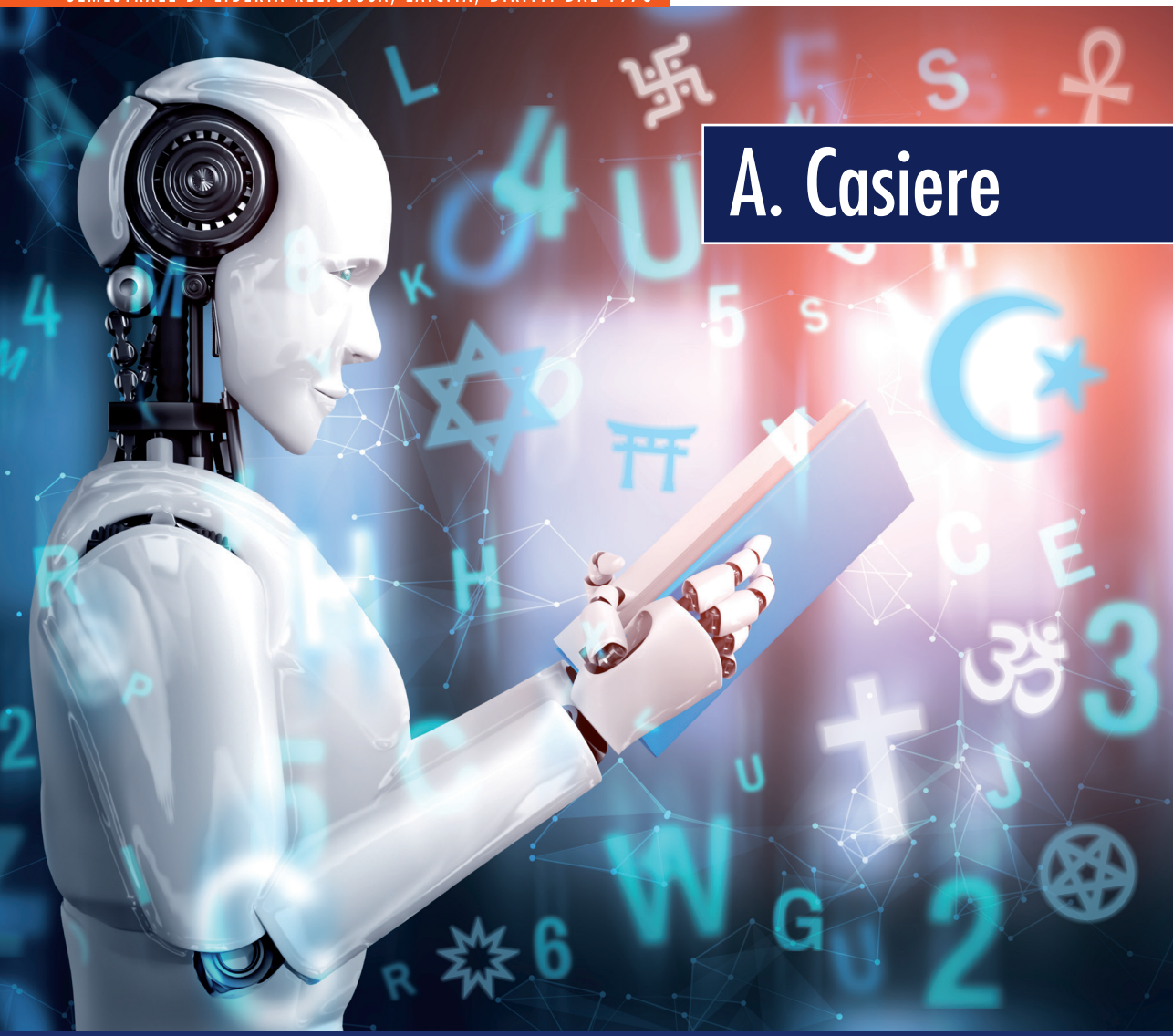
2024 NUMERO 68

Coscienza e Libertà

SEMESTRALE DI LIBERTÀ RELIGIOSA, LAICITÀ, DIRITTI DAL 1978



A. Casiere

Diritto, Religioni e Intelligenza artificiale: quali prospettive?

ISSN 0394-2732

A. Casiere - G. Cimbalo
M. Croce - A. Cupri
L. Fregoli - E. Lipilini
M.L. Lo Giacco - G. Mobilio
G. Morana - F. Rescigno
D. Romano - G. Strada

Intelligenza artificiale, terrorismo e responsabilità delle piattaforme digitali. Tra Stati Uniti e Unione europea

Andrea Casiere
Dottorando di ricerca, Università degli Studi di Foggia

ABSTRACT

A partire dalla pronuncia *Gonzalez v. Google* della Corte Suprema degli Stati Uniti in materia di terrorismo e algoritmi, il presente contributo analizza il rapporto tra intelligenza artificiale e responsabilità delle piattaforme digitali confrontando il modello 'tecno-libertario' statunitense, che privilegia la libertà di espressione e di impresa delle *tech companies*, e quello 'regolatorio' europeo, che pone maggiore enfasi sulla protezione dei diritti degli utenti, sulla privacy e sulla sicurezza online.

SOMMARIO

1. Il *trait d'union*. Terrorismo, algoritmi, *Generative AI* e piattaforme digitali

Il 18 maggio 2023, pronunciandosi sui casi *Reynaldo Gonzalez, et al., v. Google LLC*[1] e *Twitter, Inc. v. Mehier Taamneh, et al.*[2], la Corte Suprema degli Stati Uniti ha escluso la responsabilità civile di Google e Twitter per le morti di Nohemi Gonzalez e di Nawras Allassaf negli attentati jihadisti di Parigi (2015) e Istanbul

*Contributo selezionato dal Comitato Scientifico della rivista in relazione alla call "Diritto, Religioni e Intelligenza artificiale: quali prospettive?" del luglio 2024.

[1] *Reynaldo Gonzalez, et. al, v. Google, inc.*, 335 F. Supp. 3d 1156 (N.D. Cal. 2018).

[2] *Twitter, Inc. v. Mehier Taamneh, et al.*, 598 U. S. (2023).

(2017). In particolare, nel caso *Gonzalez*, la Corte era chiamata a valutare l'applicabilità della Section 230 *Communications Decency Act* (CDA)[3] agli algoritmi del *recommender system* di YouTube, responsabili di aver favorito la circolazione di materiale terroristico in relazione all'attentato del 2015 e di aver contribuito all'ascesa mediatico-finanziaria dell'ISIS[4]. Deludendo le aspettative di alcuni commentatori[5], la Corte ha rilevato l'insussistenza della *proximate causation*, elemento costitutivo della responsabilità civile prevista dall'*Anti-Terrorism Act* (ATA), e ha pertanto dichiarato l'irresponsabilità di Google senza decidere sulla Section 230[6].

La Section 230, nota come 'norma che ha creato Internet'[7], è il pilastro del modello 'techno-libertarian'[8] statunitense: essa, grazie alla previsione dell'irresponsabilità per i contenuti di terze parti e per l'attività di moderazione online, ha permesso l'ascesa delle piattaforme digitali (specie dei social) escludendo gli onerosi costi di monitoraggio e risarcimento per le condotte illecite degli utenti. L'Unione Europea, che inizialmente si era ispirata a questo approccio, pur mantenendo il divieto di obbligo generale di sorveglianza (direttiva e-Commerce prima e Digital Service Act poi), ha rivendicato progressivamente un maggiore controllo sull'operato degli intermediari digitali con atti di *soft* e *hard law* che hanno introdotto divieti, obblighi e oneri a carico delle *tech companies* (*e.g.*, Forum dell'UE su Internet, Codici di condotta, GDPR, reg. (UE) 784/2021, Digital Service Package)[9].

[3] *Communications Decency Act*, 47 U.S.C. § 230 (1996).

[4] Cfr. G. De Vynck, *The death of Nohemi Gonzalez led to a Supreme Court fight with Google*, 18 febbraio 2023, liberamente consultabile su www.washingtonpost.com

[5] Cfr. O. Chowdhury, *Gonzalez v. Google: Testing the Boundaries of section 230*, in *UC Law SF Communication and Entertainment Journal*, vol. 45(2) del 2023, p. 135 ss.

[6] Nel corso dell'*oral argument* del caso *Gonzalez*, il giudice della Corte Suprema Elena Kegan aveva già rinviato informalmente la questione al Congresso. Cfr. *Trascrizione dell'oral argument del caso Gonzalez v. Google, inc.*, pp. 45, 46, liberamente consultabile su www.supremecourt.gov

[7] Cfr. J. Kosseff, *The Twenty-Six Words That Created the Internet*, Cornell University Press, 2019; cfr. altresì O. CHOWDHURY, *Gonzalez v. Google*, cit., p. 135 ss.

[8] Anu Bradford, *Europe's Digital Constitution*, in *Virginia Journal of International Law*, vol. 64(1) del 2023, pp. 4, 5.

[9] L'UE «si è allontanata dall'approccio regolatorio degli Stati Uniti, che lascia il comando alle *tech companies*», ma, al contempo, è anche lontana dalla Cina, «il cui approccio cerca di preservare il potere politico dello Stato». Anu Bradford, *Europe's Digital Constitution*, cit., pp. 10-12, 20-21. Per un primo approfondimento, si veda anche G. De Gregorio, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, 2022.

Da ultimo, la diffusione globale delle tecnologie d'intelligenza artificiale[10] ha indotto l'UE ad approvare un regolamento che stabilisce regole armonizzate sull'AI[11] per mitigare i rischi derivanti dall'abuso di uno strumento che, secondo gli esperti, è in grado di minacciare la «sopravvivenza dell'umanità al pari della guerra nucleare e delle pandemie»[12].

