più intima dell'architettura di uno Stato (Moneta, Giurisdizione, Dibattito pubblico e flussi elettorali) [42].

Peraltro, l'esperienza statunitense, rispetto al contesto europeo, registra una minore capacità di adattamento e di evoluzione in funzione di un cambiamento del genere nella struttura dei rapporti comunicativi in quanto, mentre nell'esperienza europea la struttura delle garanzie normative attinenti la libertà di espressione del pensiero è ancorata oramai da lungo tempo ad una concezione pluralistica del medesimo assetto (per la quale, oltre alla relazione libertà e autorità, la normativa si concentra sulla disciplina dei rapporti interindividuali e sulla garanzia del rispetto reciproco della dignità umana nell'esercizio della libertà di espressione), l'ecosistema giuridico statunitense si è sempre rivelato restio a limitare il *free speech* in relazione alla tutela della correttezza dei rapporti interindividuali proponendosi, dunque, come un modello tendenzialmente dualista[43].

[41] Sul tema cfr. J.M. Balkin, *Free speech is a Triangle*, in *Columbia Law Review*, vol. 118, 2011, 2011 ss.

[42] A. Vanzoni, *Cyber-costituzionalismo: la società digitale tra silicolonizzazione, capitalismo delle piattaforme e reazioni costituzionali*, cit.

[43] Emblematica in tal senso è la giurisprudenza sulle c.d. "vere minacce" (*True Threats*) fondata, quale primissima categorizzazione, sul precedente *Watts v. US Watts v. US*, 394 US 705 (1969) e sviluppatasi da ultimo con l'assunzione della più recente decisione *Counterman v. Colorado*, 600___US (2023), *Docket n.* 22138.

Il test concernente la definizione di una minaccia come "vera" è stato inizialmente definito dalla Corte suprema nel 1971 nel caso *Cohen v. California*, 403 US 15 (1971) in cui il giudice federale ha chiarito che un'espressione verbale violenta, per essere illegittima, deve essere rivolta specificatamente a qualcuno.

I casi successivi, soprattutto a partire dagli anni 2000, si sono incentrati sul tema della necessità di dimostrare o meno l'intento soggettivo di un imputato ad avanzare una "vera minaccia". Nel 2003 nel caso *Virginia v. Black*, 538 U.S. 343 (2003) la Corte suprema, pur affermando che uno Stato può legittimamente adottare una normativa che vieti di bruciare croci a scopo intimidatorio, non può per inverso considerare un croce bruciata quale prova "prima facie" di un intento minaccioso. Nella successiva decisione *Elonis v.* US, 575 US_(2015) (sviluppatosi in relazione a delle minacce, pubblicate su Facebook da parte di un uomo nei confronti dell'ex moglie) la Corte suprema è tornata sul tema ed ha sancito che un'intimidazione per essere "vera" deve essere caratterizzata da un provato intento soggettivo e non solo essere percepita oggettivamente come tale (secondo uno *standard* tipico di un uomo ragionevole).

Il tema delle *True Threats* (peraltro nello specifico ambito digitale) è stato recentemente ripreso dalla Corte suprema nella decisione *Counterman*. In tale circostanza il giudice federale è ritornato sulla qualificazione dell'intento soggettivo dell'agente specificando la categoria e dunque inasprendo lievemente il *test*. Collegandosi ad uno *standard* definito in altra giurisprudenza (in tema di violenza domestica nella decisione *Voisine v. US*, 579 USA___ (2016), *Docket n.*14-10154) la Corte ha stabilito che, al fine di definire una vera minaccia, è sufficiente che l'imputato abbia adottato un comportamento "imprudente" (*recklessness*) ovvero abbia "consapevolmente ignorato il rischio sostanziale (ed ingiustificabile) che la sua condotta avrebbe causato un danno". Tale giurisprudenza sembra richiamare nell'esperienza italiana l'istituto del dolo eventuale. Tuttavia in questa particolare giurisprudenza si avverte una sostanziale differenza: nel contesto italiano la categorizzazione è enucleata con l'intento di definire il regime di

In un contesto normativo come quello statunitense, l'applicazione alla rete delle garanzie del I emendamento sommata alla deresponsabilizzazione del *provider* conducono allo sviluppo di modalità di controllo delle forme espressive *on line* esclusivamente fondate sui meccanismi di moderazione dei contenuti affidate alle compagnie *tech* e, dunque, a forme significative di privatizzazione della censura ("*collateral censorship*") suscettibili di assumere caratteri del tutto "arbitrari" o, cosa ancor più pericolosa, basati su bilanciamenti di interessi posti in essere e risolti direttamente dalle *corporations*[44]. Sembra dunque verificarsi il paradosso per il quale, a fronte di un'apparente estrema libertà di espressione *on line*, nel contesto statunitense, il fenomeno della privatizzazione della censura può finire per rappresentare uno strumento di limitazione della circolazione del libero pensiero in mano a dei privati consentendo alle aziende di modulare la diffusione delle opinioni sulla base delle convenienze aziendali[45]. Le garanzie costituzionali poste dal *Bill of Rights* in quanto strutturate, secondo quanto accennato poc'anzi, in consonanza con una concezione diadica (piuttosto che triangolare) dei rapporti connotanti la libertà di espressione non sono in grado di impedirlo: la specifica dicitura del I emendamento, definita come divieto per l'autorità statale di interferire nella libera espressione del pensiero, è tale da non poter ritenersi applicabile alle aziende digitali che gestiscono le piattaforme *social* ed i canali del *web*[46].

Facendo leva su di una particolare ricostruzione giurisprudenziale, una parte minoritaria della dottrina statunitense ha tentato, in realtà, una lettura peculiare del contesto digitale tale da definire i *social network* alla stregua di *public forum* (e le aziende telematiche alla stregua di *State Actors*) che, in

responsabilità di un reo (in termini di definizione di dolo o colpa); nel contesto statunitense invece, nell'ambito della giurisprudenza riferita, la categoria della *recklessness* serve a definire la stessa sussistenza di una responsabilità o meno dell'eventuale imputato.

[44] Cfr. sul tema M. Monti, *Privatizzazione della censura e Internet Platform: la libertà d'espressione e i nuovi censori dell'agorà digitale*, in *Rivista italiana di informatica e Diritto*, n. 1, 2019, 35 ss.

[45] Si viene pertanto a determinare «la singolare situazione per cui gli stessi soggetti che si sono trovati a gestire gli strumenti tecnologici che rendono possibile la più ampia partecipazione all'accesso ed alla diffusione dell'informazione sugli spazi digitali sono allo stesso tempo coloro i quali controllano il flusso dei contenuti che possono transitare sulla rete, in quanto presiedono alla loro rimozione, selezione ed organizzazione», R. Petruso, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a confronto*, Torino, 2019.

[46] Sin dal 1883 la Corte suprema ha chiarito che: «*The first section of the Fourteenth Amendment (which is the one relied on), after declaring who shall be citizens of the United States, and of the several States, is prohibitory in its character, and prohibitory upon the States. It declares that: "No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws".*

It is State action of a particular character that is prohibited. Individual invasion of individual rights is not the subject matter of the amendment. It has a deeper and broader scope. It nullifies and makes void all State legislation, and State action of every kind, which impairs the privileges and immunities of citizens of the United States or which injures them in life, liberty or property without due process of law, or which denies to any of them the equal protection of the law», *Civil Right Cases*, 109 US 3 (1883), at 10-11.

DPCE online
ISSN: 2037-6677

ragione di tale ricostruzione, sono vincolate al rispetto dei limiti posti dal primo emendamento[47]. La detta teoria affonda le proprie radici in quanto sancito in una decisione risalente nel caso *Marsh v. Alabama*[48], del 1946. La vicenda giurisprudenziale riguardava una *company town*, ovvero una città edificata e di proprietà di un'impresa privata; in un centro abitativo di tal genere la sig.ra Marsh iniziò a distribuire materiale religioso ma fu prima redarguita e poi censurata dagli addetti alla sicurezza della cittadina in quanto la sua condotta non era consentita dai regolamenti aziendali. In una decisione (assunta 5 a 3) la Corte Suprema riconobbe tuttavia che la proprietà privata «*does not always mean absolute dominion*» e che la funzione pubblica di quel contesto rispetto alla vita della comunità imponeva di tutelare la libertà di espressione giacché «*the public in either case has an identical interest in the functioning of the community in such manner that the channels of communication remain free*»[49]. In una successiva decisione, *Hudgens v. NLRB*[50], del 1976, la Corte suprema ha poi chiarito che per essere qualificato quale *State Actor*, un soggetto privato deve svolgere le medesime funzioni di controllo di un governo o di una municipalità e non devono esistere alternative altrettanto efficaci per la diffusione delle idee censurate dallo stesso[51].

Considerando i riferiti precedenti è stato dunque ipotizzato che alle piattaforme digitali sia applicabile la *State Action Doctrine* e che le stesse possano essere considerate limitate dal I emendamento al pari di un'autorità statale.

Nonostante alcune decisioni in senso contrario nella giurisprudenza statale[52], l'applicabilità della *State Actor Doctrine* alle piattaforme digitali sembrava aver trovato conforto in una più recente decisione della Corte suprema federale, il caso *Packingham v. North Carolina*[53] nella quale la Corte aveva dichiarato l'incostituzionalità di una legge dello stato della North Carolina che impediva l'iscrizione su Facebook ai c.d. *registered sex offenders* affermando che impedire l'«*access to social media altogether is to prevent the user from engaging in the legitimate exercise of First Amendment rights*» e specificando

[47] Riferiscono di tale teoria M. Monti, *Privatizzazione della censura e Internet platforms: la libertà d'espressione e i nuovi censori dell'agorà digitale*, pp. 42 ss.; M.R. Allegri, *Oltre la par condicio*, cit. 65 ss., Cuniberti, *Potere e libertà nella rete*, in *Media Laws*, n. 3, 2018.
[48] *Marsh v. Alabama*, 326 U.S. 501 (1946).
[49] *Marsh v. Alabama*, 326 U.S. at 501 (1946).
[50] *Hudgens v. NLRB*, 424 U.S.507 (1976).
[51] Tale specificazione è collegata ad un'altra decisone sul medesimo tema ovvero *Lloyd Corp. v. Tanner*, 407 U.S. 551 (1972) nella quale la Corte si è pronunciata sulla legittimità di un divieto alla distribuzione di manifesti contro la guerra in Vietnam, messo in atto da un centro commerciale stabilendo che non vi fosse violazione del I emendamento giacché coloro che volevano distribuire i volantini potevano aver accesso ad altri luoghi pubblici nelle vicinanze e, quindi, a mezzi alternativi di diffusione del pensiero altrettanto efficaci.
[52] *Langdon v. Google*, Inc., 474 F. Supp. 2d 622, 631 (D. Del. 2007); Green v. Am. Online, 318 F.3d 465, 472 (3d Cir. 2003); *Nyabwa v. Facebook* , 2018 US Dist. LEXIS 13981, Civil Action No. 2:17-CV-24, *2 (SD Tex.) (26 gennaio 2018).
[53] *Packingham v. North Carolina*, 582 U.S. (2017). L bibliografia è molto vasta. Ci si limita a rinviare esemplificativamente a M. Burnette-McGrath, *Packingham v. North Carolina, in Ohio Northern University Law Review*, vol. 44, n. 1, 2019, 117 ss.; O. Soldatov, *The Transformative Effect of Social Media: Preliminary Lessons from the Supreme Court Argument in Packingham v. North Carolina*, in *DPCE on line*, n. 2, 2017, 417 ss.

che i *social network* attuali, per le peculiari caratteristiche che li connotano, sono da considerarsi quali «*modern public square*» e «*perhaps the most powerful mechanisms available to a private citizen to make his or her voice heard*»[54].

Nondimeno, una ancor più recente decisione ha inferto una battuta d'arresto a tale ricostruzione: nel 2019, nella decisione *Manhattan Community Access Corp v. Halleck*[55], la Corte suprema ha difatti chiarito che «*The Free Speech Clause of the First Amendment constrains governmental actors and protects private actors. To draw the line between governmental and private, this Court applies what is known as the state-action doctrine. Under that doctrine, as relevant here, a private entity may be considered a state actor when it exercises a function "traditionally exclusively reserved to the State*» definendo dunque in termini restrittivi le circostanze in relazione alle quali un'azienda privata può essere considerata come vincolata agli stessi limiti dell'autorità pubblica[56]. Se pur la decisione riguardava una rete televisiva, il tenore dell'argomentazione della decisione, in alcuni passaggi chiave, sembra indirizzarla ad una portata che si estende anche alle piattaforme digitali («*In short, merely hosting speech by others is not a traditional, exclusive public function and does not alone transform private entities into state actors subject to First Amendment constraints*»[57]) e ciò conduce, dunque, almeno per il momento, a dover considerare ancora di minoranza tale teoria giurisprudenziale.

Ciò considerando è possibile affermare che l'approccio liberista statunitense con riguardo alla normazione sulla libertà di espressione on line, orientato a garantire la crescita economica delle grandi aziende

[54] La vicenda ricorda in parte quanto accaduto recentemente nel contesto italiano in relazione al cosiddetto caso *Casapound*: il 9 settembre *Facebook* ha deciso di disattivare le pagine nazionali e territoriali del movimento *Casapound* Italia e di alcuni movimenti adesso vicini. La motivazione era che i contenuti di tali pagine violavano le condizioni d'uso del *social network* (fra cui il divieto di incitamento alla violenza sancito nel punto due degli *standards* della *community* ed il divieto di istigazione all'odio sancito nel punto 13). L'associazione *Casapound* ha presentato un ricorso d'urgenza al tribunale di Roma (ex articolo 700 c.c.) ottenendo un'ordinanza cautelare emessa dal medesimo tribunale in sede monocratica il 12 dicembre 2019 (RG n. 59264/2019, ordinanza pubblicata anche in *Diritto di Internet*, n. 1, 2020,pp. 63 ss.) che ha accolto integralmente le ragioni dei ricorrenti imponendo a *Facebook Ireland limited* l'immediata riattivazione della pagina dell'associazione e del profilo personale dell'amministratore delegato. Nell'ordinanza viene sottolineato «il rilievo preminentemente assunto dal servizio di Facebook parentesi o di altri social network adesso collegati parentesi con riferimento all'attuazione di principi cardine essenziali dell'ordinamento come quello del pluralismo dei partiti politici (articolo 49) al punto che il soggetto che non è presente su Facebook è di fatto escluso (o fortemente limitato) dal dibattito politico italiano».

[55] *Manhattan Community Access Corp v. Halleck*, 587 US_ (2019). La decisione è commentata da G. L. Fisher, *Lights, Camera, State Action: Manhattan Community Access Corp. V. Halleckin*, in *Cardozo Law Review De Novo*, 2020, 165 ss.

[56] «*Relying on this Court's state-action precedents, the producers assert that MNN is nonetheless a state actor subject to First Amendment constraints on its editorial discretion. Under this Court's cases, a private entity can qualify as a state actor in a few limited circumstances—including, for example, (i) when the private entity performs a traditional, exclusive public function, see*, e.g., Jackson, *419 U. S., at 352–354; (ii) when the government compels the private entity to take a particular action, see*, e.g., *Blum* v. *Yaretsky, 457 U.S. 991, 1004–1005 (1982); or (iii) when the government acts jointly with the private entity*», 587 U.S. ___ (2019), part. B II.

[57] 587 U.S. ___ (2019), part. B II.

DPCE online
ISSN: 2037-6677

americane del *tech*, finisce paradossalmente per soffocare la filosofia liberale che, in consonanza con la tradizione culturale del Paese dovrebbe, al medesimo tempo, caratterizzare il contesto digitale nell'ottica statunitense. Ciò in quanto le scelte normative e giurisprudenziali del Paese finiscono di fatto per consegnare alle grandi aziende del digitale il controllo sulla circolazione dei contenuti sul web deprimendo, in sostanza, l'effettiva tutela del *free speech*.

Un momento di riflessione nel contesto statunitense in tema di responsabilizzazione del *provider* è stato impresso dall'adozione, il 28 maggio 2020, da parte dell'allora Presidente Donald Trump, dell'*Executive Order 13925 Preventing Online Censorship* ("EO13925").

Era accaduto che, durante le elezioni presidenziali statunitensi del 2020, Twitter aveva valutato non del tutto attendibili alcuni dei *tweet* del Presidente Trump in tema di frode elettorale per corrispondenza ed aveva dunque allegato ad essi delle segnalazioni "*fact check*".

Il Presidente Trump, in reazione a tale situazione, aveva accusato Twitter di "interferire" con le libere elezioni e di "impedire" il *free speech* sulla piattaforma *social* ed aveva pertanto predisposto un apposito *Executive Order* nel quale, ponendo in evidenza il fatto che i *social media* non possono, ad oggi, più considerarsi quali *hosting provider* neutrali, giacché sono in grado di favorire la circolazione di alcune idee o reprimerne altre, la disciplina che li riguarda, specificatamente la sez. 230 del CDA ed in particolare la clausola c.d. del buon samaritano[58], necessita di essere aggiornata rispetto alle scelte compiute decenni or sono.

L'ordine esecutivo 13925 è stato criticato sotto innumerevoli profili a partire dalla estrema carica retorica che lo caratterizza, passando per la sua inopportunità politica, sino alla sua dubbia legittimità in termini giudici[59]. Il *Center of Democracy and Technology* ha inoltre immediatamente presentato un ricorso avverso tale atto governativo[60]. Considerato, peraltro, un tentativo maldestro da parte di Trump di condizionare (attraverso l'intimidazione) le politiche sulla censura delle grandi aziende digitali a proprio favore a ridosso della campagna elettorale per il rinnovo della Presidenza[61], l'*Executive Order* è stato prontamente ritirato dal successore alla casa Bianca, Joe Biden, il 14 maggio 2021[62].

Alla teoria dello spazio digitale quale foro pubblico è collegato anche l'*iter* argomentativo sviluppato da un giudice distrettuale di New York che ha ritenuto qualificabile come *public forum* lo spazio interattivo del profilo Twitter di Donald Trump sancendo come illegittima la decisione dell'allora

[58] *Clause* 230(c)(2).
[59] Sul punto si rinvia a tutte le considerazioni di G.F. Ferrari, *L'executive order sulla prevenzione della censura online: quali effetti sull'autonomia dei social network?*, in *DPCE OnLine*, n. 2, 2020, 1145 ss.
[60] *Center for Democracy and Technology v. Trump, US District Court for the District of Columbia, case n. 20-1456*, 6/02/2020.
[61] Sul punto cfr. ancora G.F. Ferrari, *L'executive order sulla prevenzione della censura online: quali effetti sull'autonomia dei social network?*, cit.
[62] *Executive Order on the Revocation of Certain Presidential Actions and Technical Amendment.* Reperibile all'url: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/14/executive-order-on-the-revocation-of-certain-presidential-actions-and-technical-amendment/ .

Presidente degli Stati Uniti di bloccare alcuni utenti sul suo *account*[63] come contromisura al fatto che si fossero espressi in modo contrario alle sue politiche. Questa vicenda giudiziaria si inserisce in una corrente giurisprudenziale che considera gli *account social* dei rappresentanti politici e dei funzionari del governo quali *forum* pubblici nel cui ambito una selezione dell'opinione ed una repressione della stessa attraverso l'eliminazione di alcuni partecipanti al dibattito, effettuata dai titolari dell'*account*, corrisponde ad una violazione del I emendamento[64]. Non si tratta tuttavia di una giurisprudenza che intende in qualche modo responsabilizzare i *provider*: le sentenze dette, difatti, sono orientate più che altro a qualificare in termini sostanziali la differenza fra tipologie di *account* a seconda del titolare dello stesso (per le funzioni che esso svolge in un determinato momento) traendone le relative conclusioni.

La problematica non è estranea anche al contesto europeo ove recentemente si è espressa in merito anche la Corte EDU[65] nel caso *Sanchez v. Francia* del 15 maggio 2023. La diversa prospettiva attraverso cui tale questione è declinata in ambito CEDU sottolinea tuttavia, ancora una volta, la divergenza negli approcci europeo e statunitense. Nella vicenda giurisprudenziale CEDU infatti il ricorrente (un politico francese di estrema destra) lamentava la violazione dell'art.10 della Convenzione europea nella condanna da lui subita per non aver rimosso importanti discorsi d'odio nei confronti di un avversario politico e della sua compagna di origini nordafricane. Un contesto, dunque, in parte completamente ribaltato rispetto a quello statunitense: se in tale ultimo ambito il tema consiste nel sanzionare il politico che limita la libertà di espressione sui suoi *account*, nel contesto europeo la problematica attiene alla responsabilità vicaria dell'esponente politico che non censura sul proprio *account* gravi discorsi d'odio.

5. La promozione della primazia tecnologica AI e la giurisprudenza sulla raccomandazione algoritmica

[63] *Knight First Amendment Institute at Columbia University, Rebecca Buckwalter et al. v. Donald J. Trump, Hope Hicks, Sarah Huckabee Sanders, And Daniel Scavino*, 17 Civ. 5205 (NRB), 23 maggio 2018.

