2024 NUMERO 67

Coscienza e Libertà

SEMESTRALE DI LIBERTÀ RELIGIOSA, LAICITÀ, DIRITTI DAL 1978

A. Casiere

Religione e sicurezza integrata

ISSN 0394-2732

D. Romano - M. Ventura - G. Fattori - D. Curtotti - P. Annicchino - V. Ricciuto - T.F. Giupponi
E. Gianfrancesco - G. Tropea - A. Vedaschi - I. Ruggiu - A. Pin - G. Corso - N. Marchei - F. Alicino
D. Milani - A. Casiere - I.A. Caggiano - P.B. Helzel - S. Amato - A. Benzo - S. Baldassarre

A brave new (digital) world. Tra terrorismo e autoritarismo digitale*

Andrea Casiere
Dottorando di ricerca, Università di Foggia

ABSTRACT
Negli ultimi vent'anni, il mondo ha sperimentato la tensione esistente tra sicurezza e libertà religiosa. La digitalizzazione jihadista ha messo in pericolo la sicurezza pubblica, mentre il duro approccio anti-terroristico ha messo in pericolo la *privacy*, la libertà di religione o convinzione e la libertà di espressione. Nel "mondo nuovo", le parole chiave dell'autoritarismo sono sorveglianza, propaganda, disinformazione e censura digitale.

SOMMARIO

1. *A brave new (digital) world*

Negli ultimi vent'anni, lo sviluppo della tecnologia digitale ha cambiato radicalmente la vita e la società a livello globale. Volendo esemplificare la portata di questa rivoluzione, è sufficiente ricordare che Internet ha progressivamente raggiunto il 60% della popolazione mondiale[1], garantendo l'accesso generalizzato all'informazione e alla comunicazione in tempo reale che ha «promosso la

* 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] Itu-Unesco Broadband Commission For Sustainable Development, *The State of Broadband 2022: Accelerating broadband for new realities*, settembre 2022, p. IX.

libertà di espressione, facilitato il dibattito globale e favorito la partecipazione democratica»[2]. All'opposto, le nuove tecnologie hanno accresciuto drammaticamente i rischi per i diritti fondamentali e la sicurezza pubblica, come dimostrano i casi, sempre più frequenti, di sorveglianza individuale o di massa, propaganda, disinformazione e censura[3].

Anche in questo campo, il rapporto tra religione e sicurezza è andato declinandosi secondo il modello antagonista inaugurato dall'«era dell'insicurezza»[4] post-9/11: mentre le organizzazioni jihadiste hanno sfruttato gli strumenti digitali per amplificare la propria attività di propaganda, radicalizzazione, addestramento e finanziamento, con gravi conseguenze per la sicurezza pubblica, i governi hanno reagito alla violenza religiosa promuovendo un uso della tecnologia digitale che ha messo in pericolo le libertà fondamentali. Proprio sul terreno della libertà religiosa o di convinzione, poi, la tecnologia digitale ha agevolato il controllo diffuso e la repressione di minoranze da parte di «attori statali e non statali»[5].

Il generico argomento della sicurezza nazionale, spesso sufficiente a legittimare la compressione di diritti fondamentali nella prospettiva della perdurante emergenza post-9/11, ha giocato un ruolo fondamentale nello sviluppo e nella legittimazione di tecnologie digitali: nel rapporto *Human rights implications of the development, use and transfer of new technologies in the context of*

[2] Nostra traduzione. Un Human Rights Council, *The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights (A/HRC/27/37)*, 18 luglio 2014, p. 3

[3] Cfr., *ex multis*, Un Human Rights Council, *Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Fionnuala Ní Aoláin (A/HRC/52/39)*, 1° marzo 2023, I. Yilmaz (a cura di), *Digital Authoritarianism and its Religious Legitimization. The Cases of Turkey, Indonesia, Malaysia, Pakistan and India*, Palgrave Macmillan, 2023; P. Annicchino, *Se la religione diventa un laboratorio per la sorveglianza digitale*, in Domani.it, 28 luglio 2021; P. Annicchino, *La minoranza musulmana e lo stato nazionale di sorveglianza cinese*, in *Coscienza e libertà*, fascicolo n. 63/64 del 2022.

[4] L'espressione è di G. Fattori, *Il Corso di Laurea in Scienze Giuridiche della Sicurezza dell'Università di Foggia*, in Id. (a cura di), *Libertà religiosa e sicurezza*, Pacini Giuridica, Pisa, 2021, p. 173.

[5] Cfr. P. Annicchino, *Comprehensive security and religion: moving away from the securitization zeitgeist in the digital transition*, in *The Review of Faith & International Affairs*, numero 4 del 2022, pp. 66, 67.

counter-terrorism and countering and preventing violent extremism del 1 marzo 2023, lo *Special Rapporteur* delle Nazioni Unite Fionnuala Ní Aoláin ha denunciato, con profonda preoccupazione, la «portata delle violazioni dei diritti umani causate dalla proliferazione e dall'abuso, a livello globale, di sofisticate e intrusive tecnologie di cyber-sorveglianza, inizialmente giustificate dalla lotta al terrorismo o da ragioni di sicurezza nazionale»[6].

La questione relativa all'ambiguità della tecnologia digitale, di difficile soluzione a causa dell'ampio spettro di diritti e interessi sul tappeto, è stata efficacemente inquadrata da Arianna Vedaschi: quando la tecnologia digitale «viene utilizzata per lo svolgimento di una qualche attività umana, la [sua] neutralità […] si "colora" di bianco (dimensione positiva) o di nero (dimensione negativa)»; tuttavia, «persino quando l'apparente neutralità si colora di bianco – il riferimento è alla dimensione positiva della tecnologia (ad esempio, quando viene asservita alla lotta al crimine e, precisamente, al counterterrorism) – si intravedono "zone d'ombra", giacché lo strumento tecnologico, impiegato per la tutela del diritto, rischia, sul piano pratico, di violare le libertà personali»[7].

E, in effetti, oltre che dalle organizzazioni terroristiche, il rischio può provenire anche da attori pubblici e privati, spesso coinvolti in forme di cooperazione più o meno trasparenti. Nel noto lavoro *Il capitalismo della sorveglianza*, Shoshana Zuboff ha evidenziato la forte interdipendenza maturata, a partire dal 9/11, tra agenzie di intelligence statunitensi e Google, allora capitalista della sorveglianza "alle prime armi": lo stato d'emergenza permanente, determinato dalla minaccia terroristica, e i limiti imposti dalle garanzie costituzionali all'azione di polizia hanno indotto i Governi ad affidarsi all'impresa privata «per raccogliere e generare informazioni»[8]. In una seconda fase, l'affermazione della sfera pubblica digitale (o digitalizzata), con infrastrutture fisiche e virtua-

[6] Nostra traduzione. Un Human Rights Council, *Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism*, cit., 1° marzo 2023.

[7] 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*, Accademia University Press, Torino, 2021, p. 521.

[8] Cfr. S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, Roma, 2019.

li nelle mani di intermediari privati, è stata all'origine delle pressioni istituzionali dirette a provocare un maggior impegno delle piattaforme digitali nel *law enforcement* online[9]; ne è conseguita l'informale attribuzione di «poteri quasi-normativi, quasi-esecutivi, quasi-giurisdizionali»[10] in capo agli attori privati impegnati nell'amministrazione di veri e propri feudi digitali (*Intermediaries' Private Orderings*)[11].

In questo "meraviglioso mondo nuovo"[12], dunque, c'è chi ritiene che la minaccia per le democrazie costituzionali «non viene più solo dall'autorità pubblica, ma anche e soprattutto da attori privati»[13], che sono in grado di incidere su un'ampia gamma di beni e interessi, costituzionalmente e convenzionalmente rilevanti; il rischio è esasperato dalla diffusione, su larga scala, di alcuni strumenti di intelligenza artificiale, come ricordato dal Vicepresidente degli Stati Uniti rilasciate in occasione dell'*AI Safety Summit* 2023 di Londra: «se le persone, in tutto il mondo, non riescono a distinguere i fatti dalla finzione a causa del flusso di cattiva informazione o disinformazione prodotta dall'intelligenza artificiale, non è questo un problema esistenziale per la democrazia?»[14].

[9] Cfr. L. Belli, C. Sappa, *The Intermediary Conundrum Cyber-Regulators, Cyber-Police or Both?*, liberamente consultabile su https://ssrn.com/abstract=3727905 2017, p. 184.

[10] Nostra traduzione. E. Marique, Y. Marique, *Sanctions On Digital Platforms : Balancing Proportionality In A Modern Public Square*, liberamente consultabile su https://ssrn.com/abstract=3462408 1 settembre 2019, p. 6.

[11] Cfr. L. Belli, C. Sappa, *The Intermediary Conundrum*, cit., p. 183.

[12] Dal titolo del celebre romanzo distopico *Brave New World* (Il mondo nuovo) di Aldous Huxley del 1931. Nel saggio *Ritorno al mondo nuovo* del 1958, l'autore profetizza che «nel futuro immediato, c'è motivo di credere che i metodi punitivi di 1984 cederanno alle induzioni, alle manipolazioni del Mondo nuovo». È interessante osservare che, nel paragrafo dedicato al ruolo della propaganda nella società democratica, lo scrittore inglese denuncia due forme speculari di controllo: «nei paesi totalitari d'Oriente c'è la censura politica, e i mezzi della comunicazione di massa sono controllati dallo Stato. Nelle democrazie d'Occidente c'è la censura economica e i mezzi di comunicazione di massa sono controllati dalla élite al potere. Certo, la censura che si esercita alzando i costi e concentrando i mezzi di comunicazione nelle mani di poche grosse imprese, è meno ripugnante della proprietà statale e della propaganda governativa; ma è sempre cosa che un democratico jeffersoniano non approverebbe» Cfr. A. Huxley, *Il mondo nuovo e Ritorno al mondo nuovo*, Mondadori, 2011, pp. 261-267.

[13] Nostra traduzione. Cfr. G. De Gregorio, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, Cambridge, 2022, p. 4.

[14] Nostra traduzione. *Remarks by Vice President Harris on the Future of Artificial Intelligence*, 1° novembre 2023.

Ecco, allora, che «neppure il diritto può dirsi immune dal paradosso della modernizzazione»[15]: l'abuso di tecnologie dal «potenziale catastrofico»[16], specie quando legittimato da esigenze securitarie, minaccia non solo i diritti fondamentali, ma l'equilibrio del rapporto tra autorità e libertà.

Ormai ad un passo da metaverso e intelligenza artificiale, proprio quando le istituzioni europee sembrano aver trovato l'intesa politica sull'atteso *AI Act*[17], il dibattito non può più essere rimandato: in questo senso, il PRA-HE *Religion and Comprehensive Security* (Re.Co.Se.), finanziato dall'Università di Foggia, ha rappresentato un'importante occasione di confronto su religione, libertà, sicurezza e innovazione, come dimostrano i contributi ospitati in questo numero di Coscienza e Libertà.

2. Tra propaganda jihadista on-line…

Nell'ambito del recente conflitto israelo-palestinese, è tornato alla ribalta "Letter to the American People" (2002) il documento-manifesto attribuito ad Osama bin Laden, nel quale il leader di al-Qaeda, alla domanda «Why are we fighting and opposing you?», rispondeva con una serie di accuse a partire da quella relativa all'occupazione della Palestina: «because you attacked us and continue to attack us. a) You attacked us in Palestine: (i) Palestine, which has sunk under military occupation for more than 80 years»[18]. Il documento, «misteriosamente fatto riapparire su TikTok» nei giorni della controffensiva israeliana a Gaza, ha ottenuto milioni di "ri-condivisioni" sul social, al punto che il quotidiano inglese *The Guardian* ha deciso di rimuoverne la traduzione ospitata online a partire dal 24 novembre 2002: la scelta di censurare un documento di indubbio valore storico, in quanto "privo di contesto", è stata criticata

[15] Cfr. G. Fattori, *Il Corso di Laurea in Scienze Giuridiche della Sicurezza*, cit., p. 168.

[16] Cfr. *The Bletchley Declaration by Countries Attending the AI Safety Summit*, 1-2 novembre 2023. Sul potenziale catastrofico dell'AI si è espresso anche Sam Altman, CEO di OpenAI, produttrice di ChatGPT, nel corso di un'audizione celebrata presso il Senato statunitense, cfr. The Washington Post, *CEO behind ChatGPT warns Congress AI could cause "harm to the world"*, liberamente consultabile su www.washingtonpost.com, 16 maggio 2023.

[17] Agenzia Reuters, *Europe agrees landmark AI regulation deal*, liberamente consultabile su www.reuters.com, 11 dicembre 2023.

[18] S.C. Tucker, *The Encyclopedia Of Middle East Wars: The United States in the Persian Gulf, Afghanistan, and Iraq Conflicts*, vol. 5, Bloomsbury Publishing USA, 2010, p. 1770.

da chi ha sostenuto l'insensatezza di «trasformare i lunghi deliri pubblici di un terrorista in una conoscenza proibita, qualcosa che le persone si sentono entusiaste di andare a riscoprire». Nel frattempo, i supporter di al-Qaeda hanno celebrato online la "tempesta scatenata sul social media" dalla riscoperta della lettera dalla dubbia paternità[19].

In un recente contributo, abbiamo svