

LAURA FABIANO

LE POTENZIALITÀ MANIPOLATIVE DELLA DEMOCRAZIA DIGITALE FRA INTERESSI PUBBLICI E POTERI PRIVATI

SOMMARIO: 1. Le forme di Stato nel web: anarchia, dittatura, liberismo e ipotesi di costituzionalismo digitale. — 2. Democrazia e libertà di espressione *on line* fra *hard*, *soft law* ed autoregolamentazione. — 3. La disciplina sulla libertà di espressione *on line* e l'interpretazione funzionalistica della medesima libertà nelle democrazie liberali: gli Stati europei e l'Unione. — 3.1. La normativa specificatamente orientata al contrasto alla disinformazione politica: il caso francese. — 3.2. La normativa sull'*hate speech on line* nell'esperienza tedesca. — 3.3. L'ibridazione fra *hard law* e *soft law* nella proposta di legge britannica. — 3.4. L'evoluzione normativa nell'esperienza dell'Unione europea dalla direttiva *e-commerce* al *Digital Services Act*. — 4. Il liberismo nel contesto USA: dalla tutela della *content moderation* ai problemi collegati al *recommendation algorithm* e all'*affaire tiktok*. — 4.1. I emendamento e strumenti di comunicazione di massa. — 4.2. La sez. 230 del CDA: la *content moderation* e le esigenze del liberismo digitale. — 4.3. La privatizzazione della censura e la *public forum theory*. — 4.4. La responsabilità del *provider* e i sistemi di "*recommendation algorithm*". Le più recenti ipotesi di superamento dell'interpretazione estensiva della sez. 230. — 4.5. La possibile vera crisi del modello liberale statunitense: la vicenda Tik Tok ovvero ... quando nel libero mercato gli Usa perdono la *leadership*. — 5. L'ecosistema digitale, la globalizzazione e la crisi della strategia liberista.

1. LE FORME DI STATO NEL WEB: ANARCHIA, DITTATURA, LIBERISMO E IPOTESI DI COSTITUZIONALISMO DIGITALE.

L'evoluzione tecnologica nel campo delle telecomunicazioni e dell'informatica degli ultimi decenni ha fatto registrare, nella vita quotidiana di chiunque, dei cambiamenti profondi e irrinunciabili a fronte dei quali i giovani nati in questa nuova fase storica

* Il presente contributo costituisce la rielaborazione della relazione presentata al XXVI Colloquio Biennale dell'Associazione Italiana di Diritto Comparato (AIDC), Bari-Taranto, 25-27 maggio 2023. Il presente

saggio costituisce prodotto della ricerca del progetto Horizon Europe Seeds "Libertà di opinione, nuove tecnologie e formazione del consenso" bandito dall'Università degli studi di Bari (PI prof. M. Calamo Specchia).

sono stati definiti come generazione 2.0 ¹ (o addirittura 4.0) ovvero nativi digitali ².

Se, sotto innumerevoli profili, tali cambiamenti rappresentano delle immense risorse per l'evoluzione complessiva delle società umane, oltre che per gli individui singolarmente intesi, è nondimeno vero che l'evoluzione informatica (come probabilmente tutti i cambiamenti significativi nei modi di vivere e di fare le cose degli esseri umani) pone di per sé anche delle nuove ardue sfide in termini di regolazione dei rapporti e di garanzie dei diritti e delle libertà ³.

Nella prima fase della loro affermazione, i media collegati alla tecnologia della rete Internet hanno generato significative aspettative circa la loro capacità di migliorare la qualità democratica mondiale e le possibilità di espressione del pensiero individuale. Ciò in quanto era diffusa l'opinione per cui, veicolata da tali tecnologie, l'informazione sarebbe stata facilitata determinando una sfera pubblica più vitale, aperta ed inclusiva e caratterizzata da un dibattito pubblico più ampio e pluralista. Si riteneva infatti che Internet sarebbe stata un'occasione di espressione per le opposizioni democratiche e progressiste e per la società civile marginalizzata dai media *mainstream* e dalle agende politico-instituzionali ⁴.

La portata innovativa insita nell'evoluzione digitale degli ultimi

¹ Cfr. https://www.treccani.it/enciclopedia/generazione-2-0_%28altro%29/.

² L'espressione nativi digitali è stata coniata nel 2001 da Mark Prensky il quale la contrapponeva alla generazione degli immigrati digitali ovvero tutti coloro che, nati in epoche precedenti alla diffusione di determinate tecnologie, le hanno apprese in età adulta. Cfr. M. PRENSKY, *Digital Natives, Digital Immigrants*, in *On the Horizon*, 2001, vol. 9, n. 5, 1-6; si rinvia inoltre a Id., *Digital Natives, Digital Immigrants, part II. Do they really think differently?*, in *On the Horizon*, 2001, vol. 9, n. 6, 1-6; Id., *Listen to the Natives*, in *Educational Leadership*, vol. 63, n. 4, 2005, 8-13. Cfr. per la dottrina italiana anche M. MARTONI, *Datificazione dei nativi digitali, Una prima ricognizione e alcune brevi note sull'educazione alla cittadinanza digitale*, in *federalismi.it*, n. 1, 2020.

³ Sul punto la bibliografia è oramai sterminata e, dunque, ci si limita solo ad alcuni fondamentali riferimenti: S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma, 1997; V. ZENO-ZENGOVICH, *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, 395-430, maio/ago, 2020. 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.

⁴ Ancora nel 2010 Larry Diamond, professore di sociologia di Stanford, in un articolo intitolato *Liberation Technology*, (in *Journal of Democracy*, vol. 21, n. 3 e consultabile all'url <https://www.journalofdemocracy.org/articles/liberation-technology/>) sosteneva con energia le virtù socializzanti del web (anche in termini politici). Tale approccio inizialmente confermato nell'importante ruolo giocato dalla rete internet

decenni è stata tale che 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"⁵. 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 reale⁶, si è approdati — grazie probabilmente al contributo rilevante della giurisprudenza di alcune Corti⁷ —, alla concezione piena della vigenza del diritto territoriale anche nel contesto telematico⁸. 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

nelle c.d. primavere arabe (su cui *Il ruolo dei Social Network nelle Rivolte Arabe*, in *Osservatorio di Politica internazionale*, n. 40, settembre 2011) ha subito un'importante inversione di tendenza dopo quanto accaduto in occasione della prima campagna politica per le elezioni presidenziali di Donald Trump e la campagna referendaria britannica sulla Brexit. Sul tema in generale si rinvia G. GOMETZ, *Democrazia elettronica. Teoria e tecniche*, Pisa, 2017.

⁵ L'espressione è di M. BASSINI, *Internet e libertà di espressione*, cit., al quale si rinvia per una completa analisi dell'evoluzione storica della dottrina giuridica internazionale concernente la dimensione costituzionale oltre che il diritto applicabile e la giurisdizione competente per la disciplina del cyberspazio.

⁶ Concezione cui si legava, per alcuni studiosi, un'idea anarchica del medesimo contesto e per altri, all'opposto, la convinzione di possibili forme di autoregolazione del *web* ad opera dei soggetti che lo animavano e lo popolavano. 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 dot-

trinale, quelle posizioni ultraliberarie 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 paritorita da internet » (M. BASSINI, *Internet e libertà di espressione*, cit. 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 statutale per il mondo digitale e sostengono l'autosufficienza regolatoria delle comunità digitali.

⁷ Le quali, seppur attraverso un percorso accidentato, hanno indagato per prime sul tema della giurisdizione competente e del diritto applicabile al mondo digitale. Cfr., fra le tante letture interessanti, O. POLLICINO, *Internet nella giurisprudenza delle Corti europee: prove di dialogo?*, in *Forum di Quaderni costituzionali*, 31 dicembre 2013; del medesimo A. cfr. inoltre *Tutela dei diritti fondamentali nell'era digitale e contesto valoriale: una indagine transatlantica*, in *Media Laws*, n. 2, 2018, 39 e ss.

⁸ Sul punto ampiamente M. BASSINI, *Internet e libertà di espressione*, cit.

delle regole generali ⁹. 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* imponessero una seria valutazione circa la possibilità delle categorie giuridiche tradizionali di permeare i confini e quindi di soddisfare pienamente le esigenze di regolazione e tutela che anche da tale (non)luogo promanano ¹⁰.

Il fermento dottrinale riferito, animato da concezioni dell'oggetto della propria analisi (e delle sue caratteristiche) a volte diametralmente opposte, è esemplificativo della complessità insita in qualunque tentativo di regolazione di un'attività umana che si svolge "in rete" ove, peraltro, con grande frequenza, l'uomo comune tende a voler conferire ad alcuni diritti (o ad alcune pretese) pesi specifici diversi rispetto a quelli attribuiti nel mondo reale e ove, con più facilità, anche a ragione di una scarsa consapevolezza della portata potenziale dello strumento che si utilizza, si compiono azioni sulle quali normalmente si rifletterebbe molto di più.

Deludendo le iniziali attese, nel corso del tempo, si sono evidenziati alcuni elementi tecnici che connotano le tecnologie informatiche (la profilazione degli utenti, il *microtargeting*, l'organizzazione e la selezione algoritmica dei dati ecc.) i quali fanno sì che le stesse, a ben vedere, più che potenziare la partecipazione e le possibilità di espressione spesso finiscono per condizionare profondamente le scelte comunicative sia in termini di manifestazione dell'opinione sia di accesso all'informazione alterando, dunque, attraverso la dimensione tecnica del mezzo, i contenuti del processo comunicativo sia in entrata sia in uscita ¹¹. Si è evidenziata inoltre, con lo scorrere del tempo, la consapevolezza progressiva

⁹ Il giudice Easterbrook paragonando il diritto digitale ad una sorta di "legge sul cavallo" ne sostenne l'irrilevanza affermando « *the best way to learn the law applicable to specialized endeavors is to study general rules. Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any effort to collect these strands into a course on "The Law of the Horse" is doomed to be shallow and to miss unifying principles. Teaching 100 percent of the cases on people kicked by horses will not convey the law of torts very well. Far better for most students—better, even, for those who plan to go into the horse trade—to take courses in property, torts, commercial transactions, and the like, adding to the diet of horse cases a smattering of*

transactions in cucumbers, cats, coal, and cribs. Only by putting the law of the horse in the context of broader rules about commercial endeavors could one really understand the law about horses », F.H. EASTERBROOK, *Cyberspace and the Law of the Horse*, in *University of Chicago Legal Forum*, vol. 1996, 1996, 207-208.

¹⁰ Per una ricostruzione ed un'analisi critica di tale secondo filone di dibattito si rinvia ancora a M. BASSINI, *Internet e libertà di espressione*, cit., spec. 31 e ss.

¹¹ C.R. SUNSTEIN, *#Republic. La democrazia nell'epoca dei social media*, Bologna, il Mulino, 2017; Id., *Republic.com. Cittadini informati o consumatori di informazioni?*, Bologna, 2003. Sul rapporto fra informazione e formazione del consenso in ambito politico cfr. A. PAPA, *"Democrazia della comunicazione" e formazione dell'opi-*

per la quale l'*agorà* digitale non può in effetti essere considerata semplicisticamente un contesto libero ove può trovare spazio un costituzionalismo spontaneo ¹², avulso dalle pretese regolative dei poteri pubblici perché tale ricostruzione non tiene conto « dell'ingresso del potere economico nel cyberspazio, che quelle libertà ha finito per cannibalizzare e soprattutto plasmare secondo i propri fini » ¹³.

Le tecnologie informatiche della comunicazione (ICT) presentano delle evidenti differenze con i media tradizionali in primo luogo con riguardo al c.d. "modello comunicativo" giacché i media precedenti (tanto la stampa quanto radio e televisione) erano improntati ad un modello c.d. "*one to many*" ed orientati ad una comunicazione unidirezionale (ove è ben distinto il ruolo di coloro che esprimono il messaggio e di coloro che lo ricevono); diversamente le ICT sono strumenti di comunicazione c.d. "*many to many*" e si caratterizzano per il fatto che tutti gli utenti che li utilizzano sono allo stesso tempo produttori e riceventi dell'informazione ¹⁴. Questo, tuttavia, non rende gli stessi utenti padroni della medesima informazione (come invece illusoriamente spesso gli stessi internauti credono) in quanto i media digitali hanno conservato per sé, in modi meno evidenti rispetto al passato (ma non meno penetranti), la fondamentale funzione di essere selezionatori degli argomenti più importanti (la c.d. *agenda setting*) ¹⁵. Ciò avviene, diversamente all'era pre-digitale, secondo un fenomeno definito di "neo-intermediazione" ovvero in forme automatizzate tramite processi algoritmici che non sono neutrali ¹⁶ e se è vero che la mancata neutralità dei mezzi di comunicazione era fenomeno che accadeva anche all'epoca dei media tradizionali, tuttavia, rispetto a questi ultimi, i processi di selezione dell'informazione contemporanei risultano maggiormente "opachi" ¹⁷.

Le odierne ICT evidenziano, dunque, al medesimo tempo, capacità predittive e manipolative: predittive, in quanto gli algo-

nione pubblica, in *federalismi.it*, n. 1, 2017, 9 ss.

¹² Su cui criticamente P. CIARLO, *Contro l'idea di Costituzione spontanea*, in *Quaderni costituzionali*, n. 1, 2002, 101 ss.

¹³ M. BETZU, *I baroni del digitale*, Napoli, 2022, 22.

¹⁴ M. AINIS, *Democrazia digitale*, in *Rassegna parlamentare*, n. 2, 2013. Cfr. anche L. CORCHIA, *La democrazia nell'era di Internet: per una politica dell'intelligenza collettiva*, con un saggio inedito di P. LÉVY, Firenze, 2011, 173 ss.; S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 2004.

¹⁵ Su tale distorsione cognitiva cfr. G.

ORIGGI, *La democrazia può sopravvivere a Facebook? Egualitarismo epistemico, vulnerabilità cognitiva e nuove tecnologie*, in *Ragion pratica*, n. 51, 2018, 445 ss.

¹⁶ GIACOMINI, G., *Verso la neo-intermediazione. Il potere delle grandi piattaforme digitali e la sfera pubblica*, in *Iride*, n. 3, 2018, 457-468.

¹⁷ G. GIACOMINI, *Potere digitale. Come Internet sta cambiando la sfera pubblica e la democrazia*, prefazione di Michele Sorrice, Milano, 2018; C. CEPERNICH, *Le campagne elettorali al tempo della networked politics*, Roma-Bari, 2017; G. GORI, *Social media ed elezioni. I limiti del diritto e il rischio di una modulated democracy*, in *Informatica e diritto*, n. 1-2, 2017, 203 ss.

ritmi, 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; manipolativi, perché la profilazione algoritmica contribuisce a selezionare i contenuti determinanti per la formazione dell'opinione pubblica. L'algoritmo definisce gli utenti a partire dai dati che li riguarda — e che essi stessi consapevolmente o inconsapevolmente forniscono — (*profiling*) ed offre loro informazioni selezionate (*targeting*¹⁸). 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*¹⁹). Si tratta di una “esposizione selettiva” per la quale, privati di fatto della possibilità di un'informazione libera e completa²⁰ gli individui tendono ad estremizzare le proprie opinioni con un generale effetto polarizzante²¹ che riguarda l'intera collettività²². 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) »²³ al fine tanto di po-

¹⁸ 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-cos-e-quali-sono-gli-impatti-per-la-protezione-dei-dati-personali/> (23 marzo 2020).

¹⁹ 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, 29-44, 2019; M. BIANCA, *La filter bubble e il problema dell'identità digitale*, in *MediaLaws - Rivista di diritto dei media*, n. 2, 2019, 39 ss.

²⁰ 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 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.

²¹ 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/10179/12791434/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. ORICCI, *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.

²² Cfr. sul tema E. LONGO, *Dai big data alle “bolle filtro”*: nuovi rischi per i sistemi democratici, cit.

²³ B. RABAI, *I Big Data nell'ecosistema digitale: tra libertà economiche e tutela dei*

tenziare la loro capacità pubblicitaria sul mercato quanto per rivendere questi dati a soggetti terzi.

Il dibattito dottrinale e nell'opinione pubblica sul tema si è vivacizzato a partire dal 2016: le interferenze private ed il potenziale distorsivo tipico delle campagne politiche digitali si è difatti reso evidente in quell'anno in occasione della prima campagna elettorale di Donald Trump per la corsa alla presidenza degli Stati Uniti D'America ed alla campagna referendaria sulla *Brexit* nel 2016²⁴. Il tema è tuttavia esploso nel 2018 con il noto scandalo *Cambridge Analytica* in relazione al quale si è evidenziato come, attraverso l'analisi dei dati disponibili sulla rete, un'azienda privata è in grado di interferire incisivamente in una campagna elettorale alterandone la democraticità²⁵.

L'erompere della pandemia mondiale da Covid 19 ha costituito, pochi anni più tardi, un'ulteriore vicenda storica a fronte della quale si è reso evidente il potenziale pervasivo immenso delle tecnologie digitali nella vita quotidiana di chiunque e ha posto all'ordine del giorno, come priorità assoluta, la necessità di regolare numerosissimi fenomeni connessi alla rete Internet e risolvere sia tecnologicamente, ma anche giuridicamente, problematiche da tempo note divenute oramai ineludibili.

A fronte degli scandali politici del 2016 e delle problematiche sorte in relazione ad un mondo connesso prevalentemente *on line* (più che in presenza) a causa della pandemia si è reso difatti del tutto evidente l'insufficienza dell'approccio tendenzialmente liberista prescelto per orientare la regolazione dei fenomeni di espressione e costruzione del consenso (anche politico) *on line* che ha caratterizzato per diversi anni le scelte normative e giurisprudenziali nel contesto europeo e americano. In entrambe le esperienze si è dunque assistito ad un'evoluzione recente in termini di spinta ad una maggiore regolazione di alcuni fenomeni e di più significativa responsabilizzazione degli attori privati che in ambito digitale svolgono funzioni e ruoli talmente importanti da essere qualificati come veri e propri poteri²⁶ in quello che si usa oramai

diritti fondamentali, in *Amministrare*, n. 3, 2017, 407.

²⁴ Cfr. P. NORRIS, R. INGLEHART, *Cultural Backlash, Trump, Brexit and Authoritarian Populism*, Cambridge, 2019.

²⁵ Sul tema E. ASSANTE, *Cosa ci può insegnare il caso Cambridge Analytica*, in *federalismi.it*, Editoriale, 25 aprile 2018. D. MESSINA, *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali*

alla luce della vicenda "Cambridge Analytica", in *federalismi.it*, n. 20, 2018.

²⁶ M. BETZU, *Poteri pubblici e privati nel mondo digitale*, in *La Rivista del Gruppo di Pisa*, n. 2, 2021, 166 ss.; A. VENANZONI, *Neofeudalesimo digitale: Internet e l'emersione degli Stati privati*, in *MediaLaws - Rivista di diritto dei media*, n. 3, 2020, 178 ss.

chiamare, forse ancora arditamente ²⁷, il costituzionalismo digitale ²⁸.

2. DEMOCRAZIA E LIBERTÀ DI ESPRESSIONE ON LINE FRA HARD, SOFT LAW ED AUTOREGOLAMENTAZIONE.

I tentativi di normazione del contesto digitale, — compresa la disciplina concernente la libertà di espressione del pensiero *on line* e l'eventuale contrasto a forme di abuso di tale libertà a tutela dei rapporti interindividuali e, più frequentemente, a garanzia della tenuta democratica degli ordinamenti interessati (a salvaguardia, dunque, della formazione di un'opinione pubblica libera e consapevole), — a causa delle riferite peculiarità del medesimo contesto digitale ove si registra, come si è evidenziato, un intreccio inestricabile fra funzione pubblica ed interesse privato, si presentano come multiformi e spesso sfuggono alle categorie tipiche di organizzazione delle fonti del diritto.

Si registra difatti, in tali ambiti, a fianco dell'imposizione normativa realizzata attraverso i classici strumenti regolatori di *hard law* (leggi statali o anche normative sovranazionali cogenti, assistite da apposite sanzioni in caso di mancato rispetto del loro dettato) un ampio utilizzo di strumenti di *soft law* (quali ad esempio i c.d. codici di condotta) e di normative coregolamentate che rappresentano il prodotto di una negoziazione fra l'autorità pubblica portatrice dell'interesse collettivo e gli *stakeholders* privati (principalmente le grandi aziende) che accettano di partecipare alla negoziazione e che reciprocamente si impegnano al raggiungimento di obiettivi condivisi. Sussistono infine forme di autoregolamentazione e di *policies* autoimposte dalle aziende private a loro stesse ed ai propri utenti; regole che nascono come accordi contrattuali e politiche aziendali le quali tuttavia hanno assunto ormai nel contesto digitale sfumature molto più complesse. In tempi recenti infatti l'autonormazione delle aziende private digitali ha acquisito caratteristiche peculiari e significative in quanto alcune grandi società hanno finanche predisposto, quale modalità di assistenza all'efficacia di tali tipologie di autonormazione, forme interne di controllo e sanzione di tipo "paragiurisdizionale": la c.d. Corte suprema di Facebook rappresenta un emblematico esempio di tale evoluzione ²⁹. Giacché sulla base

²⁷ Critico rispetto a tale espressione che considera equivoca e atecnica è G.E. VICEVANI, *Piattaforme digitali private, potere pubblico e libertà di espressione*, in *Diritto Costituzionale*, n. 1, 2023, 41 ss.

²⁸ A. VENANZONI, *Cyber-costituzionalismo: la società digitale tra silicolizzazione, capitalismo delle piattaforme e*

reazioni costituzionali, in *Rivista italiana di Informatica e Diritto*, n. 1, 2020, 5 ss.; T.E. FROSINI, *Il Costituzionalismo nell'età tecnologica*, in *Diritto dell'Informatica*, 2020, 465 ss.

²⁹ Su cui cfr. K. KLONIK, *The Facebook Oversight Board: Creating an Independent Institution to adjudicate on line*

della violazione di tali ultime tipologie regolatorie è accaduto che sia stato possibile escludere dall'accesso ai *social network* il Capo dello Stato di una delle più importanti potenze mondiali — cosa che è si è verificata quando nel 2021 Donald Trump è stato “bannato” da *Twitter* e da *Facebook* dopo l'assalto a *Capitol Hill* il 6 gennaio di quello stesso anno e riammesso solo molto tempo dopo sulla base proprio di una decisione ³⁰ assunta dal *Facebook Oversight Board* (il quale, in tale occasione, individuava come parametri di riferimento sia la Convenzione internazionale sui Diritti civili e Politici sia, mettendoli sullo stesso piano, i *Community Standards* di *Facebook*) ³¹ — è spontaneo interrogarsi su come il sistema delle fonti del diritto sia organizzato nel contesto digitale e quali siano le tendenze regolatorie recenti ed i *trend* normativi più efficaci ³².

3. LA DISCIPLINA SULLA LIBERTÀ DI ESPRESSIONE *ON LINE* e l'interpretazione funzionalistica della medesima libertà nelle democrazie liberali: gli stati europei e l'unione.

In alcuni ordinamenti giuridici la disciplina concernente la libertà di manifestazione del pensiero *on line* (così come la correlativa inversa tutela della libertà di informazione) è affidata, in modo “tradizionale”, alla normazione statale. Nel contesto europeo, esempi di normative eteroregolamentari sono rinvenibili nell'esperienza francese e tedesca così come è in corso di dibattito e approvazione una normativa statale su tali temi in Gran Bretagna. Si tratta di ordinamenti che, nel decidere di porre in essere normative statali su tali tematiche (il contrasto alla disinformazione e la tutela della formazione del libero consenso individuale e collettivo) dimostrano di aderire ad un'interpretazione funzionalistica della libertà di espressione piuttosto che ad una concezione prettamente individualistica della stessa e di intendere

free expression, in *Yale Law Journal*, vol. 129, 2020; D. WONG, L. FLORIDI, *Meta Oversight Board: A review and Critical Assessment*, in *Mind and Machines*, 2022; per la dottrina italiana cfr. A. IANNOTTI DELLA VALLE, *La giurisprudenza private nel mondo digitale al tempo della crisi della sovranità: il “modello” dell'Oversight Board di Facebook*, in *federalismi.it*, n. 26, 2021.

³⁰ *Case decision* 2021-001-FB-FBR del 5 maggio 2021. In tale vicenda l'*Oversight Board* di *Facebook* ha ritenuto legittima la sospensione dell'account del *Tycoon* ma non appropriata la sanzione senza la previsione di un termine finale (par. 9 dec.).

³¹ M. BETZU, *I Baroni del digitale*, cit. 64 ss.

³² Il tema del rapporto sussistente fra tali fonti del diritto è stato oggetto di interesse da parte del Comitato economico e sociale europeo il quale, nel 2015, ha adottato un Parere d'iniziativa avviando una riflessione per tentare di definire il quadro giuridico in cui tali strumenti devono operare nell'ambito dell'UE e precisandone le nozioni. Cfr. *Parere del Comitato economico e sociale europeo sul tema « Autoregolamentazione e coregolamentazione nel quadro legislativo dell'UE »*, (parere d'iniziativa) (2015/C 291/05), in *eurlex.europa.eu*. Sul tema per la dottrina italiana cfr. F. CAFACCI, *Crisi della statualità, pluralismo e modelli di autoregolamentazione*, in *Politica del Diritto*, 2001, 547 ss.

pertanto la democrazia in senso almeno parzialmente "militante" ³³.

L'interpretazione della libertà di manifestazione del pensiero in senso prevalentemente individualista valorizza tale facoltà quale diritto soggettivo individuale, personale, assoluto ed inviolabile che mal tollera compressioni da parte della sfera pubblica (a meno di situazioni estreme e rigorosamente determinate) ³⁴ e arriva finanche a negare la prevalente rilevanza del nesso fra il riconoscimento della libertà di espressione del pensiero e la democrazia dello Stato ³⁵.

Diversamente, coloro che vedono nella libertà di espressione anche una dimensione strumentale al "tutto" rispetto all'individuo, che del tutto rappresenta solo una parte ³⁶, postulano la necessità di accettare le limitazioni che si giustificano nel nome delle esigenze della collettività ³⁷.