[64] *Davison v. Randall*, 912 F.3d 666 (4th Cir. 2019); Diversamente si è pronunciato l'Ottavo circuito nel caso *Campbell v. Reisch*, No. 19-2994 (8th Cir. 2021): ribaltando la precedente decisione della Corte di distretto e distinguendola dai precedenti *Davidson* e *Knight*, la Corte ha infatti evidenziato che in tale occasione il rappresentante del congresso citato in giudizio per aver rimosso dal proprio account *twitter* alcune persone utilizzava il medesimo *account* a fini elettorali (un'attività di natura privata) e non istituzionali (caso in relazione al quale sarebbe stato vincolato al rispetto del I emendamento). Sul tema si rinvia a al commento: *Eight Circuit Finds State Representative Not a State Actor When Blocking Constituents on Twitter — Campbell v. Reisch*, 986 F.3d 822 (8th Cir. 2021), *reh'g and reh'g en banc denied*, No. 19-2994, 2021 BL 76260 (8th Cir. Mar. 3, 2021), in Harvard Law Review, vol. 135, 2022, pp. 1696.

[65] *Sanchez c. Francia*, Appl. N. 45581/15, 15 maggio 2023. Su cui cfr. P. Dunn, *Responsabilità del politico per commenti d'odio pubblicati sulla sua bacheca Facebook personale: la sentenza della Grande Camera per il caso Sanchez c. Francia*, in *Diritti Comparati*, post del 5 giugno 2023.

DPCE online
ISSN: 2037-6677

Altro ambito in relazione al quale le scelte regolatorie statunitensi sembrano orientate fortemente in relazione alle esigenze economiche e geopolitiche del Paese a scapito tanto dell'impianto filosofico liberale che lo caratterizza, quanto di ogni tensione finalizzata a valorizzare la tutela della personalità umana nel mondo digitale, è quello che riguarda la disciplina della tecnologia sull'Intelligenza artificiale (AI)

Ciò a partire dalla lettura dell'*Executive Order* n. 13859/2019, significativamente intitolato *Mantaining American Leadership in Artificial Intelligence*, emanato dal Presidente Trump l'11 febbraio del 2019 sulla scorta del *White House Summit on Artificial Intelligence for American Industry* del 2018[66].

Il detto ordine esecutivo viene adottato 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[67]: a tali obiettivi strategici cinesi la presidenza Trump reagisce con vigore inaugurando un disegno regolatorio fortemente promozionale e allo stesso tempo di protezione del mercato statunitense in ambito tecnologico e specificatamente sull'AI.

Tale strategia, si pone in diretta antitesi con quella prescelta, per i medesimi temi, in ambito europeo ove, invece, la preminenza è attribuita alla considerazione delle problematiche connesse alla tutela dei diritti individuali nell'interazione umana con l'Intelligenza artificiale. Sin dal 2016, con il Regolamento generale della protezione dei dati (GDPR n. 2016/679)[68], l'UE si propone infatti 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'Intelligenza artificiale esso, tuttavia, pone numerosi principi che possono rappresentare un utile argine ad un utilizzo sconsiderato della stessa[69]. A partire dal 2016, a livello europeo, vengono pertanto introdotti e sviluppati concetti fondamentali e

[66] Su cui cfr. https://trumpwhitehouse.archives.gov/ai/ . Tale ordine esecutivo, sottolineando il ruolo degli Stati Uniti come *leader* globale nella tecnologia dell'intelligenza artificiale si compone di cinque direttive principali:- 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; - Risorse federali: ovvero l'organizzazione delle risorse già in essere orientate alla valorizzazione dell'AI di conio statunitense; - Linee guida per la regolamentazione; - investimenti nell'*expertise*; - Protezione dell'intelligenza artificiale americana.

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

[68] 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.

[69] In materia di trattamento automatizzato dei dati personali nel 2016 viene altresì adottata la Direttiva UE 680-2016 (adottata il 27 aprile 2016 dal Parlamento e dal Consiglio europeo; direttiva recepita dall'ordinamento con italiano con il Decreto Legislativo 21.5.2018 n. 51.)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.

principi cardine in tema di disciplina della decisione algoritmica quali: il diritto di contestare la decisione automatizzata[70], il principio di non discriminazione algoritmica[71], il principio di non esclusività[72], il diritto ad accedere alla logica impiegata dall'algoritmo[73]. Il tema della disciplina dell'AI è peraltro, come noto, attualmente oggetto di una proposta di Regolamento UE sull'Intelligenza artificiale[74] il quale, oltre ad elencare tassativamente alcune pratiche di AI del tutto vietate[75], è caratterizzato da un approccio *risk based* individuando nell'allegato III al Regolamento i sistemi di AI considerati ad "alto rischio" e dunque sottoposti alla stringente normativa prevista nel Regolamento stesso[76]. Con risoluzione del

[70] Artt. 13, comma 2, lett. f); 14 comma 2, lett. g) Regolamento (UE) 2016/679.
[71] Considerando 71 Regolamento (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».
[72] Art. 22 Regolamento (UE) 2016/679.
[73] Art. 15, comma 1, lett. h) Regolamento (UE) 2016/679.
[74] Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'AI) e modifica alcuni atti legislativi dell'Unione, COM/2021/206 final. Il teso è commentato da L. Milano, *Il Regolamento europeo sull'Intelligenza Artificiale*, (29 giugno 2022) reperibile all'url www.altalex.com/documents/news/2022/06/29/regolamento-europeo-intelligenza-artificiale
[75] Art. 5 Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'AI) e modifica alcuni atti legislativi dell'Unione, COM/2021/206 final. 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 la 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 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.
[76] 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. Il regolamento sull'AI, oltre a porre una serie di norme tecniche e di sorveglianza destinate ai produttori ed ai distributori di tali tecnologie

DPCE online
ISSN: 2037-6677

Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale, sono state infine proposte delle raccomandazioni dettagliate per l'elaborazione di un Regolamento europeo sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale[77] .

La diversa scelta statunitense di garantire la supremazia tecnologica americana e la sicurezza nazionale piuttosto che l'individuo nell'interazione con l'algoritmo si evidenzia, oltre che nell'attività dell'esecutivo, anche in alcune preferenze 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[78] 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*[79], 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'intelligenza artificiale 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 riuscite a concretizzarsi nell'emanazione di atti normativi[80].

sancisce, all'art. 29, anche degli obblighi in capo agli utenti della medesima intelligenza artificiale 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. La norma evidenzia la logica di cooperazione fra soggetti coinvolti nella tecnologia sottoposta a normativa che caratterizza tale disciplina 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.

[77] Proposta di Regolamento A9-178/2020. 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 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 La proposta è commentata da A. Mastromatteo, B. Santacroce, *Responsabilità civile per i danni dell'intelligenza artificiale: la proposta del Parlamento Ue* (5 gennaio 2021) reperibile all'url www.agendadigitale.eu/cultura-digitale/la-responsabilita-civile-per-lintelligenza-artificiale-le-proposte-europee/ .

[78] PL 115-232.

[79] In vigore dal primo gennaio 2021.

[80] 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).

A fronte dell'insabbiamento della questione della responsabilità del *provider* in relazione alla raccomandazione algoritmica nel contesto legislativo, il tema è stato affrontato nelle aule giudiziarie. Anche qui, nondimeno, esso sembra essersi esaurito, nel maggio del 2023, con una decisione assunta dalla Corte suprema federale.

La vicenda giurisprudenziale da cui il dibattito sull'argomento ha preso le mosse è il caso *Force v. Facebook, Inc.*[81], 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 avverso la ricostruzione proposta 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[82].

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 trasformato il ruolo dei *providers* riducendone la neutralità. Il giudice dissenziente ha considerato difatti che sia 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[83]. 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.

[81] *Force v. Facebook, Inc., 934 F.3d 53 (2nd Cir. 2019).*

[82] «*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).

[83] 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).

DPCE online
ISSN: 2037-6677

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 *Malwarebyes, Inc. v. Enigma Software Group Usa LLC*[84], una vicenda giudiziaria nella quale figuravano come controparti due aziende produttrici di *software* per l'esclusione di materiale indesiderato: la *Malwarebyes* 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[85], è stato oggetto di un recente ricorso alla Corte suprema e la relativa 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*[86], 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*[87] 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 e complesso atto terroristico verificatosi a Parigi nel Novembre del 2015. In quella circostanza perse la vita (fra i molti altri) una giovane donna americana la cui famiglia ha intentato una causa civile contro *Google* sostenendo che *Youtube* (società ad essa collegata), attraverso al diffusione algoritmicamente mirata dei suoi video, aveva favorito il reclutamento dei terroristi e la costituzione della loro rete[88]. 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

[84] *Malwarebyes, Inc. v. Enigma Software Group Usa LLC*, 592 U. S. ____ (2020).
[85] 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 si dibattito anonimo su tematiche varie ("*Experience Project*") accusato di aver favorito attraverso il suo sistema di segnalazione algoritmica l'incontro materiale fra un tossicodipendente ed uno spacciatore.
[86] 598 U. S. (2023). Docket No. 21–1333; May 18, 2023.
[87] 598 U. S. _ (2023). No. 21–1496. Argued February 22, 2023—Decided May 18, 2023.
[88] 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).

discorsi che circolano in rete 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; solo apparentemente, peraltro le stesse vedono gli utenti come soggetti attivi: esiste difatti tutto un margine di passività dell'utenza che necessita di essere normato a partire dalle problematiche concernenti la trasparenza e la discriminazione algoritmica[89].

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[90].

Come già anticipato, il *certiorari* nel caso *Gonzales v. Google* è stato concesso insieme ad un altro caso relativo alla Sezione 230 e al tema del terrorismo 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 Istambul. 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*[91] 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 ponendo in essere un'adeguata sorveglianza alle informazioni in circolo sulla rete, le dette grandi aziende avevano finito con il favorire l'azione terroristica. La Corte suprema tuttavia non ha condiviso tale ricostruzione 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)[92]. Il

[89] M. Barbera, *Discriminazioni algoritmiche e forme di discriminazione Labour and Law Issue*, vol. 7, n. 1, 2021. S. Tommasi, *Algoritmi e nuove forme di discriminazione: uno sguardo al diritto europeo*, in *Revista de Direito Brasileira*, vol. 27, n. 10, 2020, 112 ss.

[90] 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)

[91] 18 USC § 2333.

[92] «*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'*

DPCE online
ISSN: 2037-6677

giudice Thomas ha peraltro evidenziato come in molti altri casi qualcuno può sfruttare a fini "terroristici" una tecnologia, ad esempio al rete telefonica, e questo non rende le aziende che forniscono questi servizi responsabili civilmente di tali azioni[93].

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.

6. Sicurezza nazionale o protezionismo? La concorrenza tecnologica cinese e l'*affair* TikTok

L'approccio liberista statunitense alla dimensione digitale che si rivela in tanti ambiti preminente sulla filosofia liberale e sulla (in effetti non fortissima) tensione alla tutela dei diritti individuali sembra invece trovare una possibile battuta d'arresto nelle esigenze di garanzia della sicurezza nazionale del Paese in situazioni nelle quali la tecnologia detenuta da potenze straniere concorrenti si rivela essere una ipotetica minaccia all'incolumità della nazione.

Le scelte strategiche in questo caso si dirigono verso un'ottica protezionistica e tuttavia sorge il sospetto che tale diverso orientamento sia in parte anche legato a garantire, ancora una volta, la preminenza tecnologica statunitense su scala mondiale e che dunque i temi della sicurezza e dell'interesse economico siano decisamente più intrecciati di quanto la giustificazioni alle scelte politiche adottate non rivelino apertamente.

Tali osservazioni trovano almeno parziale riscontro nell'analisi della crisi sorta in relazione alle tensioni innescate dalla estrema diffusione sul

"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.

[93] «*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 conference-call or video-call features made the sale easier*» Parte IV sez. A, Justice Thomas Opinion.

territorio USA della app di *social media* conosciuta come TikTok. Questo social, che sostanzialmente ospita video in formato breve e li offre 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[94]) 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*.

La questione del pericolo posto alla sicurezza nazionale a causa dell'ampio uso dell'app TikTok negli Stati Uniti si è posta, ed ha visto un tentativo di risoluzione, sin dai tempi dell'amministrazione Trump la quale ha utilizzato a tali fini quanto sancito nell'*International Emergency Economic Powers Act* (IEEPA) del 1977[95]. L'IEEPA è un atto normativo che garantisce al Presidente, in tempo di pace, l'autorità «di affrontare qualsiasi "minaccia" straniera insolita e straordinaria alla "sicurezza nazionale" degli Stati Uniti» fintanto che «il Presidente dichiara un'emergenza nazionale rispetto a tale minaccia»[96]. A tal fine il Presidente deve attivare la procedura prevista nel *National Emergencies Act* e proclamare l'emergenza in relazione ad una minaccia straordinaria ed inusuale che ha la sua origine all'esterno del territorio statunitense.

Sulla base di quanto stabilito nell'IEEPA, Il 15 maggio 2019, il presidente Trump ha adottato un ordine esecutivo[97] proclamando che la presenza di società tecnologiche controllate da stranieri costituisce un'emergenza nazionale ed una "minaccia straordinaria" per la sicurezza nazionale degli Stati Uniti. Sulla base di tali presupposti il Presidente ha quindi deciso di vietare determinate transazioni con alcuni paesi stranieri o cittadini stranieri che pongono rischi per la sicurezza nazionale degli Stati Uniti. Il 13 maggio 2020, il Presidente ha rinnovato tale dichiarazione, sottolineando la minaccia detta riguarda specificatamente le aziende tecnologiche con sede in Cina con stretti legami con il governo della Repubblica popolare cinese ("RPC")[98]. Il 6 agosto 2020, il Presidente ha infine identificato TikTok come un'azienda tecnologica che rappresenta un

[94] Sul Cyberspionaggio cinese cfr. G. Iuvinale, N. Iuvinale, *Sicurezza. Così il governo cinese penetra nella tecnologia USA*, (20 aprile 2023), consultabile all'url https://www.agendadigitale.eu/sicurezza/la-penetrazione-del-governo-cinese-negli-ecosistemi-tecnologici-statunitensi/

[95] *Title 50 USC sez. 35.* Sul detto atto normativo cfr. il CRS Report R45618, *The International Emergency Economic Powers Act: Origins, Evolution, and Use*, 25 marzo 2022, R45618 (congress.gov) .

[96] 50 USC § 1701(a).

[97] *Executive Order* n. 13873, *Securing the Information and Communications Technology and Services Supply Chain*, 84 Fed. Reg. 22689 (15 maggio 2019)

[98] *Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain*, 85 Fed. Reg. 29321 (13 maggio 2020).

DPCE online
ISSN: 2037-6677

rischio per la sicurezza nazionale[99] ed ha concluso che, poiché TikTok è di proprietà di una società con sede in Cina, il Partito Comunista Cinese ("PCC") potrebbe essere in grado di accedere alle informazioni personali e proprietarie degli americani, consentendo potenzialmente alla Cina di tracciare le posizioni di dipendenti federali e appaltatori e costruire fascicoli di informazioni personali per manovre ricattatorie e spionaggio aziendale.

Il Presidente ha inoltre sostenuto che TikTok potrebbe essere utilizzato per trasmettere propaganda approvata dal PCC e condividere «campagne di disinformazione a beneficio del [PCC]» avanzando come esempio la diffusione di teorie sulla diffusione del Coronavirus al suo esordio. L'amministrazione Trump ha dunque ordinato al Segretario al Commercio di identificare un elenco di transazioni da vietare nei rapporti con «*ByteDance*... o le sue sussidiarie», incluso TikTok. Il 6 agosto, il Presidente Trump ha adottato un ulteriore *executive order*[100] concernente la piattaforma di messaggistica istantanea *WeChat* anch'essa di proprietà di un'azienda cinese (*Tencent Holdings Ltd*). Sulla base di quanto stabilito nei detti ordini esecutivi, il 18 settembre 2020, facendo riferimento anche ad un *memorandum* interno che valutava le minacce rappresentate da *ByteDance* e TikTok[101], il Segretario al Commercio statunitense ha pubblicato un elenco di transazioni vietate riguardanti ByteDance[102] .

Le restrizioni dette nei confronti della piattaforme TikTok sono state impugnate in sede giudiziaria attraverso due ricorsi: il primo presentato dalla stessa azienda colpita dal provvedimento[103] ed il secondo proposto da alcuni utenti della piattaforme[104]. In entrambi i ricorsi le Corti hanno dato ragione ai ricorrenti considerando che i provvedimenti disposti dall'amministrazione presidenziale fossero esorbitanti rispetto ai poteri ad essa attribuiti dall'IEEPA giacché la medesima normativa disciplina esplicitamente due eccezioni alla possibilità del Presidente di provvedere all'emergenza nazionale. Tali eccezioni si concretano nella *personal communication exception*, in base alla quale il Presidente non può predisporre

[99] *Executive Order 13942 of August 6, 2020. Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain.*
[100] *Executive Order 13943 of August 6, 2020 Addressing the Threat Posed by WeChat, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain.*
[101] *U.S. Dep't of Commerce, Mem. for the Sec'y, Proposed Prohibited Transactions Related to TikTok Pursuant to Executive Order 13942* (Sept. 17, 2020), ECF No. 48-2, AR 27-50 ("*Commerce Memorandum*").
[102] U.S. Dep't of Commerce, *Identification of Prohibited Transactions to Implement Executive Order 13942 and Address the Threat Posed by TikTok and the National Emergency with Respect to the Information and Communications Technology and Services Supply Chain*, 85 Fed. Reg. 60061, 60062 (Sept. 24, 2020) ("Commerce Identification").
[103] La decisione è stata Assunta dalla *United States District Court, District of Columbia* 507 F.Supp.3d 92 (2020) TIKTOK INC., et al., *Plaintiffs, v. Donald J. Trump, President of the United States, et al.*, Defendants. Civil Action No. 1:20-cv-02658 (CJN), 7 dicembre 2020.
[104] La sentenza è stata adottata dalla *United States District Court, E.D. Pennsylvania.* 498 F.Supp.3d 624 (2020). Douglas Marland, Cosette Rinab, and Alec Chambers, *Plaintiffs, v. Donald J. TRUMP, in his official capacity as President of the United States; Wilbur L. Ross, Jr., in his official capacity as Secretary of Commerce; and U.S. Department of Commerce, Defendants.* CIVIL ACTION NO. 20-4597.

restrizioni ad alcuna comunicazione postale, telegrafica, telefonica, o qualunque altra comunicazione personale che non comporti trasferimento di valori («*any postal, telegraphic, telephonic, or other personal communication, which does not involve a transfer of anything of value*»). Sulla base invece dell' *informational materials exception* (talvolta chiamata *Berman Amendment* sulla base del fatto che all'epoca venne caldeggiata dal rappresentante al Congresso Howard Berman), il Presidente non può porre restrizioni a «*information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs . . . artworks, and news wire feeds*».

Hanno ottenuto una vittoria giudiziaria altresì, sulla base tuttavia del parametro delle garanzie offerte dal I emendamento, un gruppo di utenti dell'app WeChat. L'amministrazione federale ha inizialmente proposto ricorso avverso tutte le decisioni; tuttavia, all'insediarsi dell'amministrazione Biden, sono stati ritirati gli *executive orders* alla base delle dette vicende giudiziarie ed è stato raggiunto un accordo extragiudiziale.

Diversamente da quanto accaduto in relazione agli *executive orders* fondati sull'IEEPA, l'amministrazione Biden ha deciso di proseguire quanto già avviato dall'amministrazione Trump e fondato invece sull'autorità legale attribuita alla *Committee on Foreign Investment in the United States* (CFIUS).

CFIUS è un comitato interagenzia presieduto dal Segretario del Tesoro che esamina gli investimenti esteri negli Stati Uniti per potenziali rischi per la sicurezza nazionale. La sua autorità è fondata sulla Sezione 721 del *Defence Production Act* (come modificato e codificato nel Title 50 USC § 4565). CFIUS è competente ad esaminare fusioni, acquisizioni che potrebbero comportare che una qualunque entità straniera finisca per assumere il controllo di un'azienda statunitense ed è dunque competente a determinare la possibilità che sussistano dei rischi per la sicurezza nazionale derivanti da una transizione economica e aziendale. La detta Commissione può conseguentemente imporre misure appropriate e raccomandare al Presidente il divieto o la sospensione della detta transazione. La funzione di CFIUS è tuttavia solo di promozione in quanto è il Presidente a detenere l'autorità ultima di vietare o sospendere una transazione segnalata dalla Commissione stessa.

Nel caso di TikTok, CFIUS ha segnalato l'acquisizione da parte di ByteDance di un altro *social* basato su video: musical.ly. Nel 2017 ByteDance ha acquistato musical.ly per 1 miliardo di dollari. Nel 2020 il presidente Trump ha considerato tale acquisizione quale possibile concreta minaccia per la sicurezza nazionale degli Stati Uniti ed ha emesso un ordine esecutivo[105] (*Divestment Order*) imponendo a ByteDance di dismettere qualunque investimento sul territorio statunitense e cedere qualunque dato ottenuto attraverso TikTok o musical.ly[106].