L'allarme per i potenziali impieghi criminali di questa tecnologia è stato ribadito anche dall'*Australian eSafety Commissioner* e da Europol[13]. In particolare, nell'ambito della lotta al terrorismo islamista, è stato osservato che l'AI potrebbe rendere la minaccia «più pervasiva che mai»[14], specie con riguardo alla radicalizzazione, al finanziamento e all'organizzazione di attentati, attività in cui il jihadismo digitale ha già dato ampia prova di sé[15].

[10] «I mesi recenti sono stati dominati dai dibattiti sulla ricerca e lo sviluppo dell'AI e sulle sue implicazioni socioeconomiche. Molti di questi hanno preso le mosse dall'ascesa dell'AI generativa – inclusi i chatbot come ChatGPT di OpenAI e Bard di Google – dei sottostanti *large language models* (LLM) (e.g., Google's LaMDA, Meta's LLaMA, OpenAI's GPT-4, and Google's PaLM 2)». M. Wörsdörfer, *Mitigating the adverse effects of AI with the European Union's artificial intelligence act: Hype or hope?*, in *Wiley*, n. 43 del 2024, pp. 106-126.

[11] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

[12] Così Sam Altman, fondatore e CEO di OpenAI, il 16 maggio 2023 dinnanzi al Congresso. Altman ha inoltre riferito che la sua più grande paura «è che noi, l'industria, possiamo causare danni significativi al mondo». Nostra traduzione. Cfr. G. Weimann (et. al.), *Generating Terror: The Risk of Generative AI Exploitation*, in *CTCSENTINEL*, vol. 17(1) del 2024. Sul punto, si veda altresì M. Wörsdörfer, *Mitigating the adverse effects of AI*, cit., p. 107.

[13] Australian eSafety Commissioner, *GenerativeAI position statement*, 15 agosto 2023 (ultimo aggiornamento), liberamente consultabile su www.esafety.gov.au Anche il recente rapporto di Europol ha evidenziato che «gli LLM come ChatGPT possono essere usati per commettere o facilitare crimini, inclusi la sostituzione di persona, gli attacchi di ingegneria sociale e la produzione di codice malevolo che può essere usato nel cy-ber-crimine». Europol, *The impact of Large Language Models on Law Enforcement, a Tech Watch Flash Report from the Europol Innovation Lab, Publications Office of the European Union, Luxembourg*, 19 dicembre 2023 (ultimo aggiornamento), p. 7 ss, liberamente consultabile su www.europol.europa.eu

[14] Nostra traduzione. G. Weimann (et. al.), *Generating Terror*, cit., p. 19 ss.

[15] «I terroristi e gli estremisti violenti hanno dato prova di sapersi adattare notevolmente nello sfruttamento delle piattaforme online per raggiungere i propri scopi. Dall'avvento deli siti web estremisti alla fine degli anni '90 alle nuove piattaforme social come Facebook, YouTube, Twitter, Instagram e TikTok, questi gruppi hanno rapidamente impiegato e sfruttato gli sviluppi del cyberspazio». Nostra traduzione. G. Weimann (et. al.), *Generating Terror*, cit.; sul punto, ci sia con

Tuttavia, nonostante l'intensità della minaccia paventata, il contrasto ai potenziali impieghi terroristici (e più in generale ad ogni impiego illecito) dell'AI non può prescindere dal ponderato bilanciamento tra sicurezza e libertà costituzionalmente garantite. Per questo motivo, è essenziale limitare l'(ab)uso dell'argomento securitario[16] che, quante volte viene applicato nella porzione digitale dell''infosfera'[17], provoca l'aumento di misure restrittive e/o sanzionatorie che possono tradursi nella limitazione della libertà di espressione religiosa (e non) online.

In proposito, uno dei principali nodi da sciogliere resta quello della responsabilità dei fornitori di servizi di AI. Se negli USA sembra prevalere, in assenza di una espressa previsione normativa, l'interpretazione che estende l''immunità' della Section 230 anche ad algoritmi e contenuti generati dall'intelligenza artificiale, l'Unione europea, rifiutata «l'idea tecno-libertaria di uno spazio digitale senza regole o auto-governato» e promossa una transizione digitale «fermamente ancorata allo stato di diritto e soggetta allo scrutinio democratico»[18], introduce un sistema di restrizioni proporzionate al rischio dello specifico sistema di AI, con poteri di controllo e sanzione attribuiti direttamente alla Commissione[19].

Nei successivi paragrafi esamineremo la questione dal punto di vista dell'ordinamento statunitense, caratterizzato dalla centralità del *free speech* e della libertà di impresa, e dell'ordinamento europeo, caratterizzato da una maggiore enfasi sulla protezione dei diritti degli utenti, sulla privacy e sulla sicurezza online.

2. Il modello statunitense. Section 230 e AI

Un recente rapporto del *Congressional Research Service* (CRS), agenzia che

sentito altresì un rinvio ad A. Casiere, *Il jihadismo digitale. Libertà religiosa, sicurezza, democrazia*, in *Stato, Chiese e pluralismo confessionale*, fascicolo 7 del 2023 e A. Casiere, *A brave new (digital) world. Tra terrorismo e autoritarismo digitale*, in *Coscienza e Libertà*, n. 67 del 2024, pp. 203-216.

[16] Cfr. A. Casiere, *A brave new (digital) world*, cit.

[17] Di 'infosfera' parla L. Floridi in Id., *The Fourth Revolution. How the Infosphere is Reshaping Human Reality,* Oxford University Press, Oxford, 2014.

[18] Nostra traduzione. Anu Bradford, *Europe's Digital Constitution*, cit., p. 12.

[19] *Ivi*, cit., pp. 4, 5 e 11.

supporta il dibattito del legislatore statunitense, ha posto l'accento sulla relazione tra Section 230 e GenAI[20]. La questione era stata affrontata incidentalmente proprio nell'*oral argument* del caso *Gonzalez*[21].

Per comprendere i termini della vicenda, è necessario tornare al 1996, quando, con l'obiettivo di promuovere la concorrenza e la diffusione delle nuove telecomunicazioni, il Congresso approvava il *Telecommunications Act*[22]. In quella sede, per impedire l'accesso dei minori alla pornografia online, la riforma introduceva anche il *Communications Decency Act* (CDA)[23], un pacchetto di disposizioni dichiarato successivamente incostituzionale per violazione del Primo Emendamento[24] a eccezione della Section 230, norma che sancisce l'irresponsabilità del provider per i contenuti di terze parti e per l'attività di moderazione di contenuti online. A partire dal 1997, la giurisprudenza statunitense ha progressivamente ampliato tale 'immunità', lasciando esclusi i soli casi in cui il provider partecipi attivamente alla creazione o allo sviluppo del contenuto illecito ospitato[25].

Ne è derivato un modello che, frutto della combinazione di «normativa debole in materia di antitrust, assenza di normativa federale sulla protezione dei dati, e regole permissive in materia di moderazione dei contenuti che

[20] L'espressione «intelligenza artificiale generativa (GenAI) si riferisce ai sistemi di AI e, in particolare, a quelli che usano il *machine learning* (ML) e sono addestrati su grandi volumi di dati e che sono capaci di generare nuovi contenuti. […] I sistemi di GenAI, quando ricevono un input (spesso un input di testo di un utente) possono creare risultati che includono risposte di testo (e.g., OpenAI's ChatGPT and Google's Bard), immagini (e.g., Stability AI's Stable Diffusion and Midjourney's self-titled program), video, codici di programmazione o musica. La recente diffusione al pubblico di molti strumenti di GenAI e la corsa delle compagnie a sviluppare modelli sempre più potenti ha suscitato un ampio dibattito sulle loro capacità, preoccupazioni in relazione al loro uso e dibattiti sulla loro governance e regolazione». Nostra traduzione. Congressional Research Service, *Generative Artificial Intelligence*, cit., p. 1.

[21] *Trascrizione dell'Oral Argument del caso Gonzalez v. Google, inc.*, p. 47 ss, liberamente consultabile su www.supremecourt.gov

[22] In riforma del Titolo 47, Capitolo 5 dello U.S. Code (U.S.C.) risalente al 1934.

[23] Il *Communications Decency Act* è un titolo del *Telecommunications Act* del 1996.

[24] *Reno v. ACLU*, 521 U.S. 844 (1997).

[25] «Dall'entrata in vigore del CDA nel 1996, sono stati sollevati 888 casi giudiziari riguardanti la Section 230 tra le giurisdizioni statali e quelle federali». Cfr. K. Dimitroff, *Mark Zuckerberg, Joe Manchin, and ISIS: What Facebook's International Terrorism Lawsuits Can Teach Us About the Future of Section 230 Reform*, in, in *Texas Law Review*, vol. 100 del 2021, p. 162.

schermano le aziende dalla responsabilità»[26], ha raggiunto gli obiettivi individuati dal legislatore del '96[27] e fatto guadagnare alla Section 230 il titolo di 'norma che ha creato Internet'[28].

Non solo. A trent'anni di distanza, l'immunità prevista dal CDA è diventata «il cuore dell'*internet regulation zeitgeist*»[29], «il Primo Emendamento potenziato, per l'era di Internet»[30]: essa, «perme[ttendo] agli internet provider di continuare a innovare evitando la responsabilità per i contenuti delle loro piattaforme»[31], ha «aperto la porta all'evoluzione dell'ecosistema digitale», ribadito «il primato del Primo Emendamento nel costituzionalismo statunitense» e gettato «il pilastro fondamentale della legittimazione dei poteri delle piattaforme»[32]. Mentre l'Unione europea ha promosso il «bilanciamento della libertà di espressione con una serie di altri diritti fondamentali» tra cui «la dignità umana, la non discriminazione e il diritto alla privacy»[33], l'ordinamento statunitense è rimasto concentrato «sulla protezione del *free speech* [delle piattaforme] inteso come *il* diritto fondamentale toccato dalla transizione digitale»[34].

Con riguardo alla diffusione di contenuti jihadisti online, sebbene indirizzi giurisprudenziali minoritari abbiano ritenuto che l'agevolazione mediante

[26] *Ivi*, p. 4.

[27] Quanto agli obiettivi indicati dal legislatore, si veda ad es. *Communications Decency Act*, 47 U.S.C. § 230 (b). Quanto ai risultati raggiunti, basti pensare al traguardo raggiunto nel 2018 con «*19 milioni di posti di lavoro*» raggiunti. Cfr. *amplius* K. Dimitroff, *Mark Zuckerberg, Joe Manchin, and ISIS*, cit., p. 161.

[28] Cfr., *supra*, nota 7.

[29] Nostra traduzione. Cfr. K. Dimitroff, *Mark Zuckerberg, Joe Manchin, and ISIS*, cit., pp. 153-186.

[30] Nostra traduzione. J. Kosseff, *The Twenty-Six Words*, cit.

[31] Nostra traduzione. O. Chowdhury, *Gonzalez v. Google*, cit., p. 135 ss.

[32] Nostra traduzione. G. De Gregorio, *Digital Constitutionalism in Europe*, cit., pp. 45, 46.

[33] Nostra traduzione. Anu Bradford, *Europe's Digital Constitution*, cit., p. 11.

[34] Nostra traduzione. Anu Bradford, *Europe's Digital Constitution*, cit., p. 11. Nel sistema statunitense, il Primo Emendamento tutela gli intermediari digitali dai poteri pubblico, mentre non opera nel rapporto (privatistico) tra piattaforma e utente: tanto in considerazione del tenore letterale della norma costituzionale, che indirizza i propri effetti ai poteri pubblici, quanto in virtù della *state action doctrine*, dottrina secondo cui «la costituzione statunitense in generale e i diritti individuali ivi riconosciuti in particolare, si applicano solo all'azione pubblica, non a quella privata», salvo che quest'ultima non sia qualificabile, per circostanze eccezionali, come '*state actor*'. Su quest'ultimo punto, per un primo approfondimento, si veda la voce *Constitution Annotated. Amdt1.7.2.4 State Action Doctrine and Free Speech*, liberamente consultabile su constitution.congress.gov

algoritmi fosse esorbitante rispetto all'immunità prevista dal CDA[35], la Section 230 «è stata interpretata in modo tanto ampio da escludere quasi ogni tipo di responsabilità civile dei fornitori di servizi informatici per le attività dei loro utenti», nonostante potessero «virtualmente essere ritenuti responsabili per i danni derivanti da atti di terrorismo»[36]. E, infatti, nessuna delle vittime statunitensi di attacchi terroristici internazionali «è riuscit[a] a ottenere un risarcimento da un fornitore di servizi informatici»[37].

Piuttosto, se qualcosa è stato fatto in tema di moderazione dei contenuti, attività che avrebbe dovuto garantire la 'pacifica convivenza online' in cambio della irresponsabilità per i contenuti di terze parti[38], ciò si deve all'affermazione globale del paradigma regolatorio europeo, importato negli USA dalle piattaforme digitali attraverso la generalizzazione delle *policies* adottate per adeguarsi a Bruxelles[39].

Oggi, la Section 230 è al centro del dibattito sull'intelligenza artificiale. Considerata la diffusione e lo straordinario potenziale di questa tecnologia e, in particolare, della GenAI, il Congresso «ha manifestato l'intenzione di regolare la materia»[40], rendendo indispensabile la soluzione della questione relativa

[35] In tal senso, ad esempio, si è espresso Chief Judge Katzmann nella *partial dissenting opinion* del caso *Force v. Facebook, Inc., 934 F.3d 53 (2d Cir. 2019)*.

[36] K. Dimitroff, *Mark Zuckerberg, Joe Manchin, and ISIS: What Facebook's International Terrorism Lawsuits Can Teach Us About the Future of Section 230 Reform*, in, in *Texas Law Review*, vol. 100 del 2021, p. 168.

[37] *Ibidem.*

[38] «Quando il Congresso ha approvato la Section 230 del CDA, ha fatto un patto implicito con ogni ISP: l'immunità per la responsabilità sussidiaria in cambio del tentativo di ripulire il proprio sito web da contenuti diffamatori o comunque illegali di terze parti». Nostra traduzione. A.M. Sevanian, *Section 230 of the Communications Decency Act: A "Good Samaritan" Law Without the Requirement of Acting as a "Good Samaritan"*, in *UCLA Entertainment Law Review*, 21(1) del 2014, pp. 122-146.

[39] Tanto da far ritenere che «anche se la costituzione statunitense potrebbe essere usata per tutelare il *free speech* online, nella pratica, le norme europee in materia digitale spesso sovrascrivono le norme di permesso». Nostra traduzione. Anu Bradford, *Europe's Digital Constitution*, cit., p. 3.

[40] «Nell'ultimo anno, le *tech companies* hanno ampliato l'accesso ai servizi in grado di creare contenuti usando l'intelligenza artificiale (AI). Man mano che gli strumenti di AI si sono diffusi e i suoi modelli sono diventati più potenti, il Congresso ha mostrato interesse nella regolazione dei modelli di AI […] le Commissioni hanno tenuto udienze e i parlamentari hanno proposto leggi per regolare l'AI (o annunciato di essere pronti a farlo). Alcuni membri hanno invocato la costituzione di una task-force o commissione per raccomandare le norme. L'Esecutivo ha altresì adottato un Executive Order, nell'ottobre 2023, affidando alle agenzie il compito di adottare azioni per affrontare l'avvento dei modelli di AI». Nostra traduzione. Cfr. Congressional Research Service, *Section 230 Immunity and Generative Artificial Intelligence*, 28 dicembre 2023.

alla possibilità che le aziende siano «ritenute responsabili per i contenuti illeciti generati»[41] dagli utenti. Ciò potrebbe indirettamente ripercuotersi anche sulla libertà di religione e di espressione, provocando l'adozione di politiche restrittive dei provider a ciò indotti dalla necessità di prevenire l'addebito di responsabilità per i contenuti generati su input degli utenti.

Per il momento, in assenza di un chiaro indirizzo legislativo, il dibattito statunitense resta aperto: a quanti ritengono che gli «AI provider dovrebbero essere considerati come creatori o sviluppatori di contenuti che non beneficiano dell'immunità della Section 230» si oppongono quelli che ritengono, seguendo l'impostazione tradizionale, che gli LLM[42] siano «interamente guidati da input di terze parti» e, perciò, «non inventano, creano, o sviluppano output senza che siano sollecitati da un *information content provider*», il quale resta l'unico responsabile dei contenuti prodotti[43].

3. Il modello europeo. 'Costituzionalismo digitale' e *AI Act*

L'approvazione dell'*AI Act*[44] ribadisce il ruolo centrale dell'Unione europea nella regolazione (del mercato interno) digitale, alla luce dei principi di primazia e attribuzione e, dunque, degli artt. 5 TUE e 4, 26, 27, 114 e 115 TFUE.

L'atto normativo, proposto dalla Commissione nel 2021 e approvato nel 2024, rappresenta «la prima significativa iniziativa governativa nel mondo ad occuparsi – e idealmente a mitigare – l'impatto negativo potenziale dei sistemi di AI», nonché «una pietra miliare»[45] e «lo sforzo internazionale più significativo per regolare lo sviluppo e l'uso dell'AI»[46]. Esso si pone l'obiettivo di assicurare l'affidabilità e l'eticità dei sistemi di intelligenza artificiale nell'interesse della

[41] Nostra traduzione. Congressional Research Service, *Section 230 Immunity and Generative Artificial Intelligence*, cit., p. 1.

[42] «I Large language models (LLMs) sono sistemi di AI che mirano a modellare il linguaggio, talvolta usando milioni o miliardi di parametri […] In particolare, i modelli di GenAI lavorano per adattarsi allo stile e all'aspetto dei dati di addestramento impiegati. È stato anche dimostrato che hanno una […] capacità nascoste che i loro sviluppatori e utenti non avevano previsto». Nostra traduzione. Congressional Research Service, *Generative Artificial Intelligence*, cit., p. 1.

[43] *Ibidem.*

[44] Cfr. *sub* nota 11.

[45] Nostra traduzione. M. Wörsdörfer, *Mitigating the adverse effects of AI*, cit., p. 111.

[46] Nostra traduzione. Così J. Tallberg (Et Al.), *AI regulation in the European Union: examining non-state actor preferences*, in *Business and Politics*, n. 26 del 2024, pp. 218-239.

stabilità e dello sviluppo del mercato interno, ma anche della tutela dei diritti fondamentali e della democrazia, nonché della sovranità digitale europea; per raggiungere questo risultato, il legislatore adotta un approccio basato sul rischio che intende minimizzare i sacrifici imposti alla libertà d'impresa in nome della sicurezza online[47].

L'approccio eurounitario in cui i diritti fondamentali hanno un ruolo centrale si è sviluppato a partire dalla giurisprudenza della Corte di Giustizia[48] ed è stato 'codificato' dal Trattato di Lisbona che ha riconosciuto il ruolo primario di diritti, libertà e principi sanciti non solo nella Carta dei diritti fondamentali dell'UE, equiparata ai Trattati, ma anche di quelli garantiti dalla CEDU e risultanti dalle 'tradizioni costituzionali comuni' degli Stati membri. Attraverso questo processo, l'UE ha conosciuto una «lenta emancipazione dall'*imprinting* economico caratterizzante il mercato unico» e un progressivo avvicinamento a una «dimensione costituzionale multilivello che sembra sempre più guidare [anche] le politiche digitali dell'Unione nella nuova stagione del costituzionalismo digitale»[49]. A partire da questa evoluzione, le istituzioni europee hanno lavorato anche per «riaffermare lo scrutinio democratico sulle *tech companies*», «rivendica[ndo] il controllo sull'industria [*tech*]» mediante le limitazioni necessarie «per proteggere la dignità umana, la privacy, o il discorso democratico»[50]. Uno dei principali effetti collaterali di questo processo ha preso il nome di 'effetto Bruxelles' e consiste nell'espansione dello «standard regolatorio più stringente»[51] al mercato statunitense, attraverso l'esportazione delle *policies* aziendali adottate per il mercato europeo.

[47] D. Mügge, *EU AI sovereignty: for whom, to what end, and to whose benefit?*, in *Journal of European Public Policy*, 28 febbraio 2024, p. 3. M. Wörsdörfer, *Mitigating the adverse effects of AI*, cit., p. 108 ss.
[48] È noto che il percorso giurisprudenziale della Corte di Giustizia in tema di diritti fondamentali e di 'tradizioni costituzionali comuni' costituisce il presupposto storico-giuridico della equiparazione della Carta dei diritti fondamentali dell'UE al rango dei Trattati (art. 6 TUE), nonché del riconoscimento di diritti, libertà e i principi ivi sanciti, assieme a quelli individuati dalla CEDU e delle 'tradizioni costituzionali comuni' agli Stati membri, quali principi generali del diritto dell'Unione. Per un primo approfondimento sul tema, si veda G. de Vergottini, *Tradizioni costituzionali comuni e Costituzione europea*, liberamente consultabile su www.forumcostituzionale.it
[49] G. De Gregorio, *Il diritto delle piattaforme digitali: un'analisi comparata dell'approccio statunitense ed europeo al governo della libertà di espressione*, in *DPCE Online*, numero speciale del 2021, p. 1.466.
[50] Nostra traduzione. Anu Bradford, *Europe's Digital Constitution*, cit., pp. 10, 20, 21.
[51] *Ivi*, p. 6.

L'ultimo tassello di questo puzzle è l'*AI Act*: con ogni probabilità, infatti, l''effetto Bruxelles' è destinato a riproporsi anche nel campo della regolazione dell'intelligenza artificiale, tanto più che l'ambito di applicazione del regolamento è rivolto espressamente agli «attori privati e pubblici, dentro e fuori l'UE, ogniqualvolta impatti sui suoi cittadini»[52].

Il regolamento (UE) 2024/1689, che stabilisce regole armonizzate sull'intelligenza artificiale, si compone di ottantacinque articoli divisi in dodici titoli e mira a garantire il funzionamento del mercato interno attraverso un quadro giuridico uniforme, che sia conforme ai valori dell'UE e che tenga conto di motivi imperativi di interesse pubblico come la salute, la sicurezza e i diritti fondamentali, senza pregiudicare la libertà di circolazione transfrontaliera di beni e servizi basati sull'AI[53]. Per realizzare questo bilanciamento, l'atto normativo regola l'uso dell'intelligenza artificiale «in funzione del rischio potenzialmente generato»[54], costruendo una piramide a tre livelli (rischio inaccettabile, alto e minimo) cui corrispondono il divieto totale e/o imposizioni che evitano «restrizioni inutili al commercio» [55]. In particolare, si prevede che ogniqualvolta i rischi siano inaccettabili, è «nega[to] l'accesso al mercato», come nel caso di sistemi che implicano la manipolazione, lo sfruttamento di vulnerabilità, danni fisici o psicologici e persino per i sistemi di identificazione biometrica remota in tempo reale in spazi accessibili al pubblico, salve le eccezioni espressamente enucleate (Titolo II, art. 5); si concede l'accesso al mercato se i sistemi, ad alto rischio, rispettano i «requisiti tecnici [previsti] ex-ante e una procedura di monitoraggio del mercato ex-post» (Titolo III, artt. 6 ss.) e, invece, 3) si prevedono, per «i sistemi a rischio minimo», solo «requisiti di sicurezza generali, come quelli inclusi nella Direttiva sulla sicurezza generale dei prodotti»[56] (Titolo IV, artt. 53

[52] Nostra traduzione. M. Wörsdörfer, *Mitigating the adverse effects of AI*, cit., pp. 109-111.

[53] Così il considerando n. 1 della proposta di regolamento europeo che stabilisce regole armonizzate sull'intelligenza artificiale (AI Act). Le restrizioni imposte, si legge, devono essere «proporzionate e limitate al minimo necessario per prevenire e attenuare rischi gravi per la sicurezza e probabili violazioni dei diritti fondamentali». Cfr. COM(2021) 206 final, *Relazione sulla proposta di regolamento europeo che stabilisce regole armonizzate sull'intelligenza artificiale*, p. 12.

[54] Ipsoa Quotidiano, *Intervista a Gabriele Mazzini – EU AI Act Team Leader, European Commission*, 8 maggio 2024, liberamente consultabile su www.iposa.it

[55] COM(2021) 206 final, *Relazione sulla proposta di regolamento europeo*, cit., p. 3.

[56] Nostra traduzione. M. Wörsdörfer, *Mitigating the adverse effects of AI*, cit., p. 109.

ss.). Come nel caso del Digital Service Act (DSA) e del Digital Market Act (DMA)[57], i poteri di controllo e sanzione della Commissione permettono di esercitare una pressione significativa sulle piattaforme.

Questa forma di 'influenza' suscita alcune perplessità, specie in quanto si presta a una potenziale forma di restrizione per via amministrativa della libertà di impresa che si traduce in una limitazione delle libertà digitali degli utenti, nel solco del progressivo «incremento di norme volte a garantire l'ordine pubblico e un maggior grado di sicurezza» attraverso atti di *soft* o *hard law* relativi alla lotta al terrorismo, *hate speech* o *fake news*[58], come ad esempio la direttiva (UE) 2017/541 in cui si invocava l'anticipazione della tutela penale con riguardo alla «diffusione o qualunque altra forma di pubblica "divulgazione di un messaggio, con qualsiasi mezzo, sia online che offline", con intenti apologetici di atti terroristici»[59].

E, invero, questo approccio ha già provocato lo scontro tra la Commissione e la piattaforma digitale X (già Twitter), con sede negli USA. In una precedente occasione, il Commissario europeo per il mercato interno Thierry Breton aveva pubblicamente invitato X a rispettare gli obblighi previsti dal DSA intervenendo per moderare i contenuti terroristici asseritamente in circolazione sulla piattaforma relativi agli attacchi di Hamas del 7 ottobre 2023 in Israele[60]. Più di recente, Elon Musk, proprietario del social, ha accusato il Commissario europeo per il mercato interno Thierry Breton di aver proposto un accordo segreto per censurare il dibattito pubblico in cambio dell'esenzione dalle sanzioni previste dal DSA[61]. Questi episodi dimostrano l'ulteriore allontanamento dell'Europa dal paradigma statunitense, che, almeno sulla carta, tutela il *free speech* dall'interferenza governativa.

[57] Sul punto, ci sia consentito il rinvio ad A. Casiere, *Il jihadismo digitale*, cit.

[58] Sul punto, cfr. *amplius* A. Casiere, *Il jihadismo digitale*, cit.

[59] F. Alicino, *La dimensione politico religiosa dell'infosfera islamista*, in Id. (a cura di), *Terrorismo di ispirazione religiosa. Prevenzione e deradicalizzazione nello Stato laico*, Editrice Apes, Roma, pp. 104 105. Sul punto, si veda anche V. Valente, *Sicurezza e libertà alla luce del terrorismo islamista. La circolazione dei modelli di contrasto e prevenzione*, in F. Alicino, *Terrorismo di ispirazione religiosa*, cit., p. 179 ss.

[60] Agenzia Ansa, *Botta e risposta Musk-Breton, 'elencateci le violazioni su X'. Commissario Ue, 'siete consapevoli dei contenuti falsi'*, 11 ottobre 2023.

[61] Cfr. E. Musk (@elonmusk), www.x.com/elonmusk/status/1811783320839008381 12 luglio 2024 (17.22).

Il 12 luglio 2024, l'*AI Act* è stato pubblicato in Gazzetta ufficiale[62]: a questo punto non resta che valutare, nel medio periodo, l'impatto sul mercato dei servizi di AI, sui diritti fondamentali e sui processi democratici, sia a livello regionale che a livello globale.

4. Conclusioni. Due modelli e l'Occidente al bivio

In Occidente, oggi si confrontano due diversi approcci di regolazione digitale e, quindi, di regolazione dell'AI, la cui comune matrice liberale non è stata sufficiente a garantire lo sviluppo unitario del quadro normativo: il modello 'liberal-liberista' statunitense, in cui il rischio (anche) significativo è considerato sostenibile in nome di una libertà che giustifica l'irresponsabilità delle piattaforme, e il modello 'liberal-regolatorio' europeo, che, sviluppatosi nel quadro del nascente costituzionalismo digitale, impone restrizioni alla libertà d'impresa e di espressione in nome della sicurezza online.

Entrambi gli approcci devono fare i conti con sfide significative.

Da un lato, il modello statunitense si confronta con la complessità del mondo post-9/11, in cui la prevalenza della libertà sulla sicurezza è complicata non solo dalla presenza della minaccia terroristica, ma anche dagli esiti della globalizzazione e della diffusione di tecnologie che producono rischi senza precedenti. Dall'altro, il modello europeo, che propende per un atteggiamento proattivo in tema di sicurezza digitale, si confronta con la tentazione di una (iper) normazione che potrebbe rivelarsi altrettanto dannosa, frustrando in senso securitario il bilanciamento tra sicurezza e libertà di religione e di espressione, con una significativa anticipazione dell'azione di contrasto e un generale incentivo alla moderazione preventiva dei contenuti online.

In questo scenario, l'accelerazione determinata dalla diffusione dell'AI mette l'Occidente difronte a un bivio: insistere sulla strada tecno-libertaria statunitense, esponendosi a rischi che potrebbero concretizzarsi (ma anche non concretizzarsi o essere contenuti dagli stessi attori economici), oppure percorrere la strada regolatoria dell'Unione europea che, pur offrendo maggiore sicurezza, potrebbe produrre effetti negativi per l'innovazione, la competitività e (forse) anche per la libertà di espressione e di religione.

[62] Cfr. *sub* nota 11.