Stato, Chiese
e pluralismo confessionale

Andrea Casiere
(dottorando di ricerca in Diritto ecclesiastico e canonico nell'Università degli Studi di Foggia, Dipartimento di Giurisprudenza)

Il jihadismo digitale. Libertà religiosa, sicurezza, democrazia *

*Digital jihadism. Freedom of religion, security, democracy **

ABSTRACT: The Digital Revolution and the emergence of the Algorithmic Society made difficult the relationship between security and liberty. On the one hand, the digitalizing of terrorism and extremism has put in danger the public safety, due to misuse of social media and platform to radicalize (lone wolves), recruit, train or planning terrorist attacks. On the other hand, the public-private model of governance of speech has endangered the freedom of religion and speech, by permitting private actors to censure users, through AI and without the shield of the rule of law, under the cloak of freedom of contracts. This paper analyzes the state of the art, trying to draw a perimeter for the study of underlying issues and relationship between religion, democracy and security in the digital era.

1 - Introduzione

Il 7 giugno 2022, termine iniziale per l'applicazione del regolamento (UE) 2021/784 relativo al contrasto della diffusione di contenuti terroristici online, il vicepresidente della Commissione Europea Margaritis Schinas ha ricordato l'importanza della lotta online al terrorismo.

> "Gli ultimi anni sono stati segnati da terribili attacchi terroristici sul suolo europeo. Le immagini degli attacchi a Parigi, Halle e Christchurch ci ricordano che la lotta al terrorismo deve avere luogo sia online che offline […] Oggi, l'Unione europea della sicurezza diviene una realtà tangibile"[1].

* Contributo sottoposto a valutazione - Peer reviewed paper.

L'attenzione dedicata dalle istituzioni dell'Unione alla sicurezza della rete è, almeno in parte, la risposta indifferibile agli attacchi islamisti e ai gravi pericoli[2] derivanti dalla digitalizzazione del fondamentalismo religioso[3]. Al contempo, però, essa risponde all'esigenza di creare un ambiente online sicuro, prevedibile e affidabile, che faciliti l'innovazione, e in cui i diritti fondamentali siano tutelati in modo effettivo dai rischi inerenti alla privacy, alla libertà di espressione e di informazione, alla libertà di religione e ai processi democratici.

Secondo la tesi sposata dall'Unione europea, infatti, la protezione della libertà e il contrasto ai contenuti illeciti online - tra cui quelli a carattere terroristico detengono senz'altro il primato di pericolosità[4] - non devono essere elementi contrastanti, "bensì obiettivi complementari che si rafforzano a vicenda"[5].

Nella medesima prospettiva va letta la recente approvazione dei regolamenti (UE) 2022/1925 (*Digital Markets Act*) e 2022/2065 (*Digital Services Act*) che compongono il *Digital Services Act package*, lo strumento normativo con cui l'Unione europea ha scelto di affrontare la difficile sfida dell'aggiornamento e dell'armonizzazione della disciplina europea sui servizi digitali.

A partire da queste premesse, le riflessioni che seguono si propongono di analizzare la questione del bilanciamento tra sicurezza e

---

Elaborato nell'ambito delle ricerche del progetto PRA-HE 2021 "RE.CO.SE - *Religion and Comprehensive Security*" finanziato dall'Università degli Studi di Foggia (bando PRA_HE 2021 UNIFG finanziato dall'Unione europea mediante il programma Next Generation EU e dal programma MUR-Fondo Promozione e Sviluppo-DM 737 del 2021).

[1] Nostra la traduzione. Cfr. **COMMISSIONE EUROPEA**, *Security Union: Rules on removing terrorist content online become applicable (Press Release)*, 7 giugno 2022.

[2] Il Consiglio Europeo, infatti, ha sottolineato che "le minacce sono diverse e cambiano costantemente. I gruppi di Al-Qaida e dello Stato islamico continuano a incoraggiare attacchi di lupi solitari […] il terrorismo jihadista resta una grande minaccia per l'UE" (nostra la traduzione): cfr. **CONSIGLIO EUROPEO**, *The EU's work to tackle terrorism*, in *www.consilium.europa.eu*, 3 agosto 2022.

[3] Per un primo approfondimento sulla differenza tra estremismo e fondamentalismo e, dunque, sulle conseguenze rispetto al pericolo di radicalizzazione, cfr. **E. PACE, R. GUOLO**, *I fondamentalismi*, Laterza, Bari, 2002, ma anche **P. NASO**, "*Le religioni sono vie di pace" (Falso!)*, Laterza, Bari, 2019.

[4] I contenuti terroristici online "fanno parte del problema del più ampio dei contenuti illegali online", come ricordato proprio dal considerando n. 3 del regolamento (UE) n. 2021/784.

[5] Regolamento (UE) 2021/784, considerando n. 10.

libertà nello spazio digitale europeo, attraverso la lente della sicurezza comprensiva (e non antagonista) della protezione dei diritti umani e quindi inclusiva della così detta "dimensione umana della sicurezza" affermatasi nel panorama regionale europeo e internazionale e, in particolare, nell'ambito OSCE e ONU[6].

[6] La Conferenza sulla sicurezza e sulla cooperazione in Europa (CSCE, poi OSCE) ha dedicato uno dei "*three baskets of comprehensive security*" (poi "*three complementary dimensions*") alla *human dimension*, affiancandola alla *politico-military dimension* e alla *economic and environmental dimension*, in un crescendo enunciativo che va dall'Atto Finale di Helsinki del 1975 alle *Linee Guida su Libertà di religione o convinzione e sicurezza* del 2019. In risposta al paradigma securitario degli anni della violenza religiosa internazionale, le Linee guida riaffermano la complementarità tra libertà religiosa e sicurezza, l'infondatezza dell'equivalenza tra religione e terrorismo e la necessità di responsabilizzazione delle religioni; questi tre elementi, contribuiscono a definire la nozione di *comprehensive security* o sicurezza integrata. Quest'ultima non va confusa con l'omonima "sicurezza integrata" che, quale sviluppo della sussidiarietà e del riparto di competenze di cui all'art. 117 cost., consiste in una integrazione dei "contributi erogabili dalle diverse realtà territoriali, integratisi appunto in un complessivo sistema d'intervento volo alla tutela del bene pubblico" e di cui vi è traccia nel d.l. "Minniti" n. 14 del 2017. In ambito ONU, invece, con la fine della Guerra Fredda, della divisione del mondo in blocchi e dell'„enfasi militare della sicurezza" è emersa una nozione di *human security*. Questa dottrina, a partire dagli anni Novanta, ha promosso la tutela dell'individuo dalle minacce derivanti da "una gamma di fattori sociali, economici e politici come la povertà, l'ambiente" e soprattutto dagli "abusi a danno dei diritti umani". Per un primo approfondimento sulle Linee Guida, cfr. **G. FATTORI**, *Freedom of Religion or Belief is security. The 2019 OSCE Policy Guidance on "Freedom of Religion or Belief and Security"*, in *The Review of Faith & International Affairs*, vol. 40, n. 4 del 2022, pp. 4-11; **ID.**, *Libertà religiosa e sicurezza. Le linee Guida OSCE-ODIHR 2019 su "Libertà di religione o convinzione e sicurezza*, in *Coscienza e Libertà*, n. 61-62 del 2021, p. 51 ss.; **ID.**, *Le Linee Guida OSCE-ODIHR 2019 su "Libertà di religione o convinzione e sicurezza". Dimensione umana e sicurezza integrata*, in *Il Diritto di Famiglia e delle Persone*, n. 1 del 2022, p. 291; ID. (a cura di), *Libertà religiosa e sicurezza (con la prima traduzione italiana delle Linee Guida OSCE 2019 su Libertà di religione o convinzione e sicurezza)*, Pacini Giuridica, Pisa, 2021 e, in particolare, nello stesso volume, i contributi di **G.M. RUOTOLO**, *Il diritto internazionale*, pp. 4-31, e quello di **P. ANNICCHINO**, *La traduzione delle Linee Guida OSCE 2019 in materia di libertà di religione o convinzione e sicurezza*, pp. 199-210; sulla diversa nozione di "sicurezza integrata" cfr. **G. TROMBETTA**, *Ordine pubblico e sicurezza nell'ordinamento italiano,* in *Democrazia e Sicurezza - Democracy and Security Review*, n. 2 del 2020, pp. 72-79, e, altresì, **F. BATTISTELLI**, *La sicurezza e la sua ombra. Terrorismo, panico, costruzione della minaccia*, Donzelli Editore, 2016, p. 121 ss.; cfr. altresì **OSCE**, *The OSCE Concept of Comprehensive and Co-operative Security. An Overview of Major Milestones*, Vienna, giugno 2009; **G. BARBERINI**, *Dalla CSCE all'OSCE. Testi e documenti*, Edizioni Scientifiche Italiane, Napoli, 1995; per un primo approfondimento su *human security* e ONU, cfr. **COMMISSIONE SULLA SICUREZZA UMANA (ONU)**, *Human security now: protecting and empowering people*, New York, 2003, p. 4; **V. DELLA SALA**, *Antiterrorismo e stato: dalla sicurezza nazionale alla sicurezza umana*, in *Quaderni di Sociologia*, n. 39 del 2005, pp. 39-54.

In proposito, è utile ricordare che, mentre la sicurezza è un prerequisito per il godimento delle libertà, allo stesso tempo la protezione delle libertà è necessaria per garantire la sicurezza dal potere pubblico (e, come vedremo, da quello privato).

> "Sicurezza e libertà sono interdipendenti: mentre la sicurezza può in un certo senso essere considerata come un prerequisito per il godimento delle libertà, in un altro senso, la protezione delle libertà è necessaria per garantire la sicurezza (dal potere dello Stato)"[7].

In questo senso, la formula di Aharon Barak, già giudice della Corte suprema israeliana, si rivela un efficace decodificatore della questione securitario-libertaria e della sua complessa evoluzione nel contesto digitale contemporaneo, che costituisce il punto di vista delle seguenti pagine.

Nel prossimo paragrafo è proposta una sintesi dei passaggi chiave della transizione digitale che ha rivoluzionato e amplificato la violenza religiosa.

2 - La transizione digitale del terrorismo jihadista

Il fenomeno dell'informatizzazione jihadista non è nuovo, tanto che, già nel 2005, si riteneva che al-Qaeda fosse "il primo movimento nella storia trasferito nel cyberspazio"[8]. Tuttavia, dalle origini della transizione

---

[7] Nostra la traduzione. Cfr. **S. MACDONALD, S. CORREJA, A. WATKIN**, *Regulating terrorist content on social media: automation and the rule of law*, in *International Journal of Law in Context*, n. 15(2) del 2019, p. 188.; cfr. altresì **A. BARAK**, *Foreword: a judge on judging: the role of the Supreme Court in a democracy*, in *Harvard Law Review*, 2002, pp. 19-162. Con formula analoga Alessandro Negri ricorda che «il rapporto tra sicurezza e diritti, in verità, appare ancora più complesso. Da una parte […] la sicurezza può essere motivo di limitazione dei diritti, ma, al tempo stesso, questi ultimi fungono da invalicabile argine contro derive securitarie […] Se lo scopo della "sicurezza dei diritti", infatti, + garantire il libero esercizio di questi, una misura che muovesse in direzione opposta ne contraddirebbe la stessa essenza. I due, sinora concepiti come nemici, sono dunque tenuti a cooperare per un obiettivo comune, per quanto non sempre di facile conseguimento»: cfr. **A. NEGRI**, *Radicalizzazione religiosa e de-radicalizzazione laica. Sfide giuridiche per l'ordinamento democratico*, Carocci editore, Roma, 2022, p. 43 ss.

[8] L'espressione è di Enzo Rutigliano, che osserva, in proposito, come il «network che continuiamo, forse impropriamente, a chiamare al-Qaeda, è senza dubbio il primo movimento nella storia trasferito in cyberspazio. Se dovessimo dire quale propriamente è il suo "luogo", questo esiste in senso virtuale. Dai loro nascondigli segreti, con i loro laptop e i dvd i militanti giovani del network programmano le loro azioni, pianificano la loro strategia e, soprattutto, diffondono la predicazione contro l'Occidente e per la lotta armata. I militanti dipendono interamente da internet e dalla rete che consente loro un

digitale qaedista, lo spazio virtuale è cresciuto al punto che i contenuti online sono divenuti un catalizzatore di radicalizzazioni[9].

> "Pur non essendo l'unico fattore, la presenza di contenuti terroristici online si è rivelata un catalizzatore della radicalizzazione degli individui che può portare ad atti terroristici e, pertanto, ha gravi conseguenze negative per gli utilizzatori, i cittadini e la società in generale"[10].

Oggi, le organizzazioni terroristiche sfruttano l'„agevole accessibilità"[11] della rete per diffondere la propria narrazione con ogni strumento disponibile:

> "dalle riviste on-line a videogame", "dalle chat e messaggi semplicemente social o cifrati, a video o lungometraggi con immagini cruente e di ferocia: sgozzamenti, decapitazioni di civili e di militari infedeli", ma anche "video apparentemente educativi d'azione e coraggio con spaccati di vita" proposti come "modelli per ragazzi alla ricerca di esperienze forti ed eroiche"[12].