[105] *Order of August 14, 2020 Regarding the Acquisition of Musical.ly by ByteDance Ltd. Federal Register / Vol. 85, No. 161 / Wednesday, August 19, 2020 / Presidential Documents.*
[106] «*ByteDance, its subsidiaries, affiliates, and Chinese shareholders, shall divest all interests and rights in: (i) any tangible or intangible assets or property, wherever located, used to enable or support ByteDance's operation of the TikTok application in the United States, as determined by the Committee; and (ii) any data obtained or derived from TikTok application or Musical.ly application users in the United States. Immediately upon divestment, ByteDance shall certify in*

DPCE online
ISSN: 2037-6677

Al fine di scongiurare la completa impossibilità di operare sul territorio statunitense ByteDance ha avviato un negoziato con le autorità federali in relazione al quale ha proposto una possibile soluzione nota come il c.d. Progetto Texas[107] fondata sull'istituzione da parte dell'azienda cinese di una apposita filiale statunitense, una *US Data Security* (USDS) governata da un Consiglio di amministrazione indipendente, supervisionata da CFIUS al quale è demandata peraltro la possibilità di definirei requisiti per l'assunzione presso USDS. L'accordo prevede inoltre che chiunque lavori per USDS sia necessariamente cittadino statunitense (o comunque in possesso di una carta verde). Ciò al fine di ridurre al minimo l'accesso dei dipendenti ai dati degli utenti statunitensi e ridurre al minimo i trasferimenti di dati tra Nazioni, inclusa la Cina.

Con l'obiettivo di garantire il trattamento dei dati dei cittadini statunitensi l'azienda cinese ha deciso inoltre, nel tempo, di avvalersi del tutto (con riguardo all'utenza USA) di *Oracle Cloud Infrastructure* che materialmente, secondo la proposta, ospiterà la piattaforma TikTok negli Stati Uniti (inclusi l'algoritmo e le funzioni di moderazione dei contenuti). Oracle sarà responsabile del monitoraggio dei dati in entrata e in uscita dall'USDS per garantire che nessun dato transiti illecitamente attraverso il confine dell'USDS e tutto il traffico dati negli Stati Uniti verrà instradato attraverso Oracle Cloud. Nel *briefing*, TikTok ha affermato che tutti i dati degli utenti statunitensi sono già attualmente archiviati in Oracle Cloud.

Poiché TikTok è un'app che opera a livello globale, alcuni dati devono necessariamente attraversare i confini e dunque "lasciare" gli Stati Uniti; a questo proposito l'accordo propone di demandare ad Oracle l'obbligo di utilizzare una combinazione di processi automatizzati e revisione umana per monitorare i flussi di dati al fine di verificare la sussistenza di violazioni della sicurezza o irregolarità. Tra le altre misure, Oracle condurrebbe controlli a campione per esaminare i dati che trasmettono il confine USDS e seguirebbe revisioni più dettagliate se uno qualsiasi dei controlli dovesse rilevare flussi di dati non conformi.

Mentre erano in corso le operazioni di negoziazione con l'azienda, a giugno del 2021 l'amministrazione Biden ha adottato un ulteriore *executive order*[108] intitolato "*Protecting Americans' Sensitive Data From Foreign Adversaries*" con il quale ha annullato diversi ordini dell'amministrazione Trump, tra cui l'ordine del 2020 e quello concernente WeChat e li ha sostituiti con nuove iniziative progettate per affrontare i rischi posti da infiltrazioni aziendali straniere. Il *Data Executive Order* ha lasciato nondimeno in vigore altri ordini esecutivi dell'era Trump, incluso quello adottato nel 2019 (*Securing the Information and Communications Technology and Services Supply*).

writing to CFIUS that all steps necessary to fully and permanently effectuate the actions required under sections 2(a) and 2(b) have been completed».

[107] Cfr. la pagina dell'azienda dedicata alla proposta consultabile all'URL https://newsroom.tiktok.com/en-us/our-approach-to-keeping-us-data-secure.

[108] *Executive Order 14034 of June 9, 2021 Protecting Americans' Sensitive Data From Foreign Adversaries, Federal Register / Vol. 86, No. 111 / Friday, June 11, 2021 / Presidential Documents.*

Considerando che alcune delle risposte alle problematiche postesi in relazione alla vicenda TikTok sono state impedite a causa di alcune eccezioni previste nella normativa sull'emergenza nazionale, alcuni membri del Congresso hanno avanzato delle proposte legislative attualmente in discussione finalizzate ad eliminare le dette eccezioni.

Fra le proposte avanzate spicca certamente il *Restrict Act* (S. 686), proposto dal senatore Mark Warner (ma sostenuto da un gruppo *bipartisan*), che propone di attribuire al Segretario al Commercio il potere di rivedere le transazioni commerciali che coinvolgono determinati prodotti o servizi di tecnologie dell'informazione e della comunicazione quando collegate a un "avversario straniero" degli Stati Uniti e sospetti di rappresentare un "rischio indebito e inaccettabile" per la sicurezza nazionale degli Stati Uniti o dei suoi cittadini.

Pur non giunto definitivamente a conclusione è possibile affermare già da ora che l' "*affair TikTok*" rappresenta certamente un momento di svolta nella filosofia complessiva e nell'orientamento statunitense al contesto digitale sottolineando, come è stato efficacemente posto in evidenza[109], un'attuale crisi americana di fiducia in un Internet aperto e libero quando il Paese si confronta con un'ipotesi di ordine liberale non guidato dagli Stati Uniti.

In qualunque caso, difatti, risulta evidente come l'iniziale approccio liberale sia definitivamente in crisi essendo divenuto necessario, anche negli Stati Uniti, procedere alla negoziazione delle autorità pubbliche con le aziende del settore o decidere, in casi più estremi di intervenire alterando la libertà del mercato che per anni è stata strenuamente preservata.

7. L'inadeguatezza della strategia liberale e liberista nel contesto statunitense: il doppio binario fra tutela individuale e garanzie dell'interesse nazionale

Il tema della libertà di espressione nel contesto digitale ha nel tempo evidenziato problemi pratici e risvolti che inizialmente non erano stati valutati del tutto nella loro complessità e pervasività. La tecnologia digitale, così come in effetti ogni esperienza tecnologica, si è peraltro a propria volta potenziata nello scorrere degli anni consentendo nel tempo forme sempre più ampie di espressione in Internet ma producendo altresì, in tal modo, maggiori interconnessioni (e relative problematiche) in termini di bilanciamento fra tali libertà e la tenuta democratica degli ordinamenti giuridici contemporanei. Di qui l'immediata constatazione per cui l'approccio iniziale, liberista, fondato sull'autoregolazione e garantito dall'irresponsabilità del *provider*, si è rivelato nel tempo insufficiente ed obsoleto. Il tema si è recentemente posto persino nell'esperienza ordinamentale più versata all'approccio liberista ovvero nel caso statunitense nel quale, come si è visto, in anni recenti il dibattito sembra aver raggiunto le aule giudiziarie e l'interesse dell'esecutivo (sia repubblicano sia

[109] Cfr. W. Duffield, T*ikTok Panic Threatens Speech*, reperibile all'url https://www.cato.org/blog/tiktok-panic-threatens-speech (21 aprile 2023).

DPCE online
ISSN: 2037-6677

democratico) e di lì forse potrebbe spiccare il salto verso l'attenzione anche del legislatore.

L'esperienza americana si è difatti confrontata con l'inaspettata ipotesi per cui la dimensione del mercato digitale possa non vedere necessariamente le aziende americane quali *leader* ed ha dovuto dunque inevitabilmente valutare con maggiore attenzione i rischi derivanti da una mancata disciplina legislativa nei confronti di colossi del mercato qualora rispondenti a valori ed ideologie diverse da quelle statunitensi.

Il tema della filosofia dominante il contesto digitale non è certo nuovo: è a partire dal caso *Yahoo v. Licra*[110] che il giurista attento è sollecitato a considerare con attenzione la questione per cui lo Stato che risulta detenere la *leadership* economica sul mercato digitale rischia di divenire conseguentemente quello che ne detta i valori. È evidente che gli Stati Uniti non avevano fatto all'epoca del tutto i conti con la possibilità che Paesi da loro molto lontani culturalmente e politicamente (addirittura considerati "avversari") potessero detenere tale posizione dominante.

In questa fase di riflessione sul tema del liberismo digitale gli Stati Uniti confermano la sussistenza in tale ordinamento di una sorta di doppio binario nelle garanzie dell'approccio tendenzialmente liberista che lo connota. L'ordinamento federale statunitense si rivela infatti ancora una volta disposto a sacrificare, se necessario, la tutela individuale (alla sicurezza così come alla dignità) al fine di garantire l'impianto liberale e liberista che lo contraddistingue e tuttavia il medesimo modello può essere messo in discussione quando l'interesse da tutelare è pubblico e nazionale.

L'attuale Corte suprema, con le decisioni *Gonzales* e *Taamneh* rinsalda la propria giurisprudenza, ostinata nel confermare la neutralità del *provider* e la necessità di tutelare le aziende digitali da possibili gravi problemi di responsabilità civile; ciò nonostante l'azione della precedente amministrazione Trump e malgrado il tema della manipolazione individuale attraverso la decisione algoritmica sia argomento di preoccupazione pressoché bipartisan.

È tuttavia altresì evidente a molti come la Corte suprema, nella sua attuale composizione, sembra essere tendenzialmente refrattaria ad esercitare la propria funzione contromaggioritaria a garanzia dei diritti individuali ritenendo che la selezione degli stessi sia competenza del Congresso a meno dei diritti espressamente garantiti dalla Costituzione o di quelli che resistono al c.d. *test* di *Glucksberg*[111] (non utilizzato nelle più recenti

[110] *Yahoo! Inc. v La Ligue Contre le Racisme et l'Antisémitisme*, 169 F. Supp. 2d 1181 (N.D. cal. 2001). Su cui cfr. E.A. Okoniewski, *Yahoo ! Inc. V. Licra : The French Challenge to Free Expression on the Internet*, in *American University International Law Review*, vol. 18, 2002, 295 ss.

[111] Partendo dalla constatazione per cui le clausole del *Due process* e dell'*Equal protection* del XIV Emendamento garantiscono la protezione di diritti non espressamente menzionati in Costituzione nel rispetto, tuttavia, di alcuni parametri che si rifanno al precedente *Washington v. Glucksberg*, 521 US 702 (1997) in cui la Suprema Corte ha negato l'esistenza nella Costituzione federale di un diritto al suicidio assistito (nei termini di omicidio del consenziente sulla base della *Due process clause*. Sull'utilizzo da parte della maggioranza della Corte del *Gluksberg test* è possibile avanzare qualche riflessione critica connessa alla fragilità argomentativa e di qualificazione giuridica che esso può innescare. Ciò che è accaduto, ad esempio, in occasione del caso *Abigail Alliance*

decisioni sulla raccomandazione algoritmica ed invece centrale nella nota decisione *Dobbs*[112] in tema di diniego del diritto federale all'aborto) in base al quale un diritto per essere considerato implicitamente garantito dalla Costituzione federale deve essere profondamente radicato nella storia e nelle tradizioni della Nazione («*deeply rooted in this Nation's history and tradition*») o deve essere considerato implicito nel concetto di "libertà ordinata" («*implicit in the concept of ordered liberty*») che caratterizza l'ordinamento statunitense.

Il potere cui sembra spettare dunque un ruolo attualmente su tali tematiche è il Congresso ed eventualmente l'Esecutivo il che solleva, tuttavia, qualche perplessità non perché non spetti all'uno o all'altro la funzione eminente di determinare il contesto giuridico di un determinato ambito (in questo caso l'ecosistema digitale) quanto perché è evidente che il venir meno della funzione contromaggioritaria della Corte suprema (nel senso di garante dei diritti, non ovviamente del semplice *status quo*) può idealmente minare l'equilibrio dei *checks and balances* disegnato nella Costituzione federale e portare, nel contesto attuale, ad un'esasperazione dell'impianto liberista (da una parte) e orientato al protezionismo economico (dall'altra).

Entrambe le filosofie citate sembrano difatti caratterizzare le scelte statunitensi nell'ecosistema digitale ove, come si è cercato di evidenziare, il dichiarato impianto liberale e liberista statunitense sottende in realtà, sostanzialmente, a promuovere il più possibile l'interesse nazionale del Paese in temini economici (avvantaggiando la *leadership* tecnologica detenuta dagli Stati Uniti) e viene preferito infatti ad un approccio politico maggiormente protezionistico; ciò solo fino a che tale supremazia tecnologica perdura per recedere, invece, quando, in un mercato tecnologico maggiormente concorrenziale si rivela essere maggiormente premiale per il Paese un impianto normativo che opti per scelte maggiormente protezionistiche.

for Better Access to Developmental Drugs v. von Eschenbach, 495 F.3d 695 (D.C. Cir. 2007), *cert denied*, 552 U.S. 1159 (2008) quando la Corte di Appello per il distretto della Columbia ha negato l'esistenza del diritto dei malati terminali ad utilizzare farmaci sperimentali mentre, in maniera evidente, il tema andava qualificato in relazione al diritto individuale di salvarsi la vita con tutti i mezzi leciti a propria disposizione. La decisione è commentata sull'*Harward Law Review*, 121, 2008, 185 ss. Cfr. inoltre P.W. Lesley, *Abigail Alliance for Better Access to Developmental Drugs v. Von Eschenbach: Access to Experimental Drugs: Is Access to Experimental Drugs a Fundamental Right When it Comes to the Treatment of the Terminally Ill?*, in *North Carolina Central University Science & Intellectual Property Law Review*, vol. 10, n. 1, *Article* 2, 2017, 27 ss.. La questione qualificatoria nella valutazione circa la sussistenza o meno di un diritto fondamentale costituzionalmente garantito non è nuova all'esperienza della Corte suprema sol se si consideri la famigerata sentenza *Bowers v. Hardwick*, 478 U.S. 186 (1986) ove il supremo giudice federale sancì l'inesistenza nella Costituzione di un "diritto alla sodomia" (e, sulla base di ciò, la legittimità delle leggi statali che sanzionavano i rapporti omosessuali) pur inquadrandosi la questione (come la stessa Corte diversi anni dopo chiarì nella sentenza *Lawrence v. Texas*, 539 U.S. 558 (2003)) nella diversa determinazione circa la portata del diritto alla *privacy* secondo i canoni costituzionali.

[112] Su cui cfr. L. Fabiano, *Tanto tuonò che piovve: l'aborto, la polarizzazione politica e la crisi democratica nell'esperienza federale statunitense*, in *BioLaw Journal – Rivista di BioDiritto*, n. 3, 2022.

DPCE online
ISSN: 2037-6677

Laura Fabiano
Dipartimento di Giurisprudenza
Università degli studi di Bari "Aldo Moro"
laura.fabiano@uniba.it