Ne discende, da tale impostazione, l'ammissibilità di regole strumentali alla formazione di un'opinione pubblica libera e consapevole, alla tutela della completezza e dell'imparzialità delle informazioni ed alla salvaguardia del pluralismo delle idee.

La dottrina giuspubblicistica che sostiene una visione funzionalistica della libertà di espressione del pensiero si fonda difatti sul presupposto fondamentale per il quale tale libertà è composta tanto da una dimensione positiva (la libertà di esprimersi) quanto da una dimensione negativa (il diritto di informarsi) e dunque, in un'ottica funzionalistica, « l'essere compiutamente e realmente informati rappresenta una premessa indispensabile del buon funzionamento di un regime liberal-democratico: non soltanto nel senso che il diritto di ricevere e di ricercare informazioni costituisce un presupposto ed uno strumento perché si renda effettiva una libertà cardinale come quella di espressione o di manifestazione del pensiero; ma, prima ancora, nel senso che si tratta di un'esigenza indeclinabile per evitare che sia distorto il formarsi della pubblica opinione, cioè del consenso sul quale si reggono le

³³ Cfr. A. DI GIOVINE (a cura di), *Democrazie protette e protezione della democrazia*, Torino, 2005.

³⁴ In tale corrente dottrinale si iscrivono certamente le riflessioni di C. ESPOSITO, *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Milano, 1958; S. FOIS, *Principi costituzionali e libera manifestazione del pensiero*, Milano, 1957; L. PALADIN, *Problemi e vicende della libertà di informazione nell'ordinamento giuridico italiano*, in P. PALADIN (cur.), *La libertà di informazione*, Torino, 3-62.

³⁵ Tale è ad esempio l'opinione di Esposito, *op. cit.*, il quale emblematicamente afferma che « una siffatta interpretazione

dell'art. 21 della Costituzione esclude dunque ogni nesso praticamente rilevante tra l'articolo stesso e la proclamazione della democraticità dello Stato italiano e ritiene errati i diffusi tentativi di configurare questo diritto (allo stesso modo di quello di iscrizione ai partiti) come "essenzialmente" diretto a garantire ai singoli la possibilità di concorrere a determinare la politica nazionale », 11.

³⁶ Su tale approccio ancora A. PACE, *op. cit.*, spec. p. 14.

³⁷ Cfr. P. BARILE, *Libertà di manifestazione del pensiero*, Milano, 1975; C. CHIOLA, *Informazione, pensiero, radiotelevisione*, Napoli, 1984.

maggioranze di governo e del dissenso da cui le opposizioni ricavano alimento »³⁸. A partire da tale presupposto è evidente come dall'indole funzionale non si intende far derivare una delimitazione sostanziale dell'espressione del pensiero a tutela delle ideologie dominanti giacché « la corretta posizione è quella di chi intende l'aggettivo "funzionale" in termini metodologici, che "prescindono da ogni preclusione di contenuti", e che anzi pongono la diffusione di ogni ideologia "quale momento irrinunciabile del metodo democratico" [...] essenziale per la definizione e l'attuazione della forma democratica di governo »³⁹.

Le concezioni individualiste della libertà di espressione concepiscono dunque la medesima libertà quale prodotto (e al tempo stesso motore) della democrazia intesa come principio (quale bene iniziale che chiede di essere realizzato aderendo a quanto da esso prescritto). Le concezioni funzionaliste pongono invece in relazione la libertà di espressione con le necessità del processo democratico e nel fare questo, nel tentativo di non scadere in deviazioni autoritarie, non assurgono la democrazia in sé ma il "metodo democratico" quale valore cui tendere⁴⁰ funzionalizzando le possibili limitazioni alla libertà di espressione del pensiero alle esigenze della democrazia come metodo in un'ottica di garanzia anche contromaggioritaria a tutela della corretta ed eguale partecipazione democratica. In questo senso non sorprende che nell'esperienza di matrice europea, ove si è sviluppata una giurisprudenza vivace in tema di limitazione della libertà di espressione del pensiero per abuso del medesimo diritto essa è collegata spesso al divieto di discriminazione⁴¹.

Tali osservazioni, nella loro essenzialità, sono sufficienti a definire la profonda differenza intercorrente fra le normative francese e tedesca (oltre alla proposta britannica) in tema di intervento statale a tutela della manipolazione informativa rispetto ad alcune normative nazionali extraeuropee rinvenibili ad esempio in Russia, Malesia e Cina ove, con il dichiarato intento di reprimere la disinformazione, si persegue invece la tutela dell'apparato al potere e la repressione del dibattito democratico⁴².

³⁸ L. PALADIN, *Problemi e vicende della libertà di informazione nell'ordinamento giuridico italiano*, in Ib. (a cura di), *La libertà di informazione*, Torino, 1979, 3.

³⁹ P. BARILE, *Libertà di manifestazione del pensiero*, Milano, 1975, 10.

⁴⁰ Sul tema valori, principi e regole cfr. G. ZACREBIRSKY, *La legge e la sua giustizia*, Bologna, 2008, 205 ss.

⁴¹ Diversamente rispetto all'esperienza statunitense la giurisprudenza europea, e in particolare la giurisprudenza CEDU, ha sanzionato difatti con grande frequenza i discorsi e le manifestazioni di

opinione d'odio utilizzando l'art. 17 come parametro accessorio (insieme, spesso, con il principio di non discriminazione sancito dall'art. 14 CEDU) nelle decisioni di inammissibilità riguardanti ricorsi per violazione dell'articolo 10 CEDU avanzati da persone condannate per espressioni negazioniste così come in relazione ad affermazioni finalizzate al sostegno di attività terroristiche. Sul punto C. CARUSO, *L'hate speech a Strasburgo: il pluralismo militante del sistema convenzionale*, in *Quaderni Costituzionali*, n. 4, 2017, 963 ss.

⁴² Cfr. sul tema T. GUERINI, *Fake news*

3.1. *La normativa specificatamente orientata al contrasto alla disinformazione politica: il caso francese.*

Un ordinamento che ha adottato una normativa specificatamente dedicata alla lotta alla manipolazione dell'informazione in ambito digitale a tutela dei momenti di esercizio dei diritti democratici è la Francia che, nel dicembre del 2018, ha varato la nota legge n. 1202. Il 22 dicembre 2018, lo stesso giorno dell'approvazione della *Loi relative à la lutte contre la manipulation de l'information*, è stata adottata anche una legge organica (la n. 1201) composta da 2 soli articoli al fine di coordinare la detta normativa ad alcune disposizioni di applicazione costituzionale.

La legge n. 1202 è stata fortemente voluta dal gruppo politico fondato dal Presidente Macron "*La République en marche*" ed è stata altresì oggetto di vivide critiche ed aspro contrasto da parte della destra radicale (e moderata) francese, opposizione che è sfociata, infine, in una *saisine parlementaire* con la quale è stato adito il Consiglio Costituzionale.

La normativa tenta di elaborare una disciplina complessiva che vada a regolare il tema della lotta alla disinformazione sia in ambito digitale sia nell'attività dei media tradizionali quando sono sottoposti ad un controllo da parte di uno Stato straniero. Ciò al più che evidente fine di sottrarre il Paese a manipolazioni intese a scuotere il sistema democratico francese al di là del dibattito politico tradizionale⁴³. Una parte della legge (gli artt. dal 5 al 10) è dedicata dunque a tali tipologie di emittenti radiotelevisive e prevede essenzialmente l'attribuzione di nuovi poteri al Consiglio superiore dell'audiovisivo ("CSA"), per impedire, sospendere o terminare la diffusione di servizi televisivi controllati da uno Stato straniero in caso di violazione degli interessi fondamentali dello Stato francese (Titolo II). A partire dall'art. 11, la legge n. 1202 riguarda invece il contrasto alla disinformazione *on line* prevedendo diverse norme orientate a predisporre obblighi e regole agli operatori delle piattaforme digitali nel periodo della campagna elettorale. Difatti, i vincoli imposti dalla legge francese sono limitati temporalmente ai quattro mesi precedenti la data delle elezioni politiche (più precisamente tre mesi prima del primo giorno del mese in cui è prevista una tornata elettorale) fino al giorno del voto. Durante tale arco temporale gli intermediari digitali, la cui attività supera un determinato numero di connessioni sul territorio francese (cifra che tuttavia la legge non definisce rinviando ad una successiva deter-

e diritto penale. la manipolazione digitale del consenso nelle democrazie liberali, Torino, 2020, spec. 83 ss.

⁴³ Cfr. P. MOURON, *Du Sénat au Con-*

seil constitutionnel: adoption des lois de lutte contre la manipulation de l'information, in *Revue européenne des médias et du numérique*, 2019, n. 49, 9 ss.

minazione amministrativa) sono tenuti a degli obblighi di trasparenza nei confronti dei propri utenti circa l'identità delle persone fisiche e giuridiche che diffondono *on line* contenuti di tipo politico a pagamento, nonché su come i dati personali degli utenti vengono utilizzati nel contesto della comunicazione politica.

I gestori delle piattaforme sono anche tenuti a dichiarare l'ammontare dei compensi ricevuti e tali dichiarazioni sono utilizzate per la compilazione di un registro elettronico disponibile *on line* per tutto il periodo della campagna elettorale ⁴⁴.

La normativa introduce poi un particolare tipo di *référé* in quanto prevede che su apposita istanza il Pubblico ministero, un candidato, un partito politico o chiunque abbia interesse ad agire (ferma restando la possibilità di chiedere ed ottenere un risarcimento al danno qualora provato) possono chiedere che l'autorità giudiziaria adotti misure necessarie e proporzionali finalizzate ad impedire la perdurante circolazione di informazioni diffuse « deliberatamente, artificialmente o automaticamente e in modo massiccio, per mezzo di un servizio di comunicazione pubblica online » in relazione alle quali si pongono in essere « accuse inesatte o fuorvianti o imputazioni di un fatto suscettibili di influenzare la sincerità del voto » ⁴⁵.

È stato efficacemente osservato come nella normativa francese si sia dunque tentato di contemperare il giusto bilanciamento fra lotta alla disinformazione politica in ambito digitale e libertà di espressione evitando di ostacolare di per sé la diffusione delle c.d.

⁴⁴ Art. 1, comma 2: « 2° Au début du chapitre VI du titre II, sont insérés des articles L. 163-1 et L. 163-2 ainsi rédigés: Art. L. 163-1.-Pendant les trois mois précédant le premier jour du mois d'élections générales et jusqu'à la date du tour de scrutin où celles-ci sont acquises, les opérateurs de plateforme en ligne au sens de l'article L. 111-7 du code de la consommation dont l'activité dépasse un seuil déterminé de nombre de connexions sur le territoire français sont tenus, au regard de l'intérêt général attaché à l'information éclairée des citoyens en période électorale et à la sincérité du scrutin; 1° De fournir à l'utilisateur une information loyale, claire et transparente sur l'identité de la personne physique ou sur la raison sociale, le siège social et l'objet social de la personne morale et de celle pour le compte de laquelle, le cas échéant, elle a déclaré agir, qui verse à la plateforme des rémunérations en contrepartie de la promotion de contenus d'information se rattachant à un débat d'intérêt général; 2° De fournir à l'utilisateur une information loyale, claire et transparente sur l'utilisation de ses données personnelles

dans le cadre de la promotion d'un contenu d'information se rattachant à un débat d'intérêt général; 3° De rendre public le montant des rémunérations reçues en contrepartie de la promotion de tels contenus d'information lorsque leur montant est supérieur à un seuil déterminé. Ces informations sont agrégées au sein d'un registre mis à la disposition du public par voie électronique, dans un format ouvert, et régulièrement mis à jour au cours de la période mentionnée au premier alinéa du présent article. Les modalités d'application du présent article sont définies par décret ». Cfr. <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559>.

⁴⁵ « Art. L. 163-2.-I.-Pendant les trois mois précédant le premier jour du mois d'élections générales et jusqu'à la date du tour de scrutin où celles-ci sont acquises, lorsque des allégations ou imputations inexactes ou trompeuses d'un fait de nature à altérer la sincérité du scrutin à venir sont diffusées de manière délibérée, artificielle ou automatisée et massive par le biais d'un service de communication au public en ligne », Cfr. <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559>.

fake news quanto invece scegliendo di impedirne la circolazione solo nella misura in cui tali informazioni false e alterate possono considerarsi in grado di influenzare negativamente la libertà del voto e quando tale disinformazione sia da intendersi intenzionale e tendenziosa ⁴⁶. Tale approccio relativamente cauto circa l'applicazione dei principi della democrazia militante richiama certamente l'orientamento concernente i temi della difesa della democrazia proposto nella più recente giurisprudenza Cedu riguardante la necessità che, al fine di limitare una forma di espressione seppur odiosa o pericolosa, occorre che possa essere provato non solo il carattere antisistemico di un'idea, ma che alla base della decisione di limitare la possibilità che quell'idea venga sostenuta attivamente vi sia un "*pressing social need*" ⁴⁷.

Nel dicembre del 2018 il *Conseil constitutionnel* si è pronunciato sulla legittimità costituzionale delle disposizioni previste nella legge n. 1202 e nella legge organica n. 1201. Il *Conseil constitutionnel* era stato adito, nell'ambito di tre ricorsi preventivi di costituzionalità sollevati da oltre sessanta deputati e sessanta senatori. Un terzo ricorso era stato invece sollevato dal Primo ministro (in applicazione del quinto comma dell'art. 46 e del primo comma dell'art. 61 della Costituzione) in merito alla legge organica che rende applicabili all'elezione presidenziale le misure introdotte dalla legge ordinaria. Con le decisioni nn. 2018-773 (DC2) e 2018-774 (DC3) il *Conseil* ha dichiarato le disposizioni impugnate conformi alla Costituzione, ponendo tuttavia alcune riserve di interpretazione. I ricorrenti lamentavano diverse lesioni di costituzionalità attinenti al principio di legalità, alla libertà di iniziativa economica ed alla libertà di informazione. Uno degli elementi interessanti del ricorso delle minoranze parlamentari è certamente il fatto che esso, fra le altre cose, stigmatizzava una generale indeterminatezza di alcuni passaggi tecnici della legge sottoposta a vaglio costituzionale ⁴⁸ e contestava l'assenza di definizione di criteri dettagliati volti a consentire al giudice ordinario, eventualmente adito, di valutare con sicurezza quando una forma espressiva merita di essere limitata a tutela dell'interesse collettivo.

Il Consiglio costituzionale ha tuttavia respinto tutti i motivi del ricorso ritenendo che la legge sottoposta a valutazione non com-

⁴⁶ M.R. ALLEGRI, *Oltre la par condicio*, p. 120.

⁴⁷ M. OROFINO, *La libertà di espressione tra Costituzione e carte europee dei diritti. Il dinamismo dei diritti in una società in continua trasformazione*, Torino, 2014. Cfr. anche C. CARUSO, *L'hate speech a Strasburgo: il pluralismo militante del sistema convenzionale*, cit., 963 ss.

⁴⁸ Ad esempio la nozione di "contenuti di informazione in relazione con un dibattito di interesse generale", la quale determina il campo di applicazione degli obblighi di imposti alle piattaforme digitali, viene contestata come concetto non sufficientemente preciso in una normativa che disciplina una sanzione penale.

portasse alcun pregiudizio alla libertà di informazione e comunicazione come prevista e disciplinata nell'ordinamento francese. Il Consiglio ha fondato la propria decisione sulla considerazione per cui spetta al legislatore, nella sua piena discrezionalità, bilanciare i valori costituzionali che in questo caso sono il principio della sincerità e libertà del voto e il diritto alla libertà di espressione del pensiero. Il Consiglio costituzionale ha evidenziato, peraltro, che in considerazione del fatto che l'applicazione della legge è circoscritta prevalentemente al momento elettorale essa è caratterizzata dalla finalità di garantire la libertà e la correttezza della formazione del consenso e tale specialità, perimetrata ad un lasso di tempo definito e particolarmente delicato, consente che le sue previsioni possano essere considerate legittime.

3.2. *La normativa sull'hate speech on line nell'esperienza tedesca.*

Diversamente rispetto a quanto posto in essere in Francia la nota legge tedesca *Netzwerkdurchsetzungsgesetz* (NetzDG), in vigore a partire dal primo ottobre 2017, non è circoscritta al momento elettorale e si pone invece quale normativa statale rivolta prevalentemente ai *social networks* al fine di contrastare sia, in generale (dunque in ogni momento), la disinformazione *on line* sia (soprattutto) i discorsi d'odio in ambito digitale ⁴⁹. È tuttavia evidente come la portata di un impianto regolatorio di tal genere abbia delle significative ricadute anche in periodo elettorale e che, se pur volta al contrasto delle notizie false e dell'*hate speech* nell'*agorà* digitale, finisce per porsi in modo importante a garanzia della corretta informazione politica.

Destinatari delle normative sono le piattaforme digitali di grandi dimensioni (individuate in quelle che vedono la registrazione di più di due milioni di utenti in Germania) non editoriali ⁵⁰.

La legge tedesca essenzialmente si propone come un modello di regolamentazione imposto per via normativa adottato sulla base della considerazione politica per cui le piattaforme digitali non

⁴⁹ Difatti, al c. 3 dell'art. 1 la legge rinvia al codice penale tedesco per definire ciò che può essere considerato contenuto illegale *on line*. Fra le condotte indicate figurano: la diffusione della propaganda di organizzazioni anticonstituzionali e l'uso di simboli di tali organizzazioni; la preparazione di azioni sovversive; l'incitamento alla commissione di reati contro lo Stato; l'istigazione pubblica a commettere atti criminali, l'apologia di reato e la creazione di organizzazioni criminali e terroristiche; la falsificazione (nel cui ambito possono essere comprese le *fake news*) nonché la falsifica-

zione di elementi probatori; il disturbo della quiete pubblica; l'incitamento all'odio, l'ingiuria e la diffamazione; la diffusione di immagini violente; il vilipendio di confessioni religiose e di associazioni religiose o ideologiche; la distribuzione, l'acquisizione e il possesso di materiale pedopornografico.

⁵⁰ L'art. 1 si riferisce infatti alle piattaforme informatiche che, a scopo di profitto, permettono la condivisione di contenuti fra utenti. Sono inoltre escluse quali destinatarie della normativa le piattaforme che offrono servizi di messaggistica istantanea.

davano adeguatamente esecuzione alle regole di autonormazione cui si erano vincolate impegnandosi a meccanismi di *content moderation*. La legge, dunque, impone normativamente un sistema di *notice and takedown* attivabile dagli utenti, obbligatorio per le aziende digitali, e prevede aspre sanzioni qualora non adeguatamente ottemperato. Essa tuttavia, attraverso tale impianto, si affida moltissimo alla discrezionalità del gestore con riguardo all'effettiva decisione da assumere circa il contenuto segnalato. Ciò con evidenti rischi di c.d. "privatizzazione della censura" paragonabile, *mutatis mutandis*, alla "*collateral censorship*" di matrice statunitense suscettibile di assumere caratteri del tutto "arbitrari" o, anche peggio, basati su bilanciamenti di interessi posti in essere e risolti direttamente dalle *corporations*⁵¹. La normativa tedesca impegna le piattaforme digitali ad impedire che si verifichino *on line* fattispecie già definite nel codice penale tedesco⁵². Con ciò tuttavia la detta normativa realizza una delegazione della repressione penale a dei privati (i gestori dei *social network*) estromettendo in tale ambito (limitato ma pur sempre significativo) la magistratura. Tale impianto è peraltro reso ancor più grave dalla considerazione per cui il detto privato affida il medesimo compito alla determinazione algoritmica⁵³.

Giacché le sanzioni previste dalla legge tedesca in caso di inottemperanza alla normativa sono significative (dai 500 mila ai 5 milioni di euro) è evidente come tale disciplina corra il rischio di spingere il gestore informatico alla rimozione di un contenuto segnalato senza procedere ad attente valutazioni di merito. Tale esito è peraltro favorito da altri elementi che connotano la normativa, ovvero i ristretti limiti di tempo di cui i gestori dispongono per la valutazione delle segnalazioni, l'assenza di criteri indicati dalla legge al fine di valutare tale illiceità, la mancata previsione di conseguenze sul piano sanzionatorio in caso di rimozione arbitraria dei contenuti illeciti, l'impossibilità per gli utenti della piattaforma (tanto gli autori della segnalazione quanto i produttori del contenuto segnalato) di ricorrere al giudice avverso la decisione di rimozione⁵⁴.

⁵¹ Cfr. sul tema M. MONTI, *Privatizzazione della censura e Internet platforms: la libertà d'espressione e i nuovi censori dell'agorà digitale*, in *Rivista italiana di informatica e Diritto*, n. 1, 2019, 35 ss.

⁵² Come l'uso di simboli di organizzazioni incostituzionali, la diffamazione del Presidente della Repubblica Federale, l'istigazione a delinquere, la violazione della pace pubblica con minacce di reati, l'istigazione all'odio, l'apologia di reato, la diffamazione religiosa o ideologica, l'insulto, la diffamazione, il possesso e la diffusione di materiale pedopornografico.

⁵³ Cfr. E. FALETTI, *Discriminazione algoritmica*, Torino, 2022.

⁵⁴ Cfr. sul punto V. CLAUSSEN, *Fighting hate speech and fake news. The Network enforcement Act (NetzDG) in Germany in the context of European Legislation*, in *Media Law*, n. 3, 2018, 110 ss. Cfr.

È proprio nella mancata previsione di un possibile intervento dell'autorità giudiziaria che risiede peraltro la maggior criticità della normativa tedesca. Difatti la procedura di *notice and take down* si svolge sotto la supervisione di un organismo di autoregolazione designato da un'autorità amministrativa (l'Ufficio federale di giustizia). Tale organismo, pur definito "indipendente" applica tuttavia principi amministrativi definiti a livello ministeriale (art. 4 c. 5) ed è inoltre finanziato nelle sue attività dagli stessi *social network* (art. 3. c. 6 punto 4) ⁵⁵. L'organismo indipendente detto, al momento dell'adozione della normativa nel 2017, era l'unica autorità dinanzi alla quale eventualmente si svolgeva una procedura in contraddittorio (di valutazione dei contenuti rimossi) fra i gestori della piattaforma e colui che aveva prodotto l'informazione segnalata e sanzionata.

Il *NetzDG*, dunque, per le sue specificità, era una normazione che si prestava a numerose critiche collegate al fatto che si trattasse di una normativa che favoriva le pratiche censorie di stampo privatistico e non offriva, d'altra parte, adeguate garanzie giurisdizionali. A ragione di ciò il dibattito sull'opportunità di apportare adeguate modifiche a tale disciplina è stato vivamente sentito in Germania ed ha condotto ad alcune novelle normative nel 2021. La legge di modifica del *NetzDG* ha, fra le altre cose, introdotto oltre alla possibilità di instaurazione di un arbitrato volontario, anche un meccanismo (garantito dall'anonimato) di confronto fra colui che segnala un illecito *on line* e il soggetto che materialmente ha prodotto il dato segnalato e sottoposto a procedura di rimozione. Tale meccanismo, che avviene attraverso la mediazione del *social network*, garantendo il reciproco anonimato delle parti, consente un confronto fra le parti di tipo preventivo e si pone a forma minimale di garanzia della libertà di espressione *on line* evitando che la semplice segnalazione di un contenuto sia elemento sufficiente per rimuoverlo.

La normativa tedesca sul contrasto alla disinformazione e l'odio *on line* in quanto pioniera nel tentativo di porre in essere una regolamentazione statale di ampio respiro sul tema è stata oggetto di ispirazione in ambito comparato tanto da essere definita "*the involuntary godmother of more and more children*" ⁵⁶. L'impianto normativo tedesco ha evidentemente influenzato anche un tentativo di proposta di legge italiana su tali temi la quale, tuttavia, non ha completato il suo *iter legis* ⁵⁷.

anche M.R. ALLEGRI, *Oltre la par condicio*, cit., 115 ss.

⁵⁵ C. MAGNANI, *Libertà di informazione online e fake news: vera emergenza? Appunti sul contrasto alla disinformazione tra legislatori statali e politiche europee*, in *Quaderni costituzionali*, 4 aprile 2019.

⁵⁶ L. SHULDT, *The rebirth of Malaysia's fake news law — and what the NetzDG has to do with it*, in <https://verfassungsblog.de/malaysia-fake-news/> (13 aprile 2021).

⁵⁷ Ci si riferisce al disegno di legge presentato a dicembre 2017 per iniziativa dei senatori Zanda e Filippin, intitolato

3.3. *L'ibridazione fra hard law e soft law nella proposta di legge britannica.*

Un'ulteriore proposta di normazione per via legislativa di tali tematiche è in corso di approvazione anche nell'esperienza britannica ove, differentemente dalla regolamentazione posta in essere da Francia e Germania, l'ipotesi normativa in discussione prevede la necessità di affiancare alla disciplina tradizionale eminentemente statale la predisposizione di misure di *soft law*.

Il percorso intrapreso da Regno Unito « *To support our ambition for the UK to be the safest place in the world to be online* » è descritto in un *Digital Charter*⁵⁸ pubblicato *on line* il 25 gennaio 2018 (modificato da ultimo l'8 aprile 2019) ove il governo britannico ha descritto la propria strategia concernente la normazione dell'ecosistema digitale caratterizzata dalla contemporanea adozione di una normativa statale impositiva di tipo tradizionale e la promozione di alcuni codici di condotta che impegnino le grandi aziende del digitale a obblighi di trasparenza e sorveglianza sui comportamenti "abusivi".

Sulla scorta di tale ipotesi di strategia d'azione è stato approvato in primo luogo il *Data Protection Act*⁵⁹, in vigore dal 25 maggio 2018, mentre ad aprile 2019 è stato pubblicato il *Code of Practice for providers of online media platforms*⁶⁰ ovvero un codice di condotta indirizzato sia ai gestori delle piattaforme di *social networking* sia a qualsiasi sito che ospiti contenuti o commenti *user-generated*. Il Codice contiene indicazioni non giuridicamente vincolanti e *best practice* da seguire al fine di impegnare gli intermediari digitali a prevenire condotte scorrette da parte degli utenti (*bullying, insulting, intimidating and humiliating behaviours*). In particolare, si raccomanda a tutti gli intermediari digitali di predisporre procedure chiare e facilmente accessibili agli utenti affinché questi ultimi possano segnalare i contenuti inappropriati; di prevedere meccanismi rapidi ed efficienti di gestione delle segnalazioni ricevute e di *feedback* (possibilmente entro ventiquattro ore); di inserire nelle condizioni d'uso rivolte agli utenti informazioni chiare e precise su quali condotte siano da ritenersi nocive (*harmful*), quali conseguenze

« Norme generali in materia di social network e per il contrasto della diffusione su Internet di contenuti illeciti e delle fake news » (AS n. 3001).

⁵⁸ <https://www.gov.uk/government/publications/digital-charter/digital-charter>.

⁵⁹ <https://ico.org.uk/for-organisations/data-protection-act-2018/>. Il *Data Protection Act*, normativa attinente al regime ed alla protezione dei dati nel Regno Unito va a sostituire il precedente *Data Protection*

Act del 1998 e si affianca al *Uk GDPR* (*General Data Protection Regulation*). La normativa britannica concernete il trattamento e la tutela dei dati personali, in quanto di derivazione europea, è stata emendata sulla base dello *European Union (Withdrawal) Act*.

⁶⁰ <https://www.gov.uk/government/publications/code-of-practice-for-providers-of-online-social-media-platforms/code-of-practice-for-providers-of-online-social-media-platforms>.

per gli utenti derivino da tali condotte e quali siano le linee guida e le *policies* seguite dalla piattaforma per la rimozione dei contenuti inappropriati ⁶¹.

Non sono tuttavia previste conseguenze in caso di mancato rispetto delle indicazioni contenute nel Codice che dunque è sostanzialmente affidato all'impegno assunto dai gestori delle piattaforme nel sottoscriverlo.

Infine, sempre ad aprile 2019, il governo britannico ha presentato un pacchetto di misure legislative e non legislative nel c.d. *Online Harms White Paper* ⁶². La proposta normativa che prevedeva la previsione di una nuova autorità indipendente preposta alla sorveglianza della sicurezza in rete, l'adozione di regole cogenti per i *social network* concernenti l'obbligo di vigilanza e la pronta rimozione della pubblicazione di contenuti illeciti è stata sottoposta ad una consultazione pubblica che si è conclusa alla fine del mese di giugno 2019. Quanto ipotizzato nell'*Online harms white paper* è confluito in una proposta di legge formulata nel 2021 e nota come *On line safety bill* ⁶³ tuttora in corso approvazione in Parlamento. Diversamente dalle proposte iniziali la normativa attualmente in discussione non prevede più la predisposizione di un'apposita autorità indipendente preposta alla sorveglianza del rispetto delle regole del contesto digitale ma affida all'*Ofcom* (l'*Office of Communication*) i detti compiti di supervisione. La stessa normativa ha inoltre visto nel corso del tempo una progressiva riduzione dell'elenco dei contenuti da rimuovere: mentre difatti, inizialmente, la proposta normativa ipotizzava come rimuovibili anche i contenuti "leciti ma dannosi" la successiva polemica sorta in relazione alla necessità di garantire *on line* il libero dibattito privo di censure non necessarie ⁶⁴ ha spinto a sancire il possibile divieto come circoscritto esclusivamente a forme di discorso illecite.

3.4. L'evoluzione normativa nell'esperienza dell'Unione europea dalla direttiva e-commerce al Digital Services Act.

L'Unione Europea si è caratterizzata per un approccio iniziale tendenzialmente liberista, mutuato probabilmente dall'esperienza statunitense. Tale orientamento si è manifestato emblema-

⁶¹ La proposta normativa è analizzata da M.R. ALLECRI, *Oltre la par condicio*, cit. 124 ss.

⁶² <https://www.gov.uk/government/news/uk-to-introduce-world-first-online-safety-laws> e <https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper>.

⁶³ <https://bills.parliament.uk/bills/>

3137. Cfr. anche <https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill>.

⁶⁴ "Online safety bill 'a recipe for censorship', say campaigners". *The Guardian*. 12 May 2021. <https://www.theguardian.com/media/2021/may/12/uk-to-require-social-media-to-protect-democratically-important-content>.

ticamente nell'adozione, in tempi oramai risalenti, della direttiva n. 2000/31/CE ⁶⁵ la quale sanciva sostanzialmente il c.d. dogma della irresponsabilità degli intermediari digitali ⁶⁶. La c.d. direttiva *e-commerce* viene adottata all'inizio degli anni duemila, in un contesto digitale decisamente più semplificato di quello attuale, con l'obiettivo di favorire la libera circolazione e la promozione dei servizi della società dell'informazione eliminando gli ostacoli allo sviluppo del commercio elettronico. A tal fine gli intermediari digitali — compresi gli *hosting provider*, quelli cioè che ospitano contenuti *user generated* — non vengono ritenuti responsabili di ciò che gli utenti di Internet producono e diffondono attraverso i servizi da essi prestati né sono tenuti ad esercitare attività di monitoraggio e controllo delle attività degli utenti *on line* in quanto si presuppone che il gestore della piattaforma digitale assuma una posizione neutrale rispetto alle condotte degli utenti. Unica forma di attenuazione rispetto a tale impianto estremamente garantista nei confronti dei gestori delle piattaforme digitali è la previsione per la quale essi sono tenuti ad attivarsi per inibire l'accesso al contenuto illecito (rimuovendolo) nel caso in cui vengano effettivamente a conoscenza dell'illiceità del contenuto (secondo un meccanismo di *notice and takedown*) ovvero per ottemperare ad un ordine delle competenti autorità giudiziarie o amministrative ⁶⁷. La presunta posizione di neutralità del *provider*, sancita per legge, esclude che i gestori delle piattaforme digitali possano essere gravati da obblighi di sorveglianza preventiva o di filtraggio sistematico.

Tale impianto regolatorio ha subito numerose critiche concernenti l'insufficienza di tali previsioni ed ha visto anche l'affermazione, per via giurisprudenziale, precipuamente nel contesto italiano, di ipotesi di attenuazione della rigidità di tale sistema facendo leva sul 42 considerando della dir. 2000/31/CE in base al quale le esenzioni di responsabilità per i contenuti di terzi possono riguardare solo il *provider* la cui attività è di ordine meramente tecnico. In considerazione del fatto che alcuni aggregatori di contenuti caricati in rete da terzi (ossia gli *User Generated Content* ovvero i *social networks*) non si limitano ad "ospitare" contenuti forniti da terzi in maniera passiva ed automatica ma svolgono una peculiare attività in termini di indicizzazione, selezione ed organizzazione e filtraggio dei contenuti stessi (giacché traggono dall'aggregazione od organizzazione dei detti contenuti

⁶⁵ 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").

⁶⁶ La bibliografia sulla direttiva *e-commerce* è sterminata. Si rinvia esemplificativamente a M. BASSINI, *Internet e diritto*, cit. ed alla bibliografia ivi citata.

⁶⁷ Art. 14 Direttiva 2000/31/CE.

un margine di profitto), l'attività di tali soggetti non appare inquadrabile nei confini dell'irresponsabilità dell'intermediario *hosting* (delineata, in Italia, dal d.lgs. n. 70/03) che, di conseguenza, va interpretata come riferita esclusivamente all'*hosting* passivo⁶⁸.

A fronte delle diffuse critiche oramai decennali nei confronti dell'insufficienza della direttiva *e-commerce* a normare il vastissimo tema della libertà di espressione del pensiero *on line* (e correlative responsabilità) oltre che in considerazione delle numerose vicende che hanno scosso l'opinione pubblica europea ed internazionale (i già citati casi *Brexit* e *Cambridge Analytica*) in relazione alle quali si è reso evidente che il tema della espressione nell'agorà digitale non può essere limitato ai suoi confini commerciali possedendo difatti, tale ambito, il potenziale per condizionare la tenuta democratica degli ordinamenti che compongono l'Unione (oltre che, ovviamente, la stessa organizzazione sovranazionale), la Commissione Europea, dopo un'ampia consultazione degli *stakeholders*, ha elaborato due proposte di regolamento che sono confluite nel *Digital services Act*⁶⁹ e il *Digital Market Act*⁷⁰.

Il *Digital Services Act* ed il *Digital Market Act* seguono ad una

⁶⁸ L'elaborazione giurisprudenziale della figura dell'*hosting* attivo è stata dibattuta nella vicenda giudiziaria avente origine nel caso *RTI c. Yahoo*, deciso dal Tribunale Di Milano il 9 settembre 2011. In tale occasione veniva affermato il principio secondo cui l'associazione di messaggi pubblicitari ai contenuti immessi in rete dagli utenti, i cui proventi concorrono a finanziare l'attività del prestatore di servizi, dovevano essere qualificati come servizi di *hosting* attivo, esorbitando dunque da qualsiasi posizione di pretesa neutralità del prestatore e rendendo inapplicabile la disciplina di cui all'art. 16 d.lgs. n. 70/03 a favore di una valutazione della sua condotta secondo le comuni regole della responsabilità civile. A fronte della decisione di accoglimento dell'impugnazione adottata in appello con sentenza del 7 gennaio 2015, n. 38, la Corte di Cassazione, con la sentenza del 19 marzo 2019, n. 7708, ha accolto il ricorso di Rete Televisive Italiane S.p.A. (R.T.I.) nei confronti di Yahoo! Inc. e di Yahoo! Italia S.r.l. sancendo il concetto di *hosting* "attivo" ravvisabile qualora vi sia una condotta di azione che completa e arricchisce in modo non passivo la fruizione dei contenuti da parte dell'*hosting provider*. Tale "attività" può desumersi da una serie di "indici di interferenza" (che il giudice è tenuto ad accertare) ovvero le attività di filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso,

modifica, estrazione o promozione dei contenuti, operate mediante una gestione imprenditoriale del servizio, come pure l'adozione di una tecnica di valutazione comportamentale degli utenti per aumentarne la fidelizzazione. Per una lettura critica sulla detta giurisprudenza si rinvia a M. BASSINI, *La Cassazione e il simulacro del provider attivo: mala tempora currunt*, in *Media Laws*, n. 2, 2019 ed a L. TORMEN, *La linea dura della Cassazione in materia di responsabilità dell'hosting provider (attivo e passivo)*, in *La nuova giurisprudenza civile commentata*, n. 5, 2019, 1039 ss. In termini maggiormente adesivi alla giurisprudenza detta è invece R. PANETTA, *Il ruolo attivo degli intermediari di Internet e la conseguente responsabilità civile*, in *Diritto e Internet*, n. 2, 2019, 173 e ss. In termini più ampi sul tema si rinvia a O. POLLICINO, E. APA, *Modeling the Liability of Internet Service Providers: Google vs. Vivi Down. A Constitutional Perspective*, Milano, 2013 ed a M.L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, Milano, 2018.

⁶⁹ 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>.

fase nel corso della quale l'Unione Europea ha tentato, tenendo fermo l'impianto normativo della direttiva *e-commerce*, di responsabilizzare maggiormente gli *Internet service providers* attraverso l'elaborazione di strumenti di *Soft Law* ⁷¹.

Nel dicembre del 2015, subito dopo gli attentati terroristici di natura islamica avvenuti a Parigi (il precedente 13 novembre) la Commissione ha avviato un progetto, l'*EU Internet forum*, per unire forze politiche, istituzioni e aziende del digitale nella lotta contro la diffusione di contenuti terroristici e odio *online*.

Successivamente, il 31 maggio 2016, la commissione ha promosso l'adozione da parte di quattro tra le principali aziende informatiche (*Facebook*, *Twitter*, *Youtube* e *Microsoft*) di un codice di condotta volto alla lotta delle forme illegali di incitamento all'odio *on line*. Il medesimo strumento è stato successivamente adottato anche da altre grandi aziende come *Google*, *Instagram*, *Snapchat* e *Dailymotion*. Il 28 settembre 2017 è stata inoltre pubblicata una comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni dal titolo "lotta e contenuti illeciti *online*". Verso una maggiore responsabilizzazione delle piattaforme *online*", seguita dalla Raccomandazione 2018/334 del primo marzo 2018 sulle misure per contrastare efficacemente i contenuti illegali *on line*. A detti strumenti di regolazione attraverso il *soft law* sono seguiti, a partire dal 2018, delle scelte normative maggiormente rigorose che si sono concretizzate nella Direttiva 2018/1808 (di modifica della direttiva sui media audiovisivi ⁷²) e nel Regolamento Ue 2021/780 relativo al contrasto della diffusione dei contenuti terroristici *on line*.

In particolare il *Digital Services Act* è stato adottato con l'intento di approntare un sistema di misure volte alla protezione dei diritti fondamentali degli utenti creando un ambiente digitale competitivo e trasparente (art. 1) con l'intento di compiere quel fondamentale passaggio, oramai ineludibile, dalla centralità del mercato unico digitale alla costruzione di una solida democrazia digitale, contrastandone l'opacità (algoritmica e normativa). Le

⁷⁰ 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 Package e il codice di buone pratiche sulla disinforma-*

zione, in *Nomos. Le Attualità nel Diritto*, n. 2, 2022.

⁷¹ cfr. I ANRÒ *Online hate speech: la prospettiva dell'UE tra regolamentazione della condotta dei prestatori di servizio intermediari e ricorso al diritto penale*, in *Osservatorio sulle fonti*, n. 1, 2023.

⁷² Che impegna gli Stati membri ad « assicurare che i servizi dei media audiovisivi erogati dai fornitori di servizi di media soggetti alla loro giurisdizione non contengano: a) istigazione alla violenza o all'odio ... b) alcuna pubblica provocazione a commettere reati di terrorismo ... ».

aspirazioni perseguite attraverso l'adozione del *Digital Services Act* ed il legame sussistente fra tale normativa e gli obiettivi di lotta all'alterazione democratica *on line* si rendono evidenti leggendo la risoluzione del Parlamento europeo recante raccomandazioni alla commissione sull'atto sui servizi digitali e le questioni sollevate in materia di diritti fondamentali ⁷³. In tale raccomandazione viene espressamente posto in evidenza che « la disinformazione e l'incitamento all'odio online si sono sempre più diffusi negli ultimi anni a causa di persone soggetti perturbatori che utilizzano le piattaforme online per aumentare la polarizzazione, che a sua volta è sfruttata a fini politici » (paragrafo F). Il Parlamento europeo ha evidenziato che « finora l'approccio politico volto a contrastare i contenuti illegali online nell'Unione europea si è concentrato principalmente sulla cooperazione volontaria e su rimozioni autorizzate da provvedimenti giudiziari, ma che è un numero crescente di Stati membri sta adottando ulteriori normative a livello nazionale ». Le normative interne, quella tedesca e francese *in primis*, sembrano dunque aver ispirato in parte un'azione regolatoria europea orientata ad un maggior rigore e all'adozione nuovamente di strumenti di *hard law*. Tale intento ambizioso è centrato solo in parte. Difatti, nel perseguire tali obiettivi il Regolamento 1065/2022 impone una serie di previsioni (differenziate a seconda che i destinatari siano aziende molto grandi, medie o piccole) che oltre a definire alcune procedure di notifica e rimozione di contenuti illeciti impongono alle piattaforme digitali delle regole in tema di trasparenza algoritmica ⁷⁴. Tuttavia la novella normativa ha ritenuto di mantenere fermi i principi chiave contenuti nella Direttiva *e-commerce in primis* l'irresponsabilità degli intermediari digitali ⁷⁵.

Con riguardo specificatamente alle c.d. le VLOPs (*Very Large Online Platforms* ovvero piattaforme e i motori di ricerca « che hanno un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a 45 milioni » ⁷⁶), il *Digital Services Act* stabilisce alcune specifiche previsioni che fanno leva sul concetto di necessità di « previsione del rischio » in considerazione dell'enorme bacino di utenza che le stesse possono raggiungere ⁷⁷.

⁷³ 2020/2022 INL.

⁷⁴ Cfr. art. 27 REGOLAMENTO (UE) 2022/2065.

⁷⁵ Ad esempio l'art. 7 del *Digital services Act* (rubricato « Indagini volontarie promosse di propria iniziativa e rispetto degli obblighi normativi ») pone in chiaro che « I prestatori di servizi intermediari non sono considerati inammissibili all'esenzione dalla responsabilità prevista agli articoli 4, 5 e 6 per il solo fatto di svolgere, in buona fede e in modo diligente, indagini volontarie di

propria iniziativa o di adottare altre misure volte a individuare, identificare e rimuovere contenuti illegali o a disabilitare l'accesso agli stessi, o di adottare le misure necessarie per conformarsi alle prescrizioni del diritto dell'Unione e del diritto nazionale conforme al diritto dell'Unione, comprese le prescrizioni stabilite nel presente regolamento ».

⁷⁶ Art. 33 Regolamento (UE) 2022/2065.

⁷⁷ Agli artt. 34 e 35 il Regolamento prevede difatti che le VLOPs siano tenute

A fronte dei rischi individuati e delle valutazioni svolte, i fornitori delle VLOPs dovranno successivamente adottare « misure di attenuazione ragionevoli, proporzionate ed efficaci, adattate ai rischi sistemici specifici » prestando particolare attenzione agli effetti di tali misure sui diritti fondamentali. La supervisione di tale attività reattiva di attenuazione dei rischi è accordata al Comitato europeo per i servizi digitali, istituito nel medesimo regolamento ⁷⁸ e composta da tutti i coordinatori dei Servizi digitali nominati in ciascuno stato con compiti di sorveglianza territoriale ⁷⁹ ed è inoltre previsto, a chiusura dell'art. 35, che « La Commissione, in cooperazione con i coordinatori dei servizi digitali, può emanare orientamenti sull'applicazione del para-

ad individuare, analizzare e valutare con diligenza gli eventuali rischi sistemici che possono derivare «dalla progettazione o dal funzionamento del loro servizio e dei suoi relativi sistemi, compresi i sistemi algoritmici, o dall'uso dei loro servizi», mediante una valutazione di rischio annuale, da rinnovarsi anche nel caso in cui siano introdotte nuove funzionalità che possono avere un impatto critico sui rischi individuati. Il regolamento individua quattro aree soggette a rischi sistemico in relazione a cui è necessario che le aziende digitali molto grandi effettuino la stima dei rischi prodotti dalla loro attività. Tali aree sono: a) la diffusione di contenuti illegali tramite i loro servizi; b) eventuali effetti negativi, attuali o prevedibili, per l'esercizio dei diritti fondamentali (in particolare i diritti fondamentali alla dignità umana sancito nell'articolo 1 della Carta, al rispetto della vita privata e familiare sancito nell'articolo 7 della Carta, alla tutela dei dati personali sancito nell'articolo 8 della Carta, alla libertà di espressione e di informazione, inclusi la libertà e il pluralismo dei media, sanciti nell'articolo 11 della Carta, e alla non discriminazione sancito nell'articolo 21 della Carta, al rispetto dei diritti del minore sancito nell'articolo 24 della Carta, così come all'elevata tutela dei consumatori, sancito nell'articolo 38 della Carta); c) eventuali effetti negativi, attuali o prevedibili, sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica; d) qualsiasi effetto negativo, attuale o prevedibile, in relazione alla violenza di genere, alla protezione della salute pubblica e dei minori e alle gravi conseguenze negative per il benessere fisico e mentale della persona.

⁷⁸ Considerando 131 Regolamento (UE) 2022/2065: « Al fine di garantire un'applicazione coerente del presente regolamento è necessario istituire un gruppo consultivo indipendente a livello dell'Unione, un comi-

tato europeo per i servizi digitali, che dovrebbe sostenere la Commissione e contribuire a coordinare le azioni dei coordinatori dei servizi digitali. Il comitato dovrebbe essere composto dai coordinatori dei servizi digitali, ove siano stati nominati, fatta salva la possibilità per questi ultimi di invitare alle riunioni del comitato • nominare delegati *ad hoc* di altre autorità competenti incaricate di compiti specifici a norma del presente regolamento, ove ciò sia richiesto dalla loro ripartizione nazionale dei compiti e delle competenze. In caso di più partecipanti da uno Stato membro, il diritto di voto dovrebbe rimanere limitato a un rappresentante per Stato membro ».

⁷⁹ Considerando 110 Regolamento (UE) 2022/2065: « In considerazione del carattere transfrontaliero dei servizi in causa e della serie orizzontale di obblighi stabiliti dal presente regolamento, una sola autorità incaricata di vigilare sull'applicazione del presente regolamento e, se necessario, della sua esecuzione dovrebbe essere designata come coordinatore dei servizi digitali in ciascuno Stato membro. Qualora più di un'autorità competente sia incaricata di vigilare sull'applicazione e di eseguire il presente regolamento, solo un'autorità in tale Stato membro dovrebbe essere designata come coordinatore dei servizi digitali. Il coordinatore dei servizi digitali dovrebbe fungere da punto di contatto unico con riguardo a tutte le questioni relative all'applicazione del presente regolamento per la Commissione, il comitato, i coordinatori dei servizi digitali degli altri Stati membri nonché per le altre autorità competenti dello Stato membro in questione. Qualora in un determinato Stato membro diverse autorità competenti siano incaricate di compiti a norma del presente regolamento, il coordinatore dei servizi digitali dovrebbe in particolare coordinarsi e cooperare con tali autorità in conformità del diritto nazionale che stabilisce i

grafo 1 in relazione a rischi concreti, con l'obiettivo specifico di presentare le migliori pratiche e raccomandare eventuali misure, tenendo debitamente conto delle possibili conseguenze di tali misure sui diritti fondamentali di tutte le parti interessate sanciti dalla Carta. Nell'elaborazione di tali orientamenti la Commissione organizza consultazioni pubbliche ».

I VLOPs dovranno inoltre sottoporsi, « a proprie spese e almeno una volta all'anno, a revisioni indipendenti volte a valutare la conformità agli obblighi normativi e agli impegni assunti a norma dei codici di condotta e dei protocolli di crisi » (art. 37).

Al successivo art. 45 del *Digital Services Act* si fa riferimento poi alla volontà da parte della Commissione e del comitato di incoraggiare ed agevolare « l'elaborazione di codici di condotta volontari a livello di Unione per contribuire alla corretta applicazione del presente regolamento, tenendo conto in particolare delle sfide specifiche connesse alla lotta ai diversi tipi di contenuti illegali e ai rischi sistemici, conformemente al diritto dell'Unione, in particolare in materia di concorrenza e protezione dei dati personali ». La normativa aggiunge subito dopo che « Qualora emerga un rischio sistemico significativo ai sensi dell'articolo 34, paragrafo 1, che interessa diverse piattaforme online di dimensioni molto grandi o diversi motori di ricerca online di dimensioni molto grandi, la Commissione può invitare i fornitori di piattaforme *online* di dimensioni molto grandi interessati o i fornitori di motori di ricerca *online* di dimensioni molto grandi interessati e altri fornitori di piattaforme online di dimensioni molto grandi, di motori di ricerca online di dimensioni molto grandi, di piattaforme *online* e di altri di servizi intermediari, se opportuno, nonché le pertinenti autorità competenti, le organizzazioni della società civile e altre parti interessate, a partecipare all'elaborazione dei codici di condotta, anche stabilendo impegni ad adottare misure specifiche di attenuazione dei rischi nonché un quadro di comunicazione periodica sulle misure adottate e sui relativi risultati » (art. 34 c. 2).

Considerando tale impianto architettonico della più recente normativa europea sembra dunque che in ambito unionale si sia

rispettivi compiti e fatta salva la valutazione indipendente delle altre autorità competenti. Pur non comportando alcuna superiorità gerarchica rispetto ad altre autorità competenti nell'esercizio dei rispettivi compiti, il coordinatore dei servizi digitali dovrebbe assicurare l'effettivo coinvolgimento di tutte le autorità competenti pertinenti e dovrebbe riferire tempestivamente la loro valutazione nell'ambito della cooperazione a fini di vigilanza e di applicazione a livello

dell'Unione. Inoltre, in aggiunta ai meccanismi specifici previsti dal presente regolamento per quanto riguarda la cooperazione a livello dell'Unione, gli Stati membri dovrebbero altresì assicurare la cooperazione tra il coordinatore dei servizi digitali e le altre autorità competenti designate a livello nazionale, ove opportuno, mediante il ricorso a strumenti adeguati, quali la messa in comune delle risorse, *task force* congiunte, indagini congiunte e meccanismi di assistenza reciproca ».

tentato da una parte di imprimere una spinta significativa alla disciplina del diritto digitale (importante, in tal senso, è anche la scelta di passare dallo strumento della direttiva a quello del regolamento), cercando di superare l'iniziale retaggio liberista; tuttavia, il prodotto normativo realizzato non sembra assumere i contorni di una disciplina del tutto rigorosa, manifestando in tal senso sia tutte le difficoltà legate alla normazione di un ambito di per sé sfuggente, sia collegandosi a quella che oramai può considerarsi una pratica consolidata nella normazione europea in ambito digitale quale l'ampio uso dello strumento della coregolazione e della spinta alla collaborazione e alla *partnership* fra dimensione pubblica e soggetti economici privati. L'impianto del *Digital Services Act* in alcuni passaggi sembra in effetti essere più orientato a definire una dimensione procedurale dei rapporti che connotano tale *partnership* piuttosto che chiarire (assumendosene la responsabilità) i contenuti sostanziali delle regole da applicare finendo per delegare ancora una volta all'autoregolazione privata, o al massimo allo strumento della coregolazione, la selezione di importanti contenuti normativi in ambiti che lo stesso Regolamento 2022/2065 definisce "sistemici" e dunque di innegabile importanza ⁸⁰.

4. IL LIBERISMO NEL CONTESTO USA: DALLA TUTELA DELLA *CONTENT MODERATION* AI PROBLEMI COLLEGATI AL *RECOMMENDATION ALGORITHM* E ALL'"AFFAIRE TIKTOK".

4.1. *I emendamento e strumenti di comunicazione di massa.* _____

Nell'esperienza statunitense 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 ⁸¹; ciò non ha condotto, tuttavia, come ben noto, ad una modulazione in termini restrittivi dell'interpretazione del I emendamento in ambito digitale.