In questo modo, la narrativa jihadista ha costituito l'occasione per alimentare quella "islamizzazione del radicalismo autonomo" delle *banlieue* europee che, secondo Olivier Roy, sarebbe all'origine della trasformazione di giovani immigrati di seconda generazione in lupi solitari[13].

---

completo anonimato eliminando anche uno degli aspetti più pericolosi della loro attività: gli spostamenti»: cfr. **E. RUTIGLIANO**, *La nuova guerra e l'Occidente*, in *Quaderni di sociologia*, n. 39 del 2005, pp. 5-20.

[9] La dimensione della crescita delle interazioni digitali, siano esse lecite e illecite, è dimostrata dal dato secondo cui ogni minuto sono postati circa 350.000 tweet, 510 commenti su Facebook, caricate 300 ore di video su YouTube, pubblicate 136.000 foto e 293.000 aggiornamenti di stato. In proposito, si veda **S. MACDONALD, S. CORREJA, A. WATKIN**, *Regulating terrorist content*, cit., p. 184.

[10] Regolamento (UE) 2021/784, considerando n. 5.

[11] Laura Martucci ha mutuato l'espressione "agevole accessibilità" da una pronuncia del Tribunale di Bari: cfr. **L.S. MARTUCCI**, *Terrorismo e contro-narrativa: i contenuti laici della deradicalizzazione*, in F. ALICINO (a cura di), *Terrorismo di ispirazione religiosa. Prevenzione e deradicalizzazione nello Stato laico*, Editrice APES, Roma, 2019, p. 316. Sul punto, cfr. altresì **A. VEDASCHI**, *Sicurezza e diritti nella digital age. La tecnologia: un'arma a doppio taglio nella lotta al terrorismo internazionale*, in *Scritti in onore di Mario G. Losano, Dalla filosofia del diritto alla comparazione giuridica*, Accademia University Press, Torino, 2021, pp. 521.

[12] **L.S. MARTUCCI**, *Terrorismo e contro-narrativa*, cit., p. 314 ss.

[13] Per un primo approfondimento cfr. **O. ROY**, *Generazione ISIS. Chi sono i giovani che scelgono il Califfato e perché combattono l'Occidente,* Editore Feltrinelli, 2017; cfr. altresì **ID:**,

> "Ammantata da riferimenti religiosamente e strumentalmente universali, l'infosfera islamista sfrutta le logiche e gli strumenti mediatici forniti dalla contemporaneità, raccogliendo consenso e adesione fra svariate sacche di disagio sociale, economico, politico o finanche personale e psichico"[14].

Per comprendere la pericolosità del fenomeno, è necessario tenere presente che, secondo il rapporto TE-SAT 2022 di Europol, la principale minaccia jihadista per l'Unione deriva, in buona parte, proprio dai *lone wolves*.

> "La minaccia del terrorismo jihadista nell'UE può concretizzarsi, con

---

Le djihadisme est un révolte générationnelle et nihiliste (in *https://lemonde.fr*) 30 novembre 2015, e **ID.**, *Who are the new jihadis?* (in *https://www.theguardian.com/*) 13 aprile 2017; *contra*, **G. KEPEL**, **A. JARDIN**, *Terreur dans l'Héxagone, génése du Djihad français*, Gallimard, Parigi, 2015; **G. KEPEL**, *La fracture,* Gallimard, Parigi, 2016; **ID.**, *La rivincita di Dio*, traduzione italiana di C. TORRE, Rizzoli, Milano, 1991; in sintesi, **L. CREMONESI**, *Gilles Kepel e Olivier Roy. A confronto i due maggiori esperti francesi di jihad*, in *Corriere della Sera*, 19 marzo 2017. Il dibattito francese sulla genesi della radicalizzazione islamista in Europa si caratterizza per il gradiente di posizioni espresse e classificabili in base al movente (cosiddetto) "determinante" politico, religioso, culturale, sociale o esistenziale. Le tesi che focalizzano l'attenzione sulla diffusione dell'islam salafita, sul jihadismo, sulla politica estera occidentale in Medio Oriente e sulle migrazioni, infatti, si distinguono da quelle che valorizzano, viceversa, il ruolo del cosiddetto determinante sociale. In quest'ultimo senso, Olivier Roy sostiene la tesi della "islamizzazione di un radicalismo autonomo", preesistente nei giovani immigrati di seconda generazione e originato dal disagio nihilista di una generazione destrutturata, marginalizzata e senza prospettiva. Per questi giovani, l'incontro (spesso solo digitale) con l'Islam è un mero pretesto che giustifica il compimento di una rivolta antieroica, individualista, apocalittica, e che sazia la sete personale e criminale di violenza e di martirio. Si contrappone alla tesi di Olivier Roy, Gilles Kepel, che sostiene la centralità del fattore religioso e, in particolare, della diffusione di degenerazioni radicalizzanti dell'Islam di stampo salafita. Per una sintesi efficace si veda **C. PATERNITI MARTELLO,** *Le radici della radicalizzazione nella riflessione della teorica francese*, in *Antigone. Rivista semestrale di critica del sistema penale e penitenziario*, n. 1 del 2017, pp. 57-61. Si vedano anche **M. VENTURA**, *Il loro Dio è la morte, non Allah. Terrore islamico a ritmo di rap*, in *Corriere della Sera*, 18 dicembre 2016, e **A. MELLONI**, *Il secondo miglio,* Fondazione Bruno Kessler, Special Editions, Trento, 2016, il quale ricorda come la discussione sia rimasta imprigionata nell'alternativa "fra la tesi di Olivier Roy (il terrorismo jihadista che ha percosso l'Europa è la islamizzazione di un nichilismo che esiste nella peggio gioventù emarginata nei tunnel della solitudine) e la tesi di Gilles Kepel (il terrorismo è un islam vero che ha subito dal 1980 in qua un processo di risemantizzazione del jihad). E ha spinto la discussione in un vicolo cieco securitario, che produce come effetti collaterali proprio i processi di emarginazione e di incubazione della violenza che voleva emarginare" (p. 13).

[14] **F. ALICINO**, *Introduzione*, in ID. (a cura di), *Terrorismo di ispirazione religiosa*, cit., p. 9 ss.

> maggiore probabilità, attraverso attacchi di individui che agiscono da soli. Come negli anni passati, i tre attacchi condotti nell'UE nel corso del 2021 sono stati perpetrati da attori solitari. Anche i piccoli gruppi rappresentano un rischio, data la facilità con cui possono formarsi e le difficoltà nell'individuarli e monitorarli. I gruppi terroristici hanno maggiori probabilità di essere individuati nella fase di pianificazione di un attacco, data la maggiore portata dell'organizzazione necessaria per coordinare un attacco più complesso"[15].

Molti dati, parallelamente, confermano la crescita esponenziale dell'islamismo digitale.

Prima del 2000, i siti jihadisti erano appena 12.

Nel 2005, erano circa 4500[16].

Nel 2014, solo su Twitter, c'erano più di 46.000 profili di supporter dello Stato islamico, con circa 1000 follower e una media di 7 tweet al giorno ciascuno[17].

---

[15] Nostra la traduzione. Il rapporto evidenzia altresì come "la minaccia del terrorismo jihadista nell'UE può concretizzarsi, con maggiore probabilità, con attacchi di individui che agiscono da soli. Come negli anni precedenti, i tre attacchi condotti nell'UE nel corso del 2021 sono stati perpetrati da attori solitari. Anche i piccoli gruppi rappresentano un rischio, data la facilità con cui possono formarsi e le difficoltà nell'individuarli e monitorarli. I gruppi terroristici hanno maggiori probabilità di essere individuati nella fase di pianificazione di un attacco, data la maggiore portata dell'organizzazione necessaria per coordinare un attacco più complesso. Nel 2021, in UE, sono stati registrati tre attacchi terroristici jihadisti, rispettivamente in Francia, Spagna e Germania. Otto attacchi sono stati sventati in sei Stati membri, mentre non si sono registrati attacchi falliti. Le accuse più comuni sono state quelle relative all'appartenenza a un'organizzazione terroristica, spesso in combinazione con la diffusione della propaganda o la pianificazione e la preparazione di un attacco. Tutti gli attacchi terroristici jihadisti portati a termine sono stati condotti da individui che agiscono da soli. Inoltre, gli Stati membri hanno condotto un numero significativo di indagini su persone sospettate di pianificare attacchi terroristici jihadisti": cfr. **EUROPOL**, *European Union Terrorism Situation and Trend report 2022 (TE-SAT)*, 2022, pp. 21 ss.

[16] Nel 2005, la dottrina sottolineava che «otto anni fa, secondo Gabriel Weimann, dell'Università di Haifa, i siti che diffondevano la jihad erano 12 mentre oggi sono 4500. "Questo mondo cibernetico, a parte la sua natura clandestina, è una rete non molto diversa dalle comunità virtuali di chi si dedica a giochi di ruolo, colleziona monete etc. […]. L'amorfa noncuranza di internet per i confini nazionali e per le connotazioni etniche si adatta perfettamente alla visione originale di Bin Laden e di al-Qaeda […]; i giovani jihadisti caricano in rete filmati che possono essere istantaneamente distribuiti a milioni di utenti" (Coll-Glasser, 2005, 13)". Inoltre, se qualcuno vuole compiere attentati, su questi siti può trovare quanto gli serve sapere»: cfr. **E. RUTIGLIANO**, *La nuova guerra*, cit., pp. 5-20.

[17] Cfr. **J.M. BERGER, J. MORGAN**, *The ISIS Twitter Census. Defining and describing the population of ISIS supporters on Twitter*, in *The Brookings Project on U.S. Relations with the*

Nel 2015, è iniziato l'esodo dei media e delle comunità jihadiste verso l'app di messaggistica Telegram[18].

> "Telegram è noto per essere la piattaforma preferita dalla messaggistica jihadista - e non a torto. Alla fine del 2015, lo Stato islamico (IS) ha trasferito l'intero apparato di distribuzione di media sulla piattaforma, con migliaia di suoi sostenitori che hanno seguito l'esempio. Non è stato il solo; poco dopo, altri gruppi come al-Qaeda hanno trasferito una significativa presenza su Telegram, e, nel 2018, anche gli estremisti di destra li hanno imitati"[19].

Nel 2019, un rapporto della George Washington University ha segnalato la presenza di circa 636 comunità (channels, groups e supergroups) pro-ISIS su Telegram, tra il 2017 e il 2018 e nella sola lingua inglese[20].

All'inizio del 2021, un report del Centre For Research And Evidence On Security Threats (CREST) ha analizzato un dataset contenente quasi otto milioni di contenuti jihadisti pubblicati su Telegram dal 2015. "Questo paper interroga un dataset contenente 7,8 milioni di post Telegram, provenienti da circa 1911 canali, gruppi e supergruppi […] affiliati con l'estremismo jihadista dal 2015 a oggi"[21].

Attualmente, Telegram è la piattaforma prediletta dal terrorismo (non solo islamista), nonostante gli esperimenti di migrazione verso il *decentralized web*[22] e la particolare efficacia dimostrata in passato dall'uso, a fini terroristici, di altre piattaforme quali Twitter, *archive.org* e *justpaste.*

Islamic World Analysis Paper, n. 20 del 2015.

[18] **P. KING,** *Islamic State group's experiments with the decentralized web*, in *Conference Paper for 3rd conference of the European Counter Terrorism Centre (ECTC) Advisory Network (EUROPOL)*, 9-10 aprile 2019, spiega così la transizione: "La resilienza è stata di sicuro un fattore nella decisione di spostarsi da Telegram a Twitter nel settembre 2015, ma fattori come la fruibilità, la sicurezza e la copertura potenziale sono stati egualmente importanti per l'IS, offrendo Telegram un'esperienza-utente e un pubblico di gran lunga superiori a qualsiasi altra piattaforma" (nostra la traduzione).

[19] Nostra la traduzione. Cfr. **A. AMARSAINGAM, S. MAHER, C. WINTER**, *How Telegram Disruption Impacts Jihadist Platform Migration (Full Report)*, CREST, 2021, p. 8.

[20] Cfr. **B. CLIFFORD, H. POWELL**, E*ncrypted Extremism. Inside the English-Speaking Islamic State Ecosystem on Telegram*, in *George Washington University Program on Extremism*, 2019.

[21] Nostra la traduzione. Cfr. **A. AMARSAINGAM, S. MAHER, C. WINTER**, *How Telegram Disruption*, cit., p. 12.

[22] **P. KING,** *Islamic State group's experiments*, cit., sostiene che "sebbene operatori di media dell'IS hanno dimostrato che le piattaforme decentralizzate possono giocare un ruolo nella distribuzione di contenuti jihadisti, al momento non stanno migrando via da

> "Ad oggi, Telegram resta il più importante hub online per la comunicazione ufficiale e non ufficiale jihadista e la distribuzione di contenuti [...] L'ecosistema di piattaforme utilizzate a questo scopo è più diversificato che mai, ma allo stesso tempo - e in qualche modo paradossalmente - rimane concentrato su Telegram"[23].

Inoltre, a dispetto della disfatta dello Stato islamico, la cui nascita aveva condotto a una significativa inflazione della comunicazione digitale jihadista, si è osservato che "resta viva l'azione di reclutamento" e, "anzi, la presenza di gruppi terroristici sul *web*, impegnati nell'opera di radicalizzazione, ha addirittura registrato un aumento"[24].

Con questi numeri, la digitalizzazione del terrorismo islamista rappresenta uno dei fenomeni più preoccupanti in materia di sicurezza e, al contempo, fornisce una ulteriore occasione di limitazione della libertà religiosa (e di manifestazione del pensiero).

3 - Libertà religiosa e modelli securitari

L'evoluzione digitale del terrorismo jihadista e, più in generale, la moltiplicazione del numero, delle forme e dell'entità dei rischi connessi all'evoluzione digitale del terrorismo di ispirazione religiosa ripropongono e complicano il grande tema del bilanciamento tra sicurezza e libertà di religione.

Telegram in gran numero. I fattori che potrebbero far pendere l'ago della bilancia includono l'introduzione da parte di Telegram di un processo automatizzato che rimuova i contenuti jihadisti in modo più sistematico o nuove piattaforme […] è possibile che la prossima piattaforma a essere sfruttata in modo così aggressive dai jihadisti non sia ancora emersa" (nostra la traduzione).

[23] Nostra la traduzione. Gli autori osservano che «in realtà, dal 2016, le piattaforme mainstream come Twitter e Facebook sono diventate inospitali per i jihadisti, la qual cosa ha costretto questi ultimi a migrare verso altri spazi online meno regolati rispetto alla distribuzione dei contenuti e alla comunicazione. Il più importante tra questi "altri" spazi è Telegram, una piattaforma ibrida di comunicazione e hosting di contenuti favorita da una vasta gamma di attori politici, *che spaziano dalla estrema destra europea agli attivisti* pro-democrazia di Iran e Hong Kong. Telegram, tuttavia, è rinomata per essere la piattaforma scelta dalla comunicazione jihadista e non a torto. Alla fine del 2015, lo Stato islamico (IS) ha trasferito l'intero apparato di distribuzione di media sulla piattaforma, con il seguito di migliaia di supporter. Vieppiù, poco dopo, altri gruppi come al-Qaeda hanno stabilito su Telegram una presenza significativa, seguiti nel 2018 anche dagli estremisti di destra» (nostra la traduzione): cfr. **A**. **AMARSAINGAM, S. MAHER, C. WINTER**, *How Telegram Disruption*, cit., pp. 8-15.

[24] Così **A. VEDASCHI**, *Sicurezza e diritti*, cit., p. 523 ss.

A livello globale competono due differenti approcci di politica securitaria, quindi due differenti modelli di regolamentazione delle interazioni tra diritto alla sicurezza e diritto alla libertà di religione o convinzione: un modello "integrato" certamente più innovativo e complesso e un modello più tradizionale a carattere "restrittivo".

Il modello innovativo è stato promosso dall'Organizzazione per la sicurezza e la cooperazione in Europa fin dalle sue origini nell'Atto Finale di Helsinki (1975), sviluppato nel tempo[25] e fondato su alcune delle fonti internazionali-sovranazionali più autorevoli[26], e infine elaborato nella forma più articolata e compiuta proposta dalle Linee Guida 2019 su Libertà di religione o convinzione e sicurezza dell'Ufficio per le Istituzioni Democratiche e i Diritti Umani dell'OSCE.

A fondamento del modello OSCE-ODIHR, la nozione "integrata" della sicurezza (cosiddetta "comprehensive security"[27]) implica un approccio securitario di attuazione multilaterale e a finalità tendenzialmente preventiva finalizzato alla creazione delle condizioni per una sicurezza di lungo periodo tramite l'integrazione di tre dimensioni di sicurezza, *politico-militare*, *economico-ambientale* e *dimensione umana* ("human dimension"[28]).

A propria volta, la dimensione umana presuppone la complementarietà e l'interdipendenza tra difesa dei diritti umani ed esigenza securitaria. Con questa premessa, una adeguata protezione dei diritti umani e della libertà religiosa in particolare concorrono alla costruzione di una società democratica, in quanto condizione di una sicurezza *inclusiva*, *non discriminatoria*, di diritti e libertà fondamentali *indivisibili*[29], *sostenibile* nel lungo termine, non unilaterale-statuale ma di *collaborazione* tra Governi, comunità di religione e convinzione, istituzioni culturali, organizzazioni sociali e media[30].

Tuttavia, anche il modello securitario integrato ammette misure restrittive della libertà religiosa, a condizione che queste siano adottate e applicate conformemente ai principi di *legittimità*, *tipicità*, *necessità*,

---

[25] **OSCE**, *The OSCE Concept of Comprehensive and Co-operative Security*, cit.

[26] Articoli 3, 18 e 19 UDHR (1948), articolo 9 CEDU (1950), articoli 4, secondo comma, 18 e 19 ICCPR (1966), articoli 12 e 13 ACHR (1969), articolo 10 CDFUE (2007).

[27] **OSCE-ODIHR**, *Freedom of Religion or Belief and Security. Policy Guidance*, 2019, paragrafo 1.

[28] **OSCE-ODIHR**, *Freedom of Religion*, cit., introduzione e paragrafo 1.

[29] Cfr. articolo 5 Dichiarazione di Vienna (1993).

[30] **OSCE-ODIHR**, *Freedom of Religion*, cit., paragrafi 1 e 3.

proporzionalità, *non discriminazione*[31] che trovano fondamento nelle fonti di diritto internazionale e unionale[32] e perfezionati dalle Corti sovranazionali sui diritti umani[33].

Alternativo al modello integrato, il modello securitario restrittivo prevalso a partire dall'11 settembre 2001 negli anni della violenza religiosa internazionale, si contraddistingue per l'„approccio competitivo tra sicurezza e diritto alla libertà religiosa"[34], intesi come diritti conflittuali o addirittura inversamente proporzionali, e per misure di reazione e prevenzione del terrorismo religiosamente motivato a carattere unilaterale-statuale, di più rapida efficacia, ma forse di respiro più corto[35].

Questo tipo di risposta securitaria, produttiva di una "temporanea rottura della tutela delle libertà" e dell'„incremento di norme volte a garantire l'ordine pubblico e un maggior grado di sicurezza", troverebbe anche una "sponda europea" nella direttiva (UE) 2017/541 sulla lotta al terrorismo. Tramite questa direttiva, l'Unione europea invoca un'anticipazione della tutela penale (secondo lo schema dei reati di pericolo) 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»[36].

Alla progressiva anticipazione preventivo-securitaria dell'intervento statuale rispetto alla condotta lesiva, corrisponde un

---

[31] **OSCE-ODHIR**, *Freedom of Religion* , cit., paragrafo 2.

[32] Articoli 3, 18 e 19 e, in particolare, 29 UDHR (1948), articolo 9 e, in particolare, 9 secondo comma, CEDU (1950), articoli 4, secondo comma, 18 e 19 e, in particolare 18, terzo comma, e 19, terzo comma, ICCPR (1966), articoli 12 e 13 e, in particolare, 12, secondo comma, e 13, secondo comma, ACHR (1969), articoli 10 e, in particolare, 52 CDFUE (2007).

[33] Per un primo approfondimento, si rinvia alla giurisprudenza citata nel corpo note di **OSCE-ODHIR**, *Freedom of Religion* , cit., e, in particolare, a Corte EDU, *Wingrove contro Regno Unito* (25 novembre 1996), *Svyato-Mykhaylivska Parafiya contro Ucraina* (14 giugno 2007), *Gorzelik e altri contro Polonia* (17 febbraio 2004), *Hasan e Chaush contro Bulgaria* (26 ottobre 2000), *Kimlya e altri contro Russia* (1 ottobre 2009), *Testimoni di Geova di Mosca e altri contro Russia* (10 giugno 2010); *Sidiropoulos e altri contro Grecia* (1 luglio 1998), *Bessarabia contro Moldavia* (31 luglio 2008), *Izzettin Dogan contro Turchia* (26 aprile 2016), *Stomakhin contro Russia* (8 ottobre 2018).

[34] L'espressione è di **R. MAZZOLA,** *Recensione a G. FATTORI (a cura di), Libertà religiosa e sicurezza. prima traduzione delle Linee Guida OSCE 2019 su Libertà di religione o convinzione e sicurezza, Pacini Giuri dica, Pisa, 2021, pp. 304*, in *Diritto e Religioni*, n. 1 del 2021, p. 869.

[35] Per approfondire, cfr. **G. FATTORI**, *Le Linee Guida OSCE-ODIHR 2019,* cit., p. 291.

[36] Cfr. *amplius* **F. ALICINO**, *La dimensione politico-religiosa dell'infosfera islamista*, in ID. (a cura di), *Terrorismo di ispirazione religiosa* cit., pp. 104-105.

sempre maggiore indebolimento della tutela della libertà religiosa (e di manifestazione del pensiero).

Si pensi a quanto avviene, in ambito amministrativo, con le espulsioni dello straniero per motivi di sicurezza e tutela dell'ordine pubblico adottate dal Ministro dell'Interno ai sensi dell'articolo 3, comma primo, del d.l. n. 144 del 2005 e largamente impiegate della "minaccia terroristica di matrice islamica"[37]. L'espulsione dello straniero, nei cui confronti siano fondati i motivi per ritenere che la sua permanenza nel territorio italiano sia funzionale alle organizzazioni o attività terroristiche, è "atto rimesso all'organo di vertice del Ministero dell'Interno" e poiché "senz'altro" costituisce "espressione di esercizio di alta discrezionalità amministrativa"[38] lo stesso è soggetto al più ristretto sindacato estrinseco (del giudice amministrativo) sulla "adeguatezza della motivazione o […] del travisamento, illogicità o arbitrarietà"[39].

In tal modo, un atto formalmente amministrativo, ma "sostanzialmente afflittiv[o] come le misure penali" e prossimo alle "misure di prevenzione previste dal d.lgs. 159/200", incide su libertà fondamentali come quella religiosa e di manifestazione del pensiero.

A tale proposito, pur essendo incontestabile "la legittimità e l'opportunità di strumenti di carattere amministrativo volti alla tutela dell'ordine pubblico", deve rilevarsi che i presupposti applicativi risultano talmente vaghi da consentire "di disporre l'espulsione anche nei confronti

---

[37] **M. TRIMARCHI**, *Il diritto amministrativo*, in G. FATTORI (a cura di), *Libertà religiosa e sicurezza*, cit., pp. 65-94.

[38] Secondo un orientamento consolidato, da ultimo ribadito da TAR Lazio, sez. I, sent. n. 9455 del 2022.

[39] Cons. Stato, sez. VI, sent. n. 88 del 2006. Per un primo approfondimento cfr. **N. DURANTE**, *Espulsione dello straniero e disciplina della regolarizzazione*. Relazione resa alla sessione formativa per magistrati amministrativi sul tema "*Il diritto dell'immigrazione*", 28 novembre 2016, il quale osserva che «per quanto attiene all'espulsione disposta dal Ministro, si registra quindi un marcato arretramento della tutela, rispetto a quel che l'ordinamento appresta avverso l'espulsione disposta dal Prefetto ed allo stesso respingimento differito. Infatti, mentre l'emanazione di questi due ultimi provvedimenti restrittivi della libertà personale non priva lo straniero della piena titolarità di posizioni di diritto soggettivo, essendo rimesso al potere amministrativo solo "l'accertamento dei presupposti di fatto che legittimano la protezione, facendo uso di una mera discrezionalità tecnica", nei riguardi della prima misura espulsiva, egli può vantare esclusivamente posizioni di interesse legittimo, conculcabili dal potere esecutivo attraverso l'adozione di un atto che è "esercizio di alta discrezionalità amministrativa" e, come tale, è sottoposto a un controllo di legittimità "ristretto al vaglio estrinseco, in ordine alla mancanza di una motivazione adeguata o alla sussistenza di eventuali profili di travisamento, illogicità o arbitrarietà"».

di persone che si limitano esprimere un parere o aderiscono a una associazione o frequentano determinati luoghi"[40].

Analogamente, in ambito penale si è assistito alla "punizione di condotte più prossime all'esercizio delle libertà fondamentali […] che a veri propositi eversivi"[41] e all'inevitabile collisione di queste politiche incriminatrici con i principi di materialità e di offensività del diritto penale[42].

È il caso, ad esempio, dei delitti di istigazione e apologia terroristica, commessi mediante la diffusione di contenuti a carattere islamista tramite piattaforme social o sistemi di messaggistica, o del delitto di associazione terroristica nella sua declinazione partecipativa come integrata dalla "sistematica reiterazione - da parte di chi intrattenga contatti […] con componenti o con soggetti comunque riconducibili, anche in via mediata, al sodalizio - di atti di indottrinamento, proselitismo e propaganda apologetica rivolti a terzi"[43], ma anche dell'addestramento e dell'autoaddestramento online[44].

---

[40] **M. TRIMARCHI**, *Il diritto amministrativo*, cit., pp. 65-94.

[41] **F. ALICINO**, *Introduzione*, cit., p.3-4.

[42] La dottrina, che ha sollevato dubbi di legittimità costituzionale per violazione del principio di offensività, ritiene che esso possa dirsi rispettato al ricorrere di talune condizioni: a) la tutela, da parte della norma incriminatrice, di un bene giuridico di rilevanza costituzionale di pari rango; b) una tecnica legislativa di costruzione della fattispecie incriminatrice in grado di veicolare il disvalore attraverso previsi elementi descrittivi della pericolosità della condotta o della peculiare intensità del dolo; c) un trattamento sanzionatorio proporzionato. Si veda **G. SALCUNI**, *Il diritto penale*, in G. FATTORI (a cura di), *Libertà religiosa e sicurezza*, cit., p. 119.

[43] Cfr. Cass. pen., sent. n. 17079 del 2022. In proposito, si veda altresì la precedente Cass. pen., sent. n. 2442 del 2020. Per un primo approfondimento, si vedano **G. SALCUNI**, *Il diritto penale*, cit., p. 115 e **N. COLAIANNI**, *Il disagio della libertà*, in F. ALICINO (a cura di), *Terrorismo di ispirazione religiosa*, cit., pp. 34 ss.

[44] Cfr. **F. ALICINO**, *La dimensione politico-religiosa*, cit., pp. 104-105. Quanto all'addestramento online, l'Autore ricorda che "la normativa europea afferma che "dell'atto di ricevere un addestramento a fini terroristici integra il reato esistente consistente nell'impartire addestramento e, in particolare, risponde alle minacce derivanti da coloro che preparano attivamente la commissione di reati di terrorismo, compresi coloro che in ultima istanza agiscono da soli. L'atto di ricevere addestramento a fini terroristici comprende l'acquisizione di conoscenze, documentazione o abilità pratiche. L'autoapprendimento, anche attraverso Internet o la consultazione di altro materiale didattico, dovrebbe altresì essere considerata ricevere addestramento a fini terroristici qualora derivi da una condotta attiva e sia effettuato con l'intento di commettere o di contribuire a commettere un reato di terrorismo. Nel contesto di tutte le circostanze specifiche del caso, tale intenzione può essere dedotta ad esempio dal tipo di materiale consultato e dalla frequenza della consultazione". In ambito nazionale, in relazione al

In questi casi, l'elemento tecnologico si "inserisce nel già complesso rapporto tra sicurezza e diritti" e complica la "relazione tra libertà personali e (restrizioni necessarie in ragione della) sicurezza nazionale"[45]. Su questo terreno, l'evoluzione digitale del terrorismo jihadista incrocia l'esercizio della libertà di professione, propaganda e proselitismo religioso in forma pubblica (esercitata in spazi digitali aperti) e in forma privata (esercitata in spazi digitali chiusi).

Da un lato, infatti, la giurisprudenza di legittimità ritiene pacificamente che "l'attività di proselitismo, fondata su ragioni di carattere etnico o religioso" possa "essere effettuata mediante i canali telematici"; tra questi ultimi, essa annovera proprio i social network, come Facebook, "attraverso cui si mantengono i contatti tra gli aderenti o i simpatizzanti […] mediante la diffusione di documenti e testi apologetici"[46].

Dall'altro, al contempo, si ritiene sufficiente a integrare il reato di apologia riguardante delitti di terrorismo la

> "condotta di chi condivide su social network link a materiale 'jihadista' di propaganda, senza pubblicarli in via autonoma, ovvero diffonde documenti di contenuto apologetico mediante il loro inserimento su piattaforme Internet (come Twitter e WhatsApp)"[47].

La dottrina più attenta ha sottolineato l'accortezza con cui la giurisprudenza di legittimità evita la repressione di "mere posizioni ideologiche". Tuttavia, è evidente che la distinzione tra attività lecite e illecite di proselitismo o indottrinamento comporta ampi margini di discrezionalità interpretativa, non esclude l'arbitrio e, pertanto, espone al "rischio di invadere il campo delle libertà, e di quella religiosa in particolare, e di comprimerlo oltre misura"[48].

---

delitto di cui all'art. 270 quinquies cod. pen., la giurisprudenza di legittimità conferma la rilevanza penale di condotte criminose "realizzate attraverso l'acquisizione dal web di materiale contenente istruzioni sul come e dove perpetrare attacchi terroristici e sulle tecniche di fabbricazione di bombe, sulle tecniche di guerriglia, di addestramento all'uso delle armi, e su tutte le altre attività connesse alla jihad, nonché sulla trasmissione di detto materiale per via telematica agli account di posta elettronica in uso a determinate persone facenti parte del circuito relazionale radicale": cfr. Cass. pen., sez. I, sent. n. 15089 del 2019.

[45] Cfr. *amplius* **A. VEDASCHI**, *Sicurezza e diritti*, cit., pp. 518-537.

[46] Cass. pen., sent. n. 24103 del 2017, che richiama le precedenti pronunce n. 33179 del 2013 e n. 8296 del 2004.

[47] Cass. pen., sent. n. 17079 del 2022.

[48] **N. COLAIANNI**, *Il disagio della libertà*, cit., p. 34 ss. Quanto alla giurisprudenza richiamata dall'Autore, si veda Cass. pen., sent. n. 48001 del 2016 e n. 30824 del 2006.

A questi rischi, tradizionalmente connessi all'adozione di misure restrittive, si aggiungono anche quelli derivanti dall'aggiornamento della strategia di contrasto alla minaccia terroristica in ambito digitale. Come negli Stati Uniti, anche in Europa si è infatti gradualmente affermato un modello "misto", basato sulla cooperazione pubblico-privata, che introduce nuove criticità nel bilanciamento tra libertà religiosa e sicurezza.

4 - La strategia europea di contrasto e il modello di public-private cooperation and co-optation

Da oltre dieci anni la progressiva infiltrazione islamista nello spazio virtuale europeo ha determinato una corrispondente espansione della strategia antiterroristica dell'Unione, con l'obiettivo di impedire la propaganda, la radicalizzazione, il reclutamento e l'addestramento online[49].

Di recente, il legislatore europeo è intervenuto con l'approvazione del regolamento (UE) 2021/784, che, all'articolo 3, introduce l'ordine di rimozione con cui l'autorità competente individuata dallo Stato membro obbliga il fornitore di servizi digitali a rimuovere o disabilitare l'accesso al contenuto, entro il più breve tempo possibile e comunque non oltre un'ora dal ricevimento del provvedimento stesso (*notice and take down*)[50]. "La rimozione immediata di contenuto terroristico è cruciale per impedire che

[49] La strategia antiterrorismo UE opera, sin dal 2005, su quattro fronti, ossia la "prevenzione, protezione, perseguimento e risposta". Già nel 2010, la Commissione riconosce l'importanza di contrastare le minacce provenienti da Internet. Sul punto cfr. **COMMISSIONE EUROPEA**, *Comunicazione della Commissione al Parlamento europeo e al Consiglio. La politica antiterorrismo dell'UE: principali risultati e sfide future*, Bruxelles, 20 luglio 2010, e **L.S. MARTUCCI**, *Terrorismo e contro-narrativa*, cit., p. 307 ss..

[50] Il modello del regolamento (UE) 2021/784 non sembra discostarsi significativamente dall'ordine di rimozione italiano, previsto dal d.l. 18 febbraio 2015, n. 7; tuttavia, l'ordine europeo ha il pregio di estendere l'efficacia "geografica" del provvedimento e di accelerare la rimozione, così da rendere prontamente inaccessibile il contenuto al pubblico europeo. Quanto alla analoga misura italiana, emanata nell'ambito della lotta al terrorismo, ci limitiamo a ricordare come essa preveda che l'A.G. può emanare un provvedimento che ordina: a) inibizione dell'accesso dei siti; b) di rimozione del contenuto illecito o c) di interdizione dell'accesso al dominio internet (oltre che l'istituzione di una black list, a cura del Ministero dell'Interno, di siti web utilizzati per le attività e le condotte di cui agli articoli 270-bis e 270-sexies cod. pen.).

i terroristi sfruttino Internet per reclutare, incoraggiare attacchi, addestrare e glorificare i loro crimini"[51].

Il regolamento non si occupa solo di armonizzare la procedura e gli obblighi che discendono dagli ordini di rimozione[52], ma persegue anche l'obiettivo di garantirne l'effettività e l'immediatezza attraverso l'obbligo, per i prestatori, di individuare un punto di contatto infra-europeo per la ricezione dei provvedimenti[53] o di nominare un rappresentante legale, per il caso in cui lo stabilimento principale sia fuori dall'Unione; questi sono ritenuti responsabili per le violazioni del regolamento[54]. Viene inoltre prevista una sanzione pecuniaria che può arrivare fino al quattro percento del fatturato mondiale del prestatore[55].

La misura arricchisce il quadro della strategia digitale dell'Unione che, oltre a contare su dinamiche cooperative giudiziarie e di polizia, dal 2010 ha previsto la promozione di un "approccio fondato sul partenariato fra settore pubblico e privato per contrastare l'uso di Internet a fini terroristici", consistente nell'istaurazione di "un dialogo fra autorità di contrasto e provider di servizi Internet per ridurre la diffusione sul web di contenuti illegali di stampo terroristico"[56].

Poiché è più semplice "regolare il proprietario o l'operatore dell'infrastruttura [digitale] che regolare e individuare i singoli utenti" [57],

---

[51] Cfr. **COMMISSIONE EUROPEA**, *Security Union: Rules on removing terrorist content online become applicable (Press Release)*, 7 giugno 2022 (nostra la traduzione)..

[52] Cfr. Regolamento (UE) 2021/784, considerando n. 17.

[53] Regolamento (UE) 2021/784, art. 15.

[54] Regolamento (UE) 2021/784, art. 17.

[55] Regolamento (UE) 2021/784, art. 18.

[56] Dal 2010, la Commissione europea, nell'ambito della strategia antiterrorismo e, segnatamente, del pilastro della prevenzione, ha dichiarato di promuovere un "approccio fondato sul partenariato fra settore pubblico e privato per contrastare l'uso di Internet a fini terroristici", avviando "un dialogo fra autorità di contrasto e provider di servizi Internet per ridurre la diffusione sul web di contenuti illegali di stampo terroristico. È anche in corso di elaborazione un modello di accordo europeo per facilitare la cooperazione in materia fra il pubblico e il privato": cfr. **COMMISSIONE EUROPEA**, *Comunicazione della Commissione al Parlamento europeo e al Consiglio. La politica antiterorrismo dell'UE: principali risultati e sfide future, Bruxelles*, 20 luglio 2010; cfr. altresì considerando n. 6, regolamento (UE) 2021/784 nel quale si afferma che "gli sforzi volti a contrastare i contenuti terroristici online, sono stati avviati a livello dell'Unione nel 2015 nel quadro della cooperazione volontaria tra gli Stati membri e i prestatori di servizi di hosting".

[57] Si è osservato, infatti, come sia più semplice "per gli Stati, regolare il gestore o il proprietario della infrastruttura piuttosto che regolare e individuare i singoli utenti. Essi infatti sono troppi, spesso anonimi o neanche umani, difficili da rintracciare o addirittura

troppi e spesso anonimi, dal 2015 sono stati avviati sforzi diretti a potenziare la cooperazione volontaria tra gli Stati membri e i prestatori di servizi di hosting[58].

Ciò è testimoniato dallo stesso regolamento, laddove si conferma che il contrasto ai contenuti terroristici online "richiede una combinazione di misure legislative, non legislative e volontarie basate sulla collaborazione tra le autorità e i servizi di hosting, nel pieno rispetto dei diritto fondamentali"[59].

Si tratta di un modello di matrice "euro-statunitense" ("*public-private cooperation and co-optation*"[60]) che affida "il compito di formulare le regole alle stesse imprese che gestiscono i servizi digitali", delega loro "il potere di occuparsi di quella zona di rete in cui si riversa parte della vita di ognuno di noi"[61] e favorisce una forma di controllo e censura privata che, in alcuni casi, può spingersi sino al tentativo di "affermare un pensiero standardizzato"[62].

In passato, questo approccio è stato duramente criticato dall'EDRi (European Digital Rights): l'associazione che tutela i diritti digitali, infatti, ha denunciato i rischi connessi alla scelta di mettere i "giganti di internet nella posizione di censurare l'Europa" senza passare dallo scrutinio

---

risiedenti fuori dalla giurisdizione nazionale": cfr. **J.M. BALKIN**, *Free speech is a triangle*, in *Columbia Law Review*, vol. 118 del 2018, p. 2020 (nostra la traduzione,).

[58] Regolamento (UE) 2021/784, considerando n. 6.

[59] Regolamento (UE) 2021/784, considerando n. 3.

[60] L'espressione è di **J.M. BALKIN,** *Free Speech in the Algorithmic Society*, University of California, Davis, 2018, p. 1179 ss.

[61] **S. FLAMINIO**, *Lotta alle fake news: dallo stato dell'arte a una prospettiva di regolamentazione per il "vivere digitale" a margine del Digital Services Act*, in *Rivista italiana di informatica e diritto*, n. 2 del 2022, p. 76.

[62] Cfr. **S. FLAMINIO**, *Lotta alle fake news*, cit., pp. 75-94, e altresì **A. VEDASCHI**, *Sicurezza e diritti*, cit., che ricorda come la "rimozione di contenuti terroristici *online*" appaia "particolarmente delicata quando viene attuata in applicazione di schemi di cooperazione tra pubblico e privato funzionanti su base volontaria e informale", fornendo gli esempi del Global Internet Forum to Counter Terrorism e dell'EU Internet Forum. Il riferimento è a "schemi di cooperazione volontaria di cui fanno parte i maggiori operatori della tecnologia e, nel caso dell'EU Internet Forum, anche soggetti pubblici, quali rappresentanti degli Stati membri dell'Unione europea ed Europol, che si impegnano congiuntamente a porre in essere strategia di controllo e rimozione dei contenuti *web*" (p. 532); l'Autrice richiama, a tale proposito, anche **C. GRAZIANI**, *Removing Terrorist Content Online: Pubblic-Private Cooperation and the Challenges of Technology from a Multilevel Perspective*, in A. VEDASCHI, K.L. SCHEPPELE (a cura di), *9/11 and the Rise of Global Anti-Terrorism Law: How the Security Council Rules the World*, Cambridge University Press, Cambridge, 2021.

democratico e giudiziario. Delegare l'attività di controllo e censura ad attori privati, infatti, equivale a spogliare le libertà delle garanzie parlamentari, amministrative e giudiziarie, sostituendole con oscuri *interna corporis* aziendali e indecifrabili algoritmi[63].

> "La Commissione Europea sta provocando una forma di censura 'volontaria' da parte dei giganti di internet per evitare una legislazione che sarebbe soggetta al controllo democratico e giudiziario [...] istituzionalizza[ndo] un ruolo per Facebook e Google nella regolazione della libertà di parola degli europei"[64].

Per costringere le piattaforme digitali ad adottare *policies* più stringenti, secondo EDRi[65], la Commissione si è avvalsa della "minaccia" dell'uso dello strumento legislativo, veicolata attraverso una pluralità di atti a efficacia indiretta o di *soft law*, come la raccomandazione sulle misure per contrastare efficacemente i contenuti illegali online[66], lo EU Internet Forum, il Codice di condotta del 2016 per contrastare l'illecito incitamento all'odio online, la direttiva sul contrasto al terrorismo[67], la direttiva sui servizi di media audiovisivi[68], il regolamento che istituisce Europol[69], la

---

[63] **A. VEDASCHI,** *Sicurezza e diritti*, cit., p. 529-530, sintetizza efficacemente le fasi del procedimento di rimozione algoritmico: "gli algoritmi […] vengono direttamente elaborati dalle medesime piattaforme digitali gestite dalle grandi società tecnologiche, il che comporta non trascurabili problemi […] gli strumenti di *machine learning* utilizzati dalle piattaforme servono, in primo luogo, ad individuare (*flag*) i contenuti (potenzialmente) terroristici. Successivamente, la piattaforma digitale procede alla (eventuale) rimozione in ottemperanza delle proprie *policies* interne. Questa azione va necessariamente coordinata con quella delle autorità di *law enforcement*, che devono essere messe in grado di agire concretamente, *ex post*, in via repressiva […] in alternativa, le medesime autorità […] possono entrare in gioco *ex ante* cioè in via preventiva, segnalando contenuti illeciti alle piattaforme digitali, affinché queste procedano alla rimozione (*notice and take down*)" ma "nella prima situazione, è il soggetto privato che si trova […] a identificare (e quindi a decidere quale sia) il messaggio radicalizzante".

[64] Cfr. **EDRI**, *EU Commission's Recommendation: Let's put internet giants in charge of censoring Europe*, 1 marzo 2018 (nostra la traduzione).

[65] «La Commissione europea si è concentrata molto sull'uso della "minaccia" della legislazione per costringere le società di Internet a mettere in campo attività di regolazione su base "volontaria"»: cfr. **EDRI**, *EU Commission's Recommendation: Let's put internet giants in charge of censoring Europe*, 1° marzo 2018 (nostra la traduzione).

[66] Raccomandazione (UE) 2018/334.

[67] Direttiva (UE) 2017/541.

[68] Direttiva (UE) 2018/1808.

[69] Regolamento (UE) 2016/794.

riforma del copyright, la comunicazione sui contenuti illegali online[70] e il Codice di condotta sulla disinformazione 2022.

5 - I rischi della gestione intermediata dei diritti fondamentali in rete

La rivoluzione digitale e la nascita della "società dell'algoritmo"[71] hanno complicato il bilanciamento tra sicurezza e libertà da un duplice punto di vista[72]. Da un lato, l'assenza di una giurisdizione universale e le vulnerabilità informatiche degli Stati hanno favorito la proliferazione di contenuti digitali illeciti. Dall'altro, la scelta di "blandire o costringere i proprietari di infrastrutture private [Big Tech] a eseguire gli ordini e aiutare nella sorveglianza e nella regolazione" ha esposto gli utenti al rischio di gravi violazioni dei diritti fondamentali, privandoli delle tutele che accompagnano l'esercizio dei poteri pubblici[73].

La prassi scaturita dall'autoregolamentazione delle piattaforme, infatti, impiega strumenti "para-sanzionatori che legittimano […] a eliminare contenuti, sospendere le attività di un soggetto o eliminarne l'account" e che possono concretamente "incidere sulla libertà di espressione" fino a produrre "forme di *censura privata*" che hanno attirato "il biasimo della dottrina"[74]. I poteri censori dell'intermediario digitale,

---

[70] **COMMISSIONE EUROPEA**, *Tackling Illegal Content Online Towards an enhanced responsibility of online platforms*, 28 settembre 2017.

[71] L'espressione "società dell'algoritmo" è largamente utilizzata in dottrina. Cfr. **J.M. BALKIN**, *Free Speech*, cit.

[72] Secondo **A. VEDASCHI,** *Sicurezza e diritti*, cit., pp. 518-537, l'elemento tecnologico «si inserisce dunque nel già complesso rapporto tra sicurezza e diritti, facendo sì che esso perda la sua "biunivocità e si trasformi in una relazione a tre fattori" e complica la "già delicata relazione tra libertà personali e (restrizioni necessarie in ragione della) sicurezza nazionale" che, sin dal settembre 2001, non è "più impostata secondo il classico schema di regola-eccezione». Peraltro, secondo l'Autrice, "l'ambiguità del fattore tecnologico" emerge anche dalla circostanza che, spesso, gli strumenti di contrasto coincidono con quelli utilizzati dai terroristi, come chiarito dall'ONU nell'ambito del documento *The use of the Internet for Terrorist Purposes*, pubblicato nel 2012.

[73] **J.M. BALKIN**, *Free Speech*, cit., p. 2019.

[74] L'Autore osserva come «tali sistemi punitivi, pur incidendo su un ambito che sovente viene ricondotto alla libertà contrattuale, non sono rimasti esenti da critiche, specie con riguardo all'impatto che gli standard delle community hanno sul rispetto del diritto all'eguaglianza, della libertà di parola, nonché sullo stesso "diritto" all'accesso a Internet, che meriterebbero una più approfondita analisi da parte degli ordinamenti statali. Infatti, va sottolineato che la delega quasi totale che gli Stati sembrano aver concesso alle big tech per individuare, normare, punire, reprimere e impedire

infatti, sono formalmente legittimati dall'adesione dell'utente-consumatore al regolamento e alle condizioni generali di contratto imposte per l'accesso al servizio, in cambio, peraltro, della corresponsione di un prezzo o della cessione di dati personali (poi commercializzati)[75].

La giurisprudenza, oltre a confermare la validità di queste clausole di autotutela inserite attraverso il richiamo a *standard* o *policies* della piattaforma, ne esclude la natura vessatoria, in quanto non riguarderebbero un servizio essenziale, anche se ammette che "l'esercizio in concreto di tali poteri non deve sfociare in comportamenti apertamente violativi della sfera di libertà espressiva che, dietro concessione dell'autorizzazione all'uso di propri dati sensibili e non gratuitamente,

---

comportamenti inappropriati sul Web è foriera di evidenti ripercussioni negative sul campo del diritto, in quanto rischia di far abdicare dal potere di regolamentare e accertare gli illeciti l'unico soggetto legittimato a farlo veramente (lo Stato). È del tutto evidente, infatti, che la libertà contrattuale dei colossi di Internet deve pur sempre rispettare i limiti imposti dalle fonti normative primarie di un ordinamento. Nondimeno, si consideri anche che la stessa attività di accertamento delle possibili condotte vietate dagli standard di un social network non è affidata a soggetti terzi e imparziali, ma a privati o ad algoritmi dal funzionamento spesso singolare e (forse) pericoloso. Tali problematiche non sono di importanza trascurabile, dato che spesso hanno indotto la stessa giurisprudenza a prendere posizione per ristabilire un equilibrio tra soggetto regolatore e singoli utenti. Tra questi, meritano una breve parentesi alcuni episodi del recente passato»: cfr. **S. FLAMINIO**, *Lotta alle fake news*, cit., p. 76, e gli Autori menzionati dallo stesso, tra cui è opportuno ricordare almeno **S. RODOTÀ,** *Nota di Stefano Rodotà per le audizioni sui disegni di legge sull'accesso a Internet presso la Commissione Affari costituzionali del Senato* (in *https://www.senato.it*), **G. PITRUZZELLA**, *La libertà di informazione nell'era di Internet,* in *MediaLaws,* n. 1 del 2018, pp. 18-47; **ID.**, *Il web ha bisogno di regole non di "censura privata"*, in *Corriere della Sera*, 8 novembre 2019, e **G.L. CONTI**, *Manifestazione del pensiero attraverso la rete e trasformazione della libertà di espressione: c'è ancora da ballare per strada?*, in *Rivista AIC*, n. 4 del 2018, pp. 209-216.

[75] Questa cessione di dati personali, secondo la giurisprudenza, ha carattere economicamente valutabile (cosiddetta patrimonializzazione del dato personale) ed è dunque qualificabile come prestazione ai sensi dell'art. 1174 cod. civ, come confermato (peraltro) dalla direttiva (UE) 2019/770, nella parte in cui sancisce che la "presente direttiva si applica altresì nel caso in cui l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico, fatto salvo il caso in cui i dati personali forniti dal consumatore siano trattati esclusivamente dall'operatore economico ai fini della fornitura del contenuto digitale o del servizio digitale a norma della presente direttiva o per consentire l'assolvimento degli obblighi di legge cui è soggetto l'operatore economico e quest'ultimo non tratti tali dati per scopi diversi da quelli previsti".

costituisce il contenuto tipico e, per così dire, la ragion d'essere dell'adesione ad una piattaforma di questo tipo"[76].

Si realizza così una gestione intermediata (o *private governance*) della libertà di espressione, che, sguarniti gli utenti delle garanzie che normalmente presidiano il rapporto tra l'azione amministrativa o penale e i diritti fondamentali, può essere occasione per una attività di censura altrimenti illegittima.

Sul piano individuale, chi assuma violati i propri diritti fondamentali non potrà contare sulla terzietà e sulla effettività dei sistemi di reclamo delle piattaforme: piuttosto, egli si troverà a dover promuovere un'azione civile, con tutto ciò che ne deriva sotto il profilo dell'effettività di una tutela destinata a spiegare i propri effetti (spesso) a distanza di tempo e solo in forma risarcitoria, senza la concreta capacità di contrastare e impedire la reiterazione della lesione e a patto di dimostrare l'esistenza del danno conseguenza derivante dalla lesione del diritto fondamentale.

Sul piano meta-individuale, invece, la concentrazione di questi poteri nelle mani di pochi intermediari digitali[77] produce un effetto collaterale sul "funzionamento dei processi democratici", con un cambio di paradigma della concezione della sfera pubblica in cui a "censori privati" è permesso "sopprimere arbitrariamente certi punti di vista senza che ai soggetti colpiti sia data la possibilità di una qualche forma [effettiva] di ricorso"[78], con ricadute significative sul diritto all'informazione e, più in generale, sui processi democratici ed elettorali[79], poiché "la sfera pubblica è il luogo dove si realizzano i valori della libertà

---

[76] C. App. L'Aquila, sent. n. 1676 del 2021; cfr. altresì TAR Lazio, sez. 1ª, sent. n. 260 del 2020, Cons. Stato, sez. 6ª, sent. n. 2631 del 2021. Inoltre, la giurisprudenza ha riconosciuto il risarcimento del danno non patrimoniale da inadempimento contrattuale (per la grave lesione di diritti fondamentali della persona, di manifesta rilevanza costituzionale) del gestore di un social network, che abbia rimosso senza una valida motivazione l'account di un utente e distrutto tutti i suoi dati: cfr. Trib. Bologna, sez. II, ordinanza 10 marzo 2021.

[77] Di "eccessivo potere conferito alle piattaforme digitali" parla, tra i molti, anche **S. FLAMINIO**, *Lotta alle fake news*, cit., p. 76.

[78] **L. BRANDIMARTE, L. PECCHI, G. PIGA**, *Le imprese Big Tech: schiave delle leggi per poter essere liberi?*, in *Diritto pubblico*, n. 3 del 2021, p. 827.

[79] È ormai nota l'interferenza sulla sfera pubblica derivante da tecniche insidiose, basate sul *profiling* e sul *recommender system* algoritmico, che sono tese a massimizzare i profitti delle aziende. Senza pretese esaustive, ricordiamo le bolle di filtraggio, le *eco-chambers*, il *targeted advertising* e, più in generale, la manipolazione dell'informazione e dei feed degli utenti anche a scopi elettorali, come dimostra il caso di Facebook-Cambridge Analytica o quello, più recente, dei Twitter Files di Elon Musk.

di parola e di espressione. La libertà di parola è alla base della partecipazione democratica che contribuisce alla formazione dell'opinione pubblica"[80].