Il principio per il quale le differenze nelle caratteristiche dei mezzi di informazione giustificano una differenziazione negli *standards* relativi all'applicazione del I Emendamento è stato enunciato e ribadito dalla Corte suprema in diverse occasioni con riguardo, specificatamente, al mezzo radiotelevisivo: il *leading case* è certamente rappresentato dalla decisione *Red Lion Broad.*

⁸⁰ Cfr. sul punto M. BETZU, *I signori del digitale*, cit., 104 ss.; G. DE MINICO, *Fundamental Rights, European Digital Regulation and algorithmic challenge*, in *Media Law*, n. 1, 2021, 9 ss.

⁸¹ *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).

Co. v. FCC ⁸², del 1969, nella quale la Corte suprema ha valutato la legittimità della c.d. *Fairness Doctrine*, una *policy* della *Federal Communications Commission* (FCC) — fondata sul *Radio Act* del 1927 e sulla sez. 307 (licenze) del Titolo 47 (radiodiffusione) dello *US Code* —, 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 tramettere all'impegno da parte dei titolari delle relative licenze a fornire un servizio di informazione pubblica orientato al pluralismo e alla correttezza ⁸³. 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 ⁸⁴.

La giurisprudenza della Corte suprema in relazione alla limitazione della libertà di espressione in ambito radiotelevisivo arriva peraltro, in alcune limitate circostanze, a pronunciarsi anche sugli stretti contenuti veicolati tramite tali mezzi; ciò avviene ad esempio quando, nel 1978, nella decisione *FCC v. Pacifica Foundation* ⁸⁵, la Corte suprema conferma il potere della FCC di regolare, in circostanze limitate (stabilendo orari e condizioni di trasmissione), programmi che pur non "osceni" fossero qualificabili come "indecenti". A fianco della motivazione concernente la "scarsità" del bene, nella decisione *Pacifica* uno dei perni in relazione al quale il 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, non si estende tuttavia alla carta stampata la quale, anche dopo la decisione del 1969, continua a godere nelle sentenze della Corte suprema federale di un'ampia libertà di espressione. La conferma emblematica di tale differenza di approccio si riscontra nell'adozione, nel 1974, della decisione *Miami Herald publishing v. Tornillo* ⁸⁶ ove la Corte suprema, in tema di diritto di replica, in una vicenda dai tratti estremamente simili a quelli accaduti nel caso *Red Lion*, senza peraltro citare mai

⁸² *Red Lion Broad. Co. v. FCC*, 395 U.S. 367 (1969).

⁸³ Sulla *Fairness doctrine* cfr. K.A. RUANE, *Fairness Doctrine, History and Constitutional Issues*, CRS Report, July 13, 2011.

⁸⁴ *Turner Broadcasting System v. FCC*, 512 US 622 (1994).

⁸⁵ *FCC v. Pacifica Foundation*, 438 U.S. 726 (1978).

⁸⁶ *Miami Herald publishing v. Tornillo*, 418 US 241 (1974).

quest'ultima decisione ⁸⁷, sancisce che imporre alla carta stampata il diritto di replica significa obbligare la stampa a dei contenuti e dunque minarne il carattere di libertà.

Così come per la carta stampata, nella giurisprudenza concernente l'applicabilità di possibili approcci restrittivi alla libertà di espressione *on line*, a partire dalla nota decisione caso *Reno v. ACLU* ⁸⁸, del 1997, i precedenti giurisprudenziali definiti per l'emittenza radiotelevisiva, pur presi in considerazione, non vengono considerati applicabili operando la Corte, in questo caso, un netto *distinguishing*. Difatti, nella decisione *Reno*, che riguardava l'incostituzionalità del *Communication Decency Act* del 1996 (un atto normativo adottato dal Congresso nel 1996 a protezione dei minori dalla diffusione di materiale osceno o pornografico) 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 dell'utente in relazione alla quale esso non poteva qualificarsi passivo ⁸⁹. Inoltre la decisione di maggioranza metteva in evidenza che Internet non fosse caratterizzato da una intrinseca limitatezza delle vie di accesso e che, dunque, non fosse necessario, nell'arena digitale, proteggere una risorsa espressiva in ragione della sua scarsità ⁹⁰.

4.2. *La sez. 230 del CDA: la content moderation e le esigenze del liberismo digitale.*

La decisione *Reno*, adottata nella seconda metà degli anni novanta, riflette il clima di ampia fiducia nelle prospettive cui internet apriva che richiedeva un atteggiamento tendenzialmente libertario nella normazione del mezzo. La decisione è stata criticata, sin dalla sua adozione, da parte di chi, già da allora, percepiva la sovrastima da parte della suprema Corte delle capacità attive di autoprotezione degli utenti digitali nella loro possibilità di scelta fra contenuti desiderati ed indesiderati ⁹¹. Se tali valutazioni erano valide all'epoca, sembrano esserlo tanto più ad oggi ove le evidenze attuali concernenti le problematiche della

⁸⁷ 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.

⁸⁸ *Reno v. American Civil Liberties Union*, 521 US 844 (1997).

⁸⁹ « 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*.

⁹⁰ « 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*.

⁹¹ D. K. DJAVAHERIAN, *Reno v. ACLU*, in *Berkeley Technology Law Journal*, 13, 1998, 371 ss. spec. 380.

trasparenza algoritmica, del *microtargeting* ecc. sottolineano ancora di più la fragilità dell'impostazione iniziale.

La decisione confermava, da parte del supremo giudice federale, l'approccio libertario assunto solo l'anno precedente anche 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 ⁹².

La normativa congressuale adottata nel 1996 seguiva alcune decisioni in tema di responsabilità del *provider*, adottate dai giudici ordinari nel quinquennio precedente che avevano evidenziato la possibilità di optare sul tema per scelte molto diverse fra loro. Nella decisione *Cubby v. Compuserve* ⁹³ la Corte distrettuale per il *Southern District* dello Stato di New York aveva equiparato una piattaforma ospitante una newsletter ad un edicolante, applicandone il relativo regime di responsabilità; diversamente, qualche anno dopo, nella decisione *Stratton Oakmont v. Prodigy Service Company* ⁹⁴, la Corte suprema di New York addivenne a conclusioni estremamente diverse condannando il gestore di una piattaforma (*Prodigy*) che ospitava una bacheca virtuale ritenendolo responsabile per i contenuti diffamatori pubblicati da terzi in relazione all'attività di moderazione che la piattaforma svolgeva in conformità con i termini d'uso. Difatti, proprio considerando tale attività di *content moderation* la Corte ritenne che lo *standard* applicato in *Compuserve* non fosse neutrale e concluse che, nel caso in discussione, il gestore *on line* potesse essere paragonato ad un editore. Tale impostazione, tuttavia, poteva finire per spingere i gestori delle piattaforme a non praticare alcuna forma di moderazione dei contenuti o, al contrario, condurre a forme di censura *on line* esasperate: in relazione a tale rischio il Congresso si risolve dunque all'adozione della nota normativa del CDA esonerando i *provider* da ogni responsabilità (salvo alcune limitate eccezioni ⁹⁵) 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. In *Zeran v. America Online* ⁹⁶ la Corte d'appello per il Quarto circuito, nel 1997, sancisce difatti l'ampiezza della portata della sez. 230

⁹² Sul tema cfr. ampiamente BASSINI, *Internet e libertà di espressione*, cit.

⁹³ *Cubby v. Compuserve*, 776 F. Supp. 135 (S.D.N.Y. 1991).

⁹⁴ *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 23 Media L. Rep. 1794 (N.Y. Sup. Ct. 1995).

⁹⁵ 47 USC sez. 230 (e)(5).

⁹⁶ 129 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

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).

La vasta estensione dei caratteri dell'immunità garantita dalla sezione 230 viene 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 autonomo⁹⁷ o nei quali il terzo abbia commesso un evidente illecito penale⁹⁸.

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 comunicazioni, 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. Su 135 (S.D.N.Y. 1991) e *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

⁹⁷ *Blumenthal v. Drudge and America Online, Inc.*, 992 F. Su 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.

⁹⁸ 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. A Oct. 14, 1998), la madre di un

4.3. *La privatizzazione della censura e la public forum theory.*

Come già rilevato, lo scorrere del tempo ha tuttavia manifestato le fragilità insite in tale impostazione adottata in una fase storica nella quale solo in pochi immaginavano che nel giro di qualche decennio le grandi compagnie *tech* sarebbero diventate compartecipi delle scelte afferenti alle grandi questioni concernenti la struttura più intima dell'architettura di uno Stato (Moneta, Giurisdizione, Dibattito pubblico e flussi elettorali) ⁹⁹.

In un contesto normativo come quello statunitense, l'applicazione alla rete delle garanzie del I emendamento sommata alla deresponsabilizzazione del *provider* hanno fatto sì che si sviluppassero modalità di controllo delle forme espressive *on line* esclusivamente fondate sui meccanismi di moderazione dei contenuti affidate alle compagnie *tech* con lo sviluppo, dunque, di una forma significativa di privatizzazione della censura; una "*collateral censorship*" suscettibile di assumere caratteri del tutto "arbitrari" o, anche peggio, basati su bilanciamenti di interessi posti in essere e risolti direttamente dalle *corporations* ¹⁰⁰. A fronte, dunque, 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 consentendo, peraltro, alle aziende di modulare tale diffusione delle opinioni sulla base delle convenienze aziendali ¹⁰¹. Le garanzie costituzionali poste dal *Bill of Rights* non sono in grado di impedirlo: la

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 stabi-

lire che un *provider* può godere dell'immunità sia in quanto editore, sia in quanto distributore.

⁹⁹ A. VANZONI, *Cyber-costituzionalismo: la società digitale tra silicolizzazione, capitalismo delle piattaforme e reazioni costituzionali*, cit.

¹⁰⁰ Cfr. sul tema M. MONTI, *Privatizzazione della censura e Internet platforms: la libertà d'espressione e i nuovi censori dell'agorà digitale*, in *Rivista italiana di informatica e Diritto*, n. 1, 2019, 35 ss.

¹⁰¹ 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, XVIII.

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* e i canali del *web* ¹⁰².

In realtà, sulla base di una particolare ricostruzione giurisprudenziale, una parte minoritaria della dottrina statunitense ha tentato 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 ragione di tale ricostruzione, sono tenute a rispettare a propria volta i limiti posti dal primo emendamento ¹⁰³. La teoria in oggetto è stata sviluppata nell'ordinamento americano a seguito della sentenza *Marsh v. Alabama* ¹⁰⁴, del 1946, un caso che 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 » ¹⁰⁵. In una successiva decisione, *Hudgens v. NLRB* ¹⁰⁶, 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

¹⁰² 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.

¹⁰³ Riferiscono di tale teoria M. MONTI, *Privatizzazione della censura e Internet platforms: la libertà d'espressione e i nuovi censori dell'agorà digitale*, p. 42 ss.; M.R. ALLEGRI, *Oltre la par condicio*, cit. 65 ss.; CONIBERTI, *Potere e libertà nella rete*, in *Media Laws*, n. 3, 2018.

¹⁰⁴ *Marsh v. Alabama*, 326 U.S. 501 (1946).

¹⁰⁵ *Marsh v. Alabama*, 326 U.S. at 501 (1946).

¹⁰⁶ *Hudgens v. NLRB*, 424 U.S. 507 (1976).

municipalità e non devono esistere alternative altrettanto efficaci per la diffusione delle idee censurate dallo stesso ¹⁰⁷.

Considerando un possibile un parallelismo fra urbanistica e rete Internet è stato ipotizzato dunque che alle piattaforme digitali sia applicabile la *State Action Doctrine* e che pertanto le stesse possano essere considerate limitate dal I emendamento al pari di un'autorità statale.

Nonostante alcune decisioni in senso contrario nella giurisprudenza ordinaria ¹⁰⁸, 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* ¹⁰⁹, 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 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*» ¹¹⁰.

Nondimeno, una ancor più recente decisione ha inferito una battuta d'arresto a tale ricostruzione: nella decisione *Manhattan*

¹⁰⁷ Tale specificazione è collegata ad un'altra decisione 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.

¹⁰⁸ *Langdon v. Google, Inc.*, 474 F. Su 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).

¹⁰⁹ *Packingham v. North Carolina*, 582 U.S. (2017).

¹¹⁰ 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, 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».

Community Access Corp v. Halleck ¹¹¹, la Corte suprema, nelle parole del giudice Kavanaugh, 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 in termini restrittivi le circostanze in relazione alle quali un'azienda privata può essere considerata come vincolata agli stessi limiti dell'autorità pubblica ¹¹². 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* » ¹¹³) e ciò conduce, dunque, almeno per il momento, a dover considerare ancora di minoranza tale teoria giurisprudenziale.

Collegato alla teoria dello spazio digitale quale foro pubblico è 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 Presidente degli Stati Uniti di bloccare alcuni utenti sul suo *account* ¹¹⁴ 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 *social account* 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 ¹¹⁵. Non si tratta tuttavia di una giurisprudenza

¹¹¹ *Manhattan Community Access Corp v. Halleck*, 587 U.S. (2019). La decisione è commentata da G. L. FISHER, *Lights, Camera, State Action: Manhattan Community Access Corp. V. Halleck*, in *Cardozo Law Review De Novo*, 2020, 165 ss.

¹¹² « *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.

¹¹³ 587 U.S. (2019), part. B II.

¹¹⁴ *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.

¹¹⁵ *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): ribal-

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.

4.4. *La responsabilità del provider e i sistemi di “recommendation algorithm”. Le più recenti ipotesi di superamento dell’interpretazione estensiva della sez. 230.*

Una 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 federale 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 dunque predisposto un apposito *Executive Order* nel quale, ponendo in evidenza il fatto che i *social media* non possono più, ad oggi, 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 ¹¹⁶, 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 ¹¹⁷. Il *Center of Democracy and Technology* ha inoltre immediatamente presentato un ricorso

tando 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 *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, 1696.

¹¹⁶ Clause 230(c)(2).

¹¹⁷ 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.

avverso tale atto governativo ¹¹⁸. 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 ¹¹⁹, l'*Executive Order* è stato prontamente ritirato dal successore alla casa Bianca, Joe Biden, il 14 maggio 2021 ¹²⁰.

Se in parte, l'ordine esecutivo di Trump è certamente collegato alle vicende personali del Presidente e alle sue controversie con alcuni *social*, tuttavia il tema in esso affrontato affonda le sue radici in un dibattito più risalente soprattutto in considerazione di alcune vicende giurisprudenziali che pongono in evidenza la problematica della neutralità del *provider* alla luce dell'evoluzione tecnologica nello scorrere degli anni.

Leading case in tale ambito è il caso *Force v. Facebook, Inc.* ¹²¹, una decisione del Secondo Circuito in cui la Corte, richiamandosi e ribadendo la nota differenziazione fra *content* e *service provider* ha stabilito che la sez. 230 garantisce un *social network* dai ricorsi per risarcimento civile in relazione a vicende che riguardano il sostegno materiale al terrorismo. Ciò veniva deciso nonostante l'evoluzione tecnologica attuale in relazione alla quale i ricorrenti 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 ¹²². 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'at-

¹¹⁸ *Center for Democracy and Technology v. Trump*, US District Court for the District of Columbia, case n. 20-1456, 6/02/2020.

¹¹⁹ Sul punto cfr. ancora G.F. FERRARI, *L'executive order sulla prevenzione della censura online: quali effetti sull'autonomia dei social network?*, cit.

¹²⁰ *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/>.

¹²¹ *Force v. Facebook, Inc.*, 934 F.3d 53 (2d Cir. 2019).

¹²² « 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).

tività algoritmica, vada a “potenziare” un pensiero diffondendolo e collegandolo ad una rete di sostenitori e dunque creando connessioni fra utenti delle quali è responsabile ¹²³. La Corte non ha tuttavia condiviso l’opinione del giudice Katzman ritenendo che la neutralità dell’algoritmo nelle sue decisioni di creazione dei rapporti sul *web* ne sani gli effetti.

Il tema della necessità di escludere la decisione algoritmica (determinata, in ultima analisi, dalla programmazione del *provider*) dalle garanzie della sez. 230 è ripreso nello *statement* del giudice Clarence Thomas nel diniego al *Writ of certiorari* al caso *Malwarebytes, Inc. v. Enigma Software Group Usa LLC* ¹²⁴, una vicenda giudiziaria nella quale figuravano come controparti due aziende produttrici di *software* per l’esclusione di materiale indesiderato: la *Malwarebytes* aveva perfezionato il suo programma per impedire che ai propri utenti pervenissero prodotti della società concorrente *Enigma* qualificandoli, nella definizione algoritmica, come prodotti indesiderati. Pur condividendo il diniego del *certiorari* disposto dalla Corte suprema, il giudice Thomas ha tratto spunto da tale vicenda per evidenziare come la portata della sez. 230 necessiti di essere rivista ed ha richiamato, nella sua argomentazione sul punto, anche l’opinione in dissenso del giudice Katzman nel caso *Force v. Facebook*.

Il tema della responsabilità del *provider* in relazione alla decisione algoritmica, oggetto di diverse decisioni delle Corti federali di distretto o di circuito ¹²⁵, 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 avve-

¹²³ 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).

¹²⁴ *Malwarebytes, Inc. v. Enigma Software Group Usa LLC*, 592 U. S. ____ (2020).

¹²⁵ 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 di 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.

nuto giacché nella decisione *Gonzales v. Google*¹²⁶, 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 tuttavia riferimento ad un altro caso congiunto *Twitter, Inc. v. Taamneh*¹²⁷ 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 rete¹²⁸. Il tribunale distrettuale si è pronunciato a favore di *Google* facendo perno sulla sez. 230 e tale decisione è stata confermata dal Nono circuito; tuttavia, la Corte suprema ha concesso il *certiorari* animando il dibattito circa l'idea per la quale le grandi aziende digitali non possano più continuare ad essere considerate figure neutrali ai discorsi che circolano in rete 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 algoritmica¹²⁹.

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 non è escluso che, in effetti, a seguito di una pronuncia giurisprudenziale

¹²⁶ 598 U. S. ____ (2023). Docket No. 21-1333; May 18, 2023.

¹²⁷ 598 U. S. ____ (2023). No. 21-1496. Argued February 22, 2023 — Decided May 18, 2023.

¹²⁸ 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).

¹²⁹ 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.

importante, il Congresso senta la necessità di intervenire esso stesso innovando il regime di responsabilità del *provider* ¹³⁰.

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 caso riguardava la morte di un cittadino giordano, Nawras Allassaf, nel 2017 durante un attacco terroristico ad Istanbul. I parenti statunitensi del ragazzo avevano citato in giudizio Twitter, Google e Facebook sostenendo che le dette compagnie digitali fossero in parte responsabili dell'accaduto. In questa vicenda processuale il parametro di valutazione non era tuttavia la sez. 230 ma l'*Anti-Terrorism Act* ¹³¹. 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) ¹³². Il giudice Thomas ha peraltro evidenziato come in molti altri casi qualcuno può sfruttare a fini "terroristici" una tecnologia, ad

¹³⁰ 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 Transparency Act*, S. 1896; il *Protecting Americans from Dangerous Algorithmic Act*, H.R. 2154).

¹³¹ 18 USC § 2333.

¹³² « 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 pas-

sive aid and constitute active, substantial assistance. We disagree. By plaintiffs' own telling, their claim is based on defendants' "provision of the infrastructure which provides material support to ISIS." A 53. Viewed properly, defendants' "recommendation" algorithms are merely part of that infrastructure. All the content on their platforms is filtered through these algorithms, which allegedly sort the content by information and inputs provided by users and found in the content itself. As presented here, the algorithms appear agnostic as to the nature of the content, matching any content (including ISIS' content) with any user who is more likely to view that content. The fact that these algorithms matched some ISIS content with some users thus does not convert defendants' passive assistance into active abetting. Once the platform and sorting-

esempio al rete telefonica, e questo non rende le aziende che forniscono questi servizi responsabili civilmente di tali azioni ¹³³.

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

4.5. *La possibile vera crisi del modello liberale statunitense: la vicenda Tik Tok ovvero ... quando nel libero mercato gli Usa perdono la leadership.*

L'approccio liberale statunitense alla dimensione digitale sembra vivere recentemente un'ulteriore ragione di crisi in relazione alle tensioni innescate dalla estrema diffusione sul 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 ¹³⁴ in base alla quale le autorità statali cinesi possono richiedere ai propri cittadini e alle aziende di fornire dati rilevanti per il loro lavoro di *intelligence*.

La questione del pericolo posto alla sicurezza nazionale a causa

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.

¹³³ « 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.

¹³⁴ 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/>.

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 ¹³⁵. 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" ¹³⁶. 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 ¹³⁷ 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 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") ¹³⁸. Il 6 agosto 2020, il Presidente ha infine identificato *TikTok* come un'azienda tecnologica che rappresenta un rischio per la sicurezza nazionale ¹³⁹ 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 ed 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

¹³⁵ 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 reperibile all'url R45618 (congress.gov).

¹³⁶ 50 USC § 1701(a).

¹³⁷ Executive Order n. 13873, *Securing the Information and Communications Technology and Services Supply Chain*, 84 Fed. Reg. 22689 (15 maggio 2019).

¹³⁸ *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).

¹³⁹ 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*.

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* ¹⁴⁰ 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* ¹⁴¹, il Segretario al Commercio statunitense ha pubblicato un elenco di transazioni vietate riguardanti *ByteDance* ¹⁴².

Le restrizioni dette nei confronti della piattaforma *TikTok* sono state impugnate in sede giudiziaria attraverso due ricorsi: il primo presentato dalla stessa azienda colpita dal provvedimento ¹⁴³ ed il secondo proposto da alcuni utenti della piattaforma ¹⁴⁴. 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 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

¹⁴⁰ *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.*

¹⁴¹ 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").

¹⁴² 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").

¹⁴³ La decisione è stata Assunta dalla United States District Court, District of Columbia. 507 F.Su3d 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.

¹⁴⁴ La sentenza è stata adottata dalla United States District Court, E.D. Pennsylvania. 498 F.Su3d 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.

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 e acquisizioni che potrebbero comportare che una qualunque entità straniera finisca per assumere il controllo di un'azienda statunitense. CFIUS è dunque competente a determinare la possibilità che sussistano dei rischi per la sicurezza nazionale derivanti da una transizione economica e aziendale e può conseguentemente imporre misure appropriate e raccomandare al Presidente il divieto o la sospensione della detta transazione. Il Presidente ha l'autorità ultima di vietare o sospendere una transazione segnalata dalla Commissione.

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 ¹⁴⁵ (*Divestment Order*) imponendo a *ByteDance* di dismettere qualunque investimento sul territorio statunitense e cedere qualunque dato ottenuto attraverso *TikTok* o *musical.ly* ¹⁴⁶.

¹⁴⁵ 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.

¹⁴⁶ « *ByteDance, its subsidiaries, affiliates, and Chinese shareholders, shall divest all interests and rights in: (i) any tan-*

gible 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, Byte-

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 ¹⁴⁷ fondata sull'istituzione da parte dell'azienda cinese di una apposita filiale statunitense, una *US Data Security* (USDS) governato da un Consiglio di amministrazione indipendente, supervisionato da CFIUS al quale è demandata peraltro la possibilità di definire i 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 regioni, inclusa la Cina. Con l'obiettivo di garantire il trattamento dei dati dei cittadini statunitensi l'azienda cinese ha deciso inoltre 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 varcano il confine e seguirà revisioni più dettagliate se uno qualsiasi dei controlli dovesse rilevare flussi di dati non conformi.

Mentre sono in corso le operazioni di negoziazione con l'azienda, a giugno del 2021 l'amministrazione Biden ha adottato un ulteriore *Executive Order* ¹⁴⁸ intitolato "*Protecting Americans' Sensitive Data From Foreign Adversaries*" con il quale ha annul-

Dance shall certify in 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».

¹⁴⁷ Cfr. la pagina dell'azienda dedicata alla proposta consultabile all'URL <https://newsroom.tiktok.com/en-us/our-approach-to-keeping-us-data-secure>.

¹⁴⁸ 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.

lato 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 dell'era Trump, incluso quello adottato nel 2019 (*Securing the Information and Communications Technology and Services Supply*).

Considerando che alcune delle risposte alle problematiche postesi in relazione alla vicenda *TikTok* sono state impedita a causa di alcune eccezioni previste nelle normative preposte alla sicurezza nazionale, alcuni membri del Congresso hanno avanzato delle proposte legislative attualmente in discussione finalizzate ad eliminare le dette eccezioni relative alle comunicazioni personali e ai materiali informativi.

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.

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 ¹⁴⁹, 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 ipotesi 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.

5. L'ECOSISTEMA DIGITALE, LA GLOBALIZZAZIONE E LA CRISI DELLA STRATEGIA LIBERISTA.

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

¹⁴⁹ Cfr. W. DUFFIELD, *TikTok Panic Threatens Speech*, reperibile all'URL <https://www.cato.org/blog/tiktok-panic-threatens-speech> (21 aprile 2023).

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 dalle 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 democratico) e di lì forse potrebbe spiccare il salto verso decisioni assunte anche dal 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 dei 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. Lycra*¹⁵⁰ 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

¹⁵⁰ *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. ●koniewski, *Yahoo! Inc. V. Lycra: The*

French Challenge to Free Expression on the Internet, in *American University International Law Review*, vol. 18, 2002, 295 ss.

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 sebbene il tema della manipolazione individuale attraverso la decisione algoritmica sia argomento di preoccupazione pressoché bipartisan.

Nel contesto europeo invece, meno restio all'intervento normativo (anche in relazione ad una concezione funzionalista della libertà di espressione), si assiste alla difficoltà del normare in un contesto tanto fluido come quello digitale e si evidenzia l'impossibilità pratica di esimersi dall'intraprendere soluzioni normative spurie a metà strada fra l'*hard* ed il *soft law* valorizzando la *partnership* pubblico/privato che domina il contesto digitale e che sembra dunque un concetto, allo stato attuale, irretrattabile.

In entrambi i contesti si evidenzia, come detto, la necessità di superare l'iniziale, forse oramai ingenuo, approccio liberista e prendere atto che anche nell'ecosistema digitale la teoria della mano invisibile può rivelarsi del tutto fallimentare.

Abstract

The digital environment is characterized by a complex relationship between public and private entities. The regulation of the digital environment must therefore address intricate and unique matters that relate to the safeguarding of fundamental freedoms, national security, and the safeguarding of the economic interests of the state. This paper examines these topics from both European and American perspectives, emphasizing the similarities and disparities between the two.