La materia è tanto delicata che, già in passato, si è ritenuta indispensabile la predisposizione di idonee garanzie giurisdizionali al fine di evitare la

> "attività di censura o di imbavagliamento" e la "illegittima compressione della stessa libertà di espressione [che è un] diritto consacrato non solo a livello costituzionale dall'art. 21 cost., ma anche dalle fonti sovranazionali all'art. 19 della Dichiarazione universale dei diritti dell'uomo e all'art. 10 CEDU"[81].

Considerato che i provider di servizi digitali "possono imporre regole più restrittive dello Stato", alcuni hanno sperato nel correttivo derivante dal pluralismo delle piattaforme, che dovrebbe garantire "le diverse sensibilità, culture e credi che sono presenti in una società ideale"; tuttavia, i cinque giganti statunitensi (Google, Amazon, Facebook, Apple e Microsoft) hanno un valore economico di oltre nove trilioni di dollari e cioè "più dell'intero mercato azionario europeo (Regno Unito e Svizzera inclusi)" e continuano ad acquisire realtà promettenti (si veda il caso di WhatsApp e Instagram) con effetti che conducono "automaticamente al monopolio, o al più, all'oligopolio"[82].

C'è, poi, l'annosa questione della irresponsabilità degli intermediari digitali per i contenuti pubblicati dagli utenti o terze parti (con l'omologo dibattito statunitense sulla *Section-230* del *Communications Decency Act* del 1996)[83].

---

[80] **L. BRANDIMARTE, L. PECCHI, G. PIGA**, *Le imprese Big Tech*, cit., p. 826.

[81] **S. SIGNORATO**, *Le misure di contrasto in rete al terrorismo*, in R.E. KOSTORIS, F. VIGANÒ (a cura di), *Il nuovo pacchetto antiterrorismo*, Giappichelli, Torino, 2015, p. 62. Sul punto, si veda altresì **A. VEDASCHI,** *Sicurezza e diritti*, cit., p. 533-534, che parla di "limitazione di diritti fondamentali, primo fra tutti quello della libertà di espressione, a seguito della valutazione di un sistema algoritmico, e non di un procedimento giurisdizionale svoltosi in contraddittorio, o perlomeno, dell'intervento di un'autorità amministrativa che abbia i caratteri di indipendenza".

[82] **L. BRANDIMARTE, L. PECCHI, G. PIGA**, *Le imprese Big Tech*, cit., pp. 811-826.

[83] Di recente, la stampa internazionale ha rilanciato la notizia del caso *Gonzalez v. Google*, attualmente pendente davanti alla Corte suprema degli Stati Uniti e avente a oggetto la *Section 230* del *Communications Decency Act*. La vicenda trae origine dall'accusa rivolta dalla famiglia di una vittima americana degli attentati di Parigi contro YouTube, ritenuta responsabile di aver promosso contenuti Isis che avrebbero "indirettamente causato la morte della figlia". Sebbene, come si apprende dai giornali, i giudici avrebbero mostrato perplessità «riguardo all'argomentazione secondo la quale YouTube dovrebbe

L'esclusione dei gestori di servizi digitali dal novero degli editori[84] e la mancata previsione di un obbligo generale di sorveglianza attiva sui contenuti[85] ha consentito lo sviluppo di un settore indispensabile per l'innovazione, sgravandolo di conseguenze giuridico-tecniche che ne avrebbero pregiudicata (o addirittura impedita) l'economicità. Tuttavia, questa forma di immunità è sostenibile nella sola misura in cui l'intermediario mantenga la propria neutralità, rinunciando a compiere scelte "editoriali" sui contenuti e garantendo l'eguale fruibilità di un servizio che, forse, è divenuto essenziale per il corretto funzionamento della democrazia.

L'urgenza del dibattito sulla disciplina delle piattaforme digitali è rappresentata plasticamente dal recentissimo *affaire* Twitter.

---

essere ritenuta responsabile per il modo in cui il suo algoritmo "ha gestito" i contenuti dell'Isis», essi avrebbero anche considerato la possibilità di una distinzione tra «hosting (il semplice atto di "ospitare" post o video) e amplificazione dei contenuti, e l'eventualità di lasciare che sia il Congresso a dirimere la controversia». Nel corso dell'udienza, peraltro, il giudice progressista Ketanji Brown Jackson ha suggerito che la Section 230 "non avrebbe mai avuto lo scopo di fare scudo alle piattaforme tecnologiche dalle cause", provocando la reazione dell'avvocato di Google che ha sostenuto come "Internet non sarebbe mai decollata […] se qualcuno avesse potuto fare causa in qualsiasi momento". Tra i molti, cfr. **M. CATUCCI**, *Alla Corte suprema un caso che può rivoluzionare il web*, in *Il Manifesto*, 22 febbraio 2023. Si segnala che una distinzione (per certi versi) analoga a quella tra 'ospitare e amplificare' è presente anche nella giurisprudenza italiana. La Corte di cassazione, infatti, ha ritenuto sussistente la responsabilità per concorso in diffamazione aggravata del titolare di un blog che non rimuova i contenuti diffamatori pubblicati dagli utenti: in particolare, ribadita la non estensibilità degli obblighi di garanzia previsti in capo all'editore per i contenuti pubblicati, il Giudice ha ritenuto la colpevolezza del titolare del blog per la (diversa) condotta attiva consistita nella "consapevole condivisione del contenuto diffamatorio" realizzata "mediante il mantenimento consapevole sul blog" che equivarrebbe ad "adesione volontaria […] con l'effetto a questo punto voluto di consentirne l'ulteriore divulgazione". Cfr. *ex multis* Cass., sez. V, sent. n. 2386 del 2022.

[84] A tal proposito, **S. FLAMINIO,** *Lotta alle fake news*, cit., p. 76, osserva che "pur potendosi prospettare soluzioni giuridiche simili a quelle generalmente applicate nell'editoria, il mondo occidentale ha scelto un'altra strada, spesso generando anche insanabili contraddizioni tra il dato letterale delle norme e gli esiti dei procedimenti giudiziari. Un esempio di tale discrasia è quello per cui, mentre da un lato si prevede che una piattaforma digitale svolte un'attività esente da responsabilità per mancato controllo dei contenuti, ampia giurisprudenza considera le condotte diffamatorie degli utenti come illeciti commessi *con mezzo della stampa o con altro mezzo di pubblicità*".

[85] Cfr. direttiva n. 2000/31/CE, come confermata dal DSA package, e d.lgs. n. 70 del 2013

In un contributo che ha preceduto di qualche giorno la notizia dell'interesse di Elon Musk per la proprietà del noto social statunitense[86], si è dato atto delle dichiarazioni del magnate che descrivevano la piattaforma digitale alla stregua di una piazza pubblica e invocavano retoricamente il rispetto della libertà di espressione online al fine di garantire il corretto funzionamento della democrazia.

> "Il free speech è essenziale per il funzionamento della democrazia. Credete che Twitter aderisca in modo rigoroso a questo principio? / Poiché Twitter funge come una piazza pubblica de facto, la mancata adesione al principio della libertà di espressione mina la democrazia alle fondamenta. Che cosa dovrebbe essere fatto?".

Acquisita la proprietà del social, Elon Musk ha promosso una campagna denominata "*The Twitter Files*", consistente nella pubblicazione di documenti interni dell'azienda che dimostrerebbero: a) l'arbitraria censura di notizie di pubblico rilievo, anche durante l'ultima campagna elettorale per l'elezione del Presidente degli Stati Uniti D'America; b) la rimozione o la revisione di contenuti e notizie non illeciti o illegali, su richiesta di parti politiche e di agenzie federali; c) l'utilizzo sistematico di *shadowban*, un meccanismo consistente nella restrizione arbitraria e non denunciata della visibilità degli utenti, in base alle opinioni espresse dagli stessi[87].

In apparenza, la strategia del nuovo "*Chief Twit*" sembra inseguire il sogno di una "piazza comune digitale", ritenuta fondamentale per il futuro della civiltà[88]; tuttavia, sarà il tempo a dimostrare la bontà del

---

[86] Cfr. **A. CASIERE**, *Libertà e sicurezza. L'„era dell'insicurezza digitale" ci espone anche al rischio di una private governance della libertà di espressione e di religione*, in *Portale I.S.I. Pacini Giuridica*, 11 aprile 2022.

[87] Il 3 e il 9 dicembre 2022, Elon Musk ha pubblicato dei *thread*, su Twitter, in collaborazione con due diversi giornalisti, dal titolo "*The Twitter files*" e "*The Twitter files part two*". È emerso, peraltro, che James Baker, ex agente dell'FBI e deputy general counsel di Twitter, ha manipolato alcuni documenti oggetto della divulgazione voluta dal magnate di Tesla. A seguito di questa vicenda, Baker è stato licenziato. Per approfondire è possibile consultare il profilo Twitter di Elon Musk. In breve, cfr. **AGENZIA ANSA**, *Musk, Twitter cancellerà presto 1,5 mld account inattivi da anni. Posta nuovi 'Twitter files', 'blacklist e post oscurati'*, 9 dicembre 2022.

[88] **AGENZIA AGI**, *Per Elon Musk, Twitter dovrebbe essere più inclusivo possibile* (*www.agi.it*), 25 ottobre 2022. Alcune ore dopo l'iconico ingresso nell'HQ di Twitter con un lavandino tra le braccia ("*let that sink-in*!"), Musk ha dichiarato in un Tweet che la ragione per cui ha acquistato il social è che "it is important to the future of civilization to have a common digital town square, where a wide range of beliefs can be debated in a healthy manner, without resorting to violence. There is currently great danger that social

progetto dell'imprenditore che, giova ricordarlo, ha interessi fortemente radicati nel settore delle tecnologie, dell'intelligenza artificiale (il cui sviluppo si nutre di dati) e dell'integrazione neurale uomo-macchina[89].

La "*public town square*" (o *public sphere*[90]) menzionata da Elon Musk è oggi una "*digital public sphere*"[91], in cui gli utenti esercitano delle facoltà intimamente connesse alle libertà fondamentali e al principio democratico e che sono esposte al rischio di oscure decisioni di piattaforme e algoritmi[92].

È stato ricordato come il giudice della Corte Suprema Anthony Kennedy abbia, per primo, descritto la rete quale "moderna piazza pubblica", nonché come il luogo più importante per lo scambio di opinioni; ciò ha condotto, nel caso *Packingham v. North Carolina* (2017), a ritenere l'incostituzionalità, per violazione del Primo Emendamento, di una legge che negava *tout-court* l'utilizzo di social media a una categoria di condannati[93].

---

media will splinter into far-right wing and far left-wing echo chambers that generate more hate and divide our society. […] I did it to try to help humanity, whom I love".

[89] Per un approfondimento sulle implicazioni giuridiche degli investimenti di Elon Musk, si legga **P. ANNICCHINO**, *Il dibattito sui neurodiritti e il transumanesimo di Musk*, in *Il Domani* (*https://editorialedomani.it*), 3 dicembre 2022.

[90] **M.N. SINGH**, *Jurgen Habermas's Notion Of The Public Sphere: A Perspective On The Conceptual Transformations In His Thought*, in *The Indian Journal of Political Science*, n.4 del 2012, pp. 633-42.

[91] L'espressione è mutuata da **J.M. BALKIN**, *Free Speech*, cit., p. 2012. Luca Vanoni scrive invece che "nei secoli passata, la concezione di *public square* (o *space*) è stata centrale per definire I confine fisici in cui il dibattito politico e democratico ha luogo"; tuttavia, prosegue l'Autore, "le nuove tecnologie stanno digitalizzando la tradizionale *public square*, non solo attraverso la sostituzione della stessa con i social network, ma anche ridefinendo il perimetro dei luoghi tradizionalmente istituzionali" (nostra la traduzione): cfr. **L.P. VANONI**, *Dematerializing the traditional public square: new challenges for religious freedom?*, in L.P. VANONI, A. CESARINI, F. COLOMBO, A. NEGRI, T. PAGOTTO, G. PAVESI, G. RAGONE., *The spatial ramifications of religion: new and traditional legal challenges*, in *Stato, Chiese e pluralismo confessionale*, Rivista telematica (*https://www.statoechiese.it*), n. 21 del 2022, pp. 2-6.

[92] In particolare, come suggerisce **A. VEDASCHI**, *Sicurezza e diritti*, cit., p. 529-530, "gli algoritmi capaci di identificare questo tipo di messaggi vengono direttamente elaborati dalle medesime piattaforme digitali gestite dalle grandi società tecnologiche, il che comporta non trascurabili problemi sotto il profilo della trasparenza dei sistemi", poiché "i colossi tecnologici si trovano quindi a giocare un ruolo particolarmente rilevante, che implica un'imprescindibile cooperazione con le autorità pubbliche, al fine di prevenzione".

[93] Di un certo rilievo appare anche la *concurring opinion* redatta dal giudice Samuel A. Alito, Jr., il quale, in sintesi, sostiene che "L'opinione di maggioranza sbaglia

> «In Packingham v. North Carolina (2017), il giudice Kennedy definisce internet per la prima volta come "the modern public square"», argomentando che oggi "il cyberspazio in generale […] e i social media in particolare" sono "gli spazi più importanti per lo scambio di opinioni". Come riconosciuto dalla stessa Corte, questa affermazione solleva problemi sui 'limiti spaziali' delle leggi e dei principi stabiliti per garantire la libertà di espressione e di religione»[94].

Analogamente, il Tribunale di Roma ha paragonato Facebook a

> "una pubblica piazza, con le conseguenti ricadute che questo fatto ha su le libertà garantite in Costituzione" e che richiede una "speciale protezione [dell'utente] che non può che essere tutelata dallo Stato e dalle sue istituzioni"[95].

6 - Il Digital Services Act package: verso un nuovo modello?

---

nell'equiparare l'intero web al classico *public forum* e nel non riconoscere l'importanza di consentire agli Stati di regolamentare determinati tipi di siti web. Il Governo ha certamente l'interesse primario della protezione dei bambini da potenziali violenze sessuali e Internet è il luogo che consente ai molestatori di comunicare con i bambini in modi che altrimenti impossibili; perciò, il Governo dovrebbe poter limitare, in una certa misura, l'uso di Internet da parte di molestatori sessuali. E tuttavia, la legge della Carolina del Nord si è spinta troppo oltre, perché ha incluso siti web che difficilmente possono facilitare la commissione di una molestia sessuale su un bambino. Poiché la legge della Carolina del Nord ha limitato più del necessario la libertà di espressione, allora, essa ha violato il Primo Emendamento" (nostra la traduzione): cfr. **ISTITUTO OYEZ**, *Packingham v. North Carolina*, (liberamente consultabile su *https://www.oyez.org*).

[94] Cfr. **L.P. VANONI**, *Dematerializing the traditional public square*, cit., p. 6 ss. (nostra la traduzione).

[95] **S. FLAMINIO**, *Lotta alle fake news*, cit., p. 77. Per quanto riguarda le pronunce in commento, cfr. Trib. Roma, sez. spec. in materia di impresa, ord. 11 dicembre 2019, e Trib. Roma, sez. civ. XVII, ord. 29 aprile 2020. L'Autore, inoltre, dà atto della presenza di una sentenza di segno opposto, pronunciata dalla medesima autorità giudiziaria, "nella quale è stato affermato che Facebook non avrebbe soltanto la facoltà di rimuovere contenuti contrari alle sue condizioni contrattuali, bensì sarebbe gravata da un vero e proprio *dovere giuridico* di rimuovere i suddetti contenuti, in virtù di obblighi di diritto internazionale. Il contrasto giurisprudenziale è stato oggetto di una riflessione in dottrina" per dare atto della quale Sebastiano Flaminio richiama **C. CARUSO**, *I custodi di silicio. Protezione della democrazia e libertà di espressione nell'era dei social network*, in *Consulta Online*, *Liber Amicorum per Pasquale Costanzo*, 17 marzo 2020, e, *contra*, **M. BASSINI,** *Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione*, in *Rivista italiana di informatica e diritto*, n. 2 del 2021.

Nel dicembre 2020, la Commissione europea ha avviato l'iniziativa legislativa relativa al Digital Services Act package, un pacchetto normativo composto dal Digital Markets Act (DMA[96]) e dal Digital Services Act (DSA[97]), promosso per aggiornare e armonizzare il quadro normativo europeo relativo ai servizi digitali e contribuire al corretto funzionamento del mercato e alla tutela effettiva dei diritti fondamentali.

I due regolamenti sono stati approvati rispettivamente il 14 settembre e il 19 ottobre 2022 e prevedono diversi termini di efficacia iniziale: il DMA troverà applicazione a decorrere dal 2 maggio 2023[98]; il DSA, invece, troverà applicazione a decorrere dal 17 febbraio 2024[99].

La forte contrapposizione degli interessi in gioco ha avuto eco, da subito, nelle diverse reazioni di quanti hanno ritenuto eccessivi gli obblighi imposti dalla riforma e quanti, invece, avevano sperato in una maggiore tutela dei diritti fondamentali rispetto ai poteri degli intermediari digitali[100].

Pertanto, alla luce dell'importanza del Digital Services Act package, accenneremo ora ad alcuni aspetti che ci paiono conferenti rispetto al tema oggetto del presente contributo.

Il DMA o "regolamento sui mercati digitali", modificando le direttive (UE) 2019/1937 e 2020/1828, persegue l'obiettivo di assicurare l'equità e la contendibilità nei mercati del settore digitale in cui sono presenti gatekeeper (controllori dell'accesso)[101], a beneficio delle imprese più piccole e degli utenti finali (art. 1, par. 1).

---

[96] 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).

[97] 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).

[98] A eccezione di alcuni articoli che si applicano dal 1 novembre 2022 e di altri che si applicheranno a decorrere dal 25 giugno 2023. Cfr. articolo 54, Regolamento (UE) 2022/1925.

[99] A eccezione di alcuni articoli che si applicano dal 16 novembre 2022. Cfr. articolo 93, Regolamento (UE) 2022/2065.

[100] Sul punto cfr. **C. CAUFFMAN, C. GOANTA**, *A New Order: The Digital services Act and Consumer Protection*, in *European Journal of Risk Regulation (Cambridge University Press)*, n. 12 del 2021, p. 759.

[101] Si tratta degli intermediari digitali più grandi, che forniscono servizi di piattaforma di base (intermediazione online, motori di ricerca, social network, condivisione video, comunicazione, sistemi operativi, browser web, assistenti virtuali, cloud computing, servizi pubblicitari": cfr. artt. 1 e 2 Regolamento (UE) 2022/1925.

La lettura dei numerosi considerando, che introducono le disposizioni, chiarisce come lo spirito del regolamento sia quello di fronteggiare i gravi squilibri in termini di potere contrattuale, pratiche sleali e condizioni inique che danneggiano gli utenti commerciali e finali e che derivano, principalmente, dai condizionamenti imposti dal numero esiguo di (grandi) imprese che forniscono servizi di base ed esercitano un controllo su interi ecosistemi di piattaforme[102].

L'ambito applicativo (artt. 1 e 2) è limitato ai servizi forniti o offerti dai gatekeeper (artt. 2 e 3), ossia da quegli intermediari digitali la cui presenza online "è tanto dominante che gli stessi sono profondamente coinvolti nella vita quotidiana dell'utente" e ha «il tremendo potere di potere di "filtrare" i contenuti dalle imprese all'utente»[103].

Per ottenere il risultato sperato, il DMA prevede una procedura di designazione del gatekeeper, individua le pratiche sleali o che limitano la contendibilità e sancisce, a carico di questi, una serie di obblighi; inoltre, attribuisce poteri di controllo, indagine, esecuzione, sanzione e monitoraggio alla Commissione europea.

---

[102] Cfr. Regolamento (UE) 2022/1925, considerando nn. 3 e 4, in cui si legge che "è emerso un numero ridotto di grandi imprese che forniscono servizi di piattaforma di base dotate di considerevole potere economico che potrebbe qualificarle per essere designate come gatekeeper a norma del presente regolamento. Generalmente esse vantano una capacità di connettere molti utenti commerciali con molti utenti finali attraverso i loro servizi e ciò, a sua volta, consente loro di sfruttare i vantaggi acquisiti in un settore di attività, quali l'accesso a grandi quantità di dati, in un altro settore. Alcune di tali imprese esercitano un controllo su interi ecosistemi di piattaforme nell'economia digitale e per gli operatori di mercato esistenti o nuovi è estremamente difficile, a livello strutturale, sfidarle o contrastarle, indipendentemente dal livello di innovazione o efficienza di tali operatori di mercato. La contendibilità è ridotta in particolare a causa dell'esistenza di barriere molto alte all'ingresso o all'uscita, tra cui i costi di investimento elevati, che in caso di uscita non possono essere recuperati o possono essere recuperati con difficoltà, e l'assenza di alcuni input chiave nell'economia digitale, quali i dati, o l'accesso ridotto agli stessi. Cresce di conseguenza la probabilità che i mercati sottostanti non funzionino correttamente, o non siano in grado di farlo nell'immediato futuro. È probabile che la combinazione di tali caratteristiche del gatekeeper determini, in molti casi, squilibri gravi in termini di potere contrattuale e, di conseguenza, pratiche sleali e condizioni inique tanto per gli utenti commerciali quanto per gli utenti finali dei servizi di piattaforma di base forniti dai gatekeeper, a discapito dei prezzi, della qualità, della concorrenza leale, della scelta e dell'innovazione nel settore digitale".

[103] Cfr. **F. POP, J. BEZEMER, L. GRANT**, *The Digital Markets Act: more choice and improved data protection for users* (in *https://www.eipa.eu*), 19 agosto 2022; **ID.**, *The Digital Services Act: creating accountability for online platforms and protecting users' rights?* (in *https://www.eipa.eu*), 6 settembre 2022 (nostra la traduzione).

Se il regolamento riuscirà a centrare l'obiettivo di un mercato più equo, gli utenti avranno la possibilità di scegliere tra una pluralità di servizi; tuttavia, resta da verificare se essi potranno sottrarsi alle condizioni imposte dalle piattaforme più severe o, nel frattempo, anche i nuovi intermediari saranno raggiunti efficacemente dalle pressioni istituzionali[104].

Il DSA o "regolamento sui servizi digitali", modificando la direttiva (CE) 2000/31 (direttiva *e-commerce*), persegue l'obiettivo di contribuire al corretto funzionamento del mercato interno dei servizi intermediari, stabilendo norme armonizzate per un ambiente online sicuro, prevedibile e affidabile che faciliti l'innovazione e in cui i diritti fondamentali, compreso il principio della protezione dei consumatori, siano tutelati in modo effettivo (art. 1, par. 1).

L'atto è composto da novantatré articoli divisi in cinque capi che, a esclusione del primo (disposizioni generali) e del quinto (disposizioni finali), ribadiscono l'esonero di responsabilità degli intermediari digitali (artt. 4-10), impongono obblighi di *due diligence* (artt. 11-48) e, infine, prevedono norme di attuazione, cooperazione, sanzione ed esecuzione (artt. 49-88).

Infatti, se da un lato il regolamento ribadisce il principio della generale irresponsabilità degli intermediari per i contenuti online ospitati o trasmessi e l'assenza di obblighi di sorveglianza e accertamento attivo (artt. 4-8), nel tentativo di bilanciare questo regime di favore prevede o armonizza gli ordini di contrastare i contenuti illegali e di fornire informazioni emanati dalle autorità[105] (artt. 9 e 10) e, soprattutto, impone obblighi (societari) di cosiddetta *due diligence* (capo terzo), che dovrebbero garantire la sicurezza e l'equità dei (e nei) servizi digitali[106], specie con riguardo ad alcune categorie di rischi menzionati dai considerando nn. 3 e 4 e dagli artt. 34 e 35.

I destinatari degli obblighi devono dunque valutare e attenuare quattro categorie di rischi sistemici: *a*) quelli associati alla diffusione di contenuti illegali; *b)* quelli collegati agli effetti (reali o prevedibili) sull'esercizio dei diritti fondamentali, incluse la dignità umana, la libertà

---

[104] **F. POP, J. BEZEMER, L. GRANT**, *The Digital Markets Act*, cit.

[105] Previsti rispettivamente agli artt. 9 e 10 sono rivolti dalle competenti autorità degli Stati membri agli intermediari e sono analoghi a quello previsto dal regolamento (UE) 2021/784 relativo al contrasto della diffusione di contenuti terroristici online .

[106] Per un primo approfondimento sul tema, si veda **M. HUSOVEC, I.R. LAGUNA**, *Digital Services Act: A Short Primer* (*https://private-law-theory.org/?p=44753*), 18 luglio 2022.

di espressione e informazione, la libertà e il pluralismo dei media, il diritto alla vita privata, la protezione dei dati, il diritto alla non discriminazione; *c*) i rischi derivanti dagli effetti negativi (reali o prevedibili) sui processi democratici, sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica e, infine, *d*) i rischi per la salute pubblica derivante dall'uso di piattaforme e motori di ricerca di dimensioni molto grandi.

Com'è evidente, nel regolamento trovano spazio due diversi interessi, contrapposti sul piano pratico: quello di "ampliare ulteriormente la tutela dei diritti fondamentali nella sfera privata delle infrastrutture di Big Tech" e quello "di promuovere la competizione, l'innovazione e lo sviluppo economico"[107].

Questa sintesi è stata ritenuta ambigua da quanti hanno segnalato il rischio di mettere le piattaforme nella "non invidiabile posizione di dover risolvere autonomamente il problema", producendo "approcci incoerenti tra le piattaforme, a una iper-regolazione dei contenuti, con tutto ciò che comporta per i diritti umani"[108].

Secondo altri, invece, la disciplina risultante dal combinato degli obblighi di *due diligence* e dalle disposizioni che promuovono l'equità e la contendibilità nei mercati digitali renderebbe il DSA package "assai vicino all'obiettivo di superare i problemi della censura privata e del ripianamento del dislivello contrattuale tra le parti"[109].

7 - Conclusioni

È indubbio che l'ordine materiale si collochi tra le cause efficienti e finali dell'ordinamento[110], nella misura in cui si occupa di assicurare la pacifica

---

[107] A ben vedere, infatti, gli ordini di rimozione e gli obblighi di *due diligence* rispondo all'interesse della tutela dei diritti fondamentali e del principio democratico, mentre con l'esonero da responsabilità per i contenuti di terze parti e l'assenza di un obbligo generale di sorveglianza o accertamento attivo rispondono agli interessi di tutela della libertà di iniziativa economica e dello sviluppo tecnologico ed economico (**C. CAUFFMAN, C. GOANTA**, *A New Order*, cit., p. 759; nostra la traduzione).

[108] **K. PENTNEY**, *The DSA, due diligence & disinformation: a disjointed approach or a riscky compromise?*, in *TechReg CHRONICLE*, dicembre 2022.

[109] **S. FLAMINIO,** *Lotta alle fake* news, cit., p. 79.

[110] Una parte significativa della dottrina rifiuta la costruzione di un "diritto (soggettivo) alla sicurezza", tenendo salda la distinzione tra funzioni dell'ordinamento e diritti soggettivi: in accordo con la giurisprudenza costituzionale, infatti, si parla esclusivamente di "funzione di sicurezza" pubblica o di "interesse collettivo alla sicurezza". Cfr. **A. PACE**, *La sicurezza pubblica*, cit., p. 1-2. Per un primo approfondimento

convivenza che è essenziale per il godimento dei diritti e delle libertà e per la sopravvivenza dell'ordinamento stesso.

Ciononostante, lo sforzo richiesto per il presidio della sicurezza non può che passare attraverso l'attuazione di regole e principi costituzionali che delimitano lo spazio di legittimità dell'azione pubblica e privata, specie in una esperienza costituzionale rigida, formale e che non prevede alcuno stato d'eccezione, come è quella italiana.

Detto altrimenti, il fine politico-securitario non giustifica per sé stesso il mezzo, in quanto l'atto del potere costituente ha scelto di tradurre in principi dei valori che fungono da parametri di legittimità delle modalità attuative dei fini, al punto da circoscrivere persino l'esercizio della sovranità alle forme e ai limiti previsti dalla Costituzione[111].

Roberto Mazzola, nel 2005, ha giustamente osservato che "la domanda di sicurezza dei cittadini non può trovare soddisfazione e risposta se non nella politica di tutela dei diritti fondamentali e nello sviluppo dei rapporti economico-sociali", come testimoniato dal fatto che la Costituzione preveda, all'articolo 2, la tutela dei diritti inviolabili dell'uomo e che la Repubblica italiana abbia sin da subito aderito a

---

sul significato di "sicurezza" e sulla natura di diritto soggettivo o interesse collettivo, cfr. **A. VEDASCHI**, *Sicurezza e diritti*, cit., p. 519 ss.; In proposito, si legga altresì **N. COLAIANNI**, *Il disagio della libertà*, in F. ALICINO (a cura di), *Terrorismo di ispirazione religiosa*, cit., p. 18 ss. **A. NEGRI**, *Radicalizzazione religiosa*, cit., p. 38 ss., invece, ricorda, come l'ordinato vivere civile sia un fine ineludibile dello Stato, poiché i consociati ambiscono naturalmente all'ordinato vivere civile, quale indubbia "meta dello Stato di diritto, libero e democratico", che "consente il libero godimento dei diritti".

[111] In questo senso, sono significative le parole di **A. BARAK**, *Radicalizzazione religiosa*, cit., p. 47, secondo cui "è questo il destino della democrazia, perché non tutti i mezzi sono accettabili in democrazia e non tutte le pratiche attuate dai suoi nemici possono essere utilizzate. Sebbene una democrazia debba spesso combattere con una mano legata, avrà comunque l'altra a sua disposizione. Il mantenimento dello Stato di diritto e il riconoscimento della libertà del singolo […] sono questi gli elementi che rinsaldano lo spirito e la forza della democrazia e le consento di superare le difficoltà", come citato *sub nota* 159 in **A. NEGRI**, *Radicalizzazione religiosa*, cit.. Parimenti significative sono le parole di **G. CASUSCELLI**, *Una disciplina-quadro delle libertà di religione: perché, oggi più di prima, urge "provare e riprovare" a mettere al sicuro la pace religiosa*, Stato, Chiese e pluralismo confessionale, cit., n. 26 del 2017, pp. 5-6, il quale tra i «"macro fenomeni" di vaste dimensioni che hanno suscitato prima e alimentato poi, considerati ognuno a sé stante e ancora di più nel reciproco combinarsi, la "paura della libertà religiosa"» pensa anzitutto «all'ansia accresciuta per la sicurezza, al clima di sospetto e al suo portato di richieste rinnovate di discipline limitative delle libertà fondamentali, spinte talora sino alla soglia di illiberali compressioni, al fine di contrastare con misure efficaci l'emergenza del terrorismo internazionale, anche al prezzo di giungere alle soglie di una "democrazia autoritaria"».

Convenzioni (CEDU e Patto internazionale sui diritti civili e politici) che prevedono limitazioni delle libertà fondamentali solo se "funzionali alla prevenzione dei reati, alla protezione della salute e della morale pubblica, nonché alla tutela dei diritti e delle libertà altrui"[112].

Ciò detto, come si possono coniugare la sicurezza, le libertà di religione e di espressione e il principio democratico nell'era digitale?

Mentre si sostiene che la sicurezza è un interesse collettivo, al contempo si riconosce anche che "i diritti inviolabili non [sono] mai affermati in termini assoluti", in quanto essi sono inseriti "in una complessa trama costituzionale in cui la loro portata può essere limitata da altri diritti e interessi tutelati" tra cui, certamente, l'interesse alla sicurezza. Tanto è vero che, si è detto, "la sicurezza può essere motivo di limitazione dei diritti, ma al tempo stesso, questi ultimi fungono da invalicabile argine contro derive securitarie" e, soprattutto, che "tutelare la sicurezza dei diritti significa infatti tutelare la possibilità di godere delle libertà garantite costituzionalmente e, di riflesso, lo sviluppo della persona umana e della sua dignità"[113].

Sul piano teorico, dunque, la dimensione umana della "sicurezza integrata" OSCE consente di ricomporre la tensione, attraverso l'integrazione della tutela dei diritti umani: non può esserci sicurezza che non garantisce anche le libertà fondamentali; dunque, la sicurezza è anche "sicurezza della libertà".

Va ricercato, allora, quel "ragionevole compromesso" che garantisce al contempo "l'ordine pubblico e la sicurezza contro forme di eversione tanto imprevedibili quanto devastanti" e "i diritti fondamentali di tutte le persone"[114].

Questa prospettiva è astrattamente condivisa dall'Unione europea nel regolamento (UE) 2021/784, nella parte in cui si sostiene che

---

[112] **R. MAZZOLA**, *La convivenza delle regole. Diritto, sicurezza e organizzazioni religiose*, Giuffrè, Milano, 2005, p. 12.

[113] **A. NEGRI**, *Radicalizzazione religiosa*, cit., p. 42 ss., nel ricordare che l'ordinato vivere civile è un "fine ineludibile" dell'ordinamento in quanto "consente il libero godimento dei diritti" e, dunque, che «lo scopo della "sicurezza dei diritti"» è di "garantire il libero esercizio di questi", sostiene che questa «è una ricostruzione non lontana da quella di "sicurezza integrata" proposta dalle recenti Linee guida dell'OSCE" tanto che "in particolare […] si legge che libertà di religione o convinzione - ma il discorso è ampliabile a ogni altro diritto soggettivo - e sicurezza "collaborano al rafforzamento di obiettivi che possono e devono essere perseguiti insieme"».

[114] **F. ALICINO**, *La dimensione politico-religiosa*, cit., pp. 109-111.

> "l'adozione di misure online efficaci per contrastare i contenuti terroristici online e la protezione della libertà di espressione e informazione non sono elementi contrastanti, bensì obiettivi complementari che si rafforzano a vicenda"[115].

Sul piano pratico, la soluzione è ben più complicata.
Si è detto, tradizionalmente, che

> "l'unica via ragionevole per uscire da questo intreccio" è "quella di vietare" o "limitare la libertà di espressione in generale o quella di espressione religiosa in particolare […] solo quando" queste realizzino "l'apologia di comportamenti" che "abbia la concreta capacità di provocare l'immediata esecuzione di delitti"[116].

Questo approccio, tuttavia, si adatta con difficoltà a un mondo, come quello digitale, in cui le minacce (e la possibilità che esse si traducano in delitti) si moltiplicano al punto da rendere impossibile una valutazione immediata e completa delle stesse.

Le soluzioni proposte riflettono il grado di sensibilità rispetto ai principi dello Stato di diritto e della democrazia liberale.

Fermo l'assetto delle garanzie costituzionali, i principi di ragionevolezza e proporzionalità sembrano offrire il migliore di bilanciamento tra esigenza securitaria e tutela libertaria.

In particolare, il principio generale di proporzionalità, coniato nel 1912 da Fritz Fleiner per il *Polizeirecht* e assunto trai i principi generali del diritto europeo[117], permette di individuare la regola migliore per la

---

[115] Regolamento (UE) 2021/784, considerando n. 10.

[116] **A. PACE**, *La sicurezza pubblica*, cit., p. 2 ss. In tal senso, disponeva altresì la direttiva (UE) 2017/541, che all'art. 5 imponeva un obbligo di incriminazione, a carico degli Stati nazionali, per la sola diffusione di contenuti che istigassero o promuovessero "il compimento di reati di terrorismo, creando in tal modo il pericolo che uno o più di tali reati possano essere commessi".

[117] Tanto con riguardo alla significativa giurisprudenza della Corte EDU, quanto con riguardo all'esplicita previsione del TUE e alla giurisprudenza della CGUE. Per un primo approfondimento sul principio di proporzionalità cfr. **D.U. GALETTA**, voce *Principio di proporzionalità [dir. amm.]*, in *Diritto Online*, Treccani, 2012, e **ID.**, *Il principio di proporzionalità fra diritto nazionale e diritto europeo (e con uno sguardo anche al di là dei confini dell'Unione Europea)*, in *Rivista italiana di diritto pubblico comunitario*, n. 6 del 2019, pp. 903-927; vi sarebbe, inoltre, già traccia di questo principio in **G.D. ROMAGNOSI**, *Principj fondamentali di diritto amministrativo onde tesserne le instituzioni*, 3ª ed., Stamperia Guasti, Prato, 1835, p. 15, laddove l'Autore sostiene che la regola direttrice dell'amministrazione pubblica nel caso del conflitto degli interessi del privato con quelli del pubblico sia *"far prevalere la cosa pubblica alla privata entro i limiti della vera necessità*. Lo che è sinonimo di *far prevalere la cosa pubblica alla privata col minimo possibile sacrificio della privata proprietà e libertà*. Qui la prevalenza della cosa pubblica alla privata non colpisce il fine o l'*effetto* ma

comparazione degli interessi in gioco, grazie allo stress test operato attraverso i corollari della idoneità (della misura adottata rispetto allo scopo da raggiungere), della necessarietà (o del minimo mezzo possibile) e della adeguatezza (o minor sacrificio possibile in relazione allo scopo).

L'applicazione di tale principio, anche in campo normativo, consente l'individuazione a priori di misure che, con il minimo sacrificio imposto dal raggiungimento dello scopo, ottengano al contempo di garantire la sicurezza attraverso limitazioni dei diritti strettamente proporzionate ai beni da tutelare.

Si tratta proprio dello stesso metodo richiamato dal regolamento (UE) 2021/784, nella parte in cui si dichiara che le autorità competenti e i prestatori di servizi di hosting "dovrebbero adottare solo le misure che sono necessarie, adeguate e proporzionate in una società democratica", alla luce della centralità della libertà di espressione e di informazione e del pluralismo dei media, "che costituiscono i fondamenti essenziali di una società pluralista e democratica, nonché valori su cui si fonda l'Unione"[118].

L'ordine di rimozione di contenuti illeciti, grazie al meccanismo di *notice and take down* affidato al controllo preventivo o alla convalida dell'autorità giudiziaria, mette al riparo dalla elusione delle garanzie costituzionali ed è conforme ai canoni della proporzionalità.

Restano, invece, le perplessità espresse in relazione all'obiettivo istituzionale di uno spazio digitale che si vorrebbe (addirittura) più sicuro, prevedibile e affidabile di quello tradizionale, al punto da delegare la gestione di una significativa porzione di sfera pubblica a società a dimensione (e con interessi) transnazionale.

Una simile scelta, invero, impone un ripensamento della "sicurezza della libertà", in modo che essa garantisca i diritti fondamentali non soltanto dal potere dello Stato, ma anche dallo strapotere di Big Tech.

---

il semplice *mezzo*".

[118] "Le misure che incidono sulla libertà di espressione e di informazione dovrebbero essere rigorosamente mirate a contrastare la diffusione di contenuti terroristici online, nel rispetto del diritto di ricevere e comunicare informazioni in modo lecito, tenuto conto del ruolo centrale dei prestatori di servizi di hosting nel facilitare il dibattito pubblico e la diffusione e la ricezione di informazioni, pareri e idee nel rispetto della legge": cfr. Regolamento (UE) 2021/784, considerando n. 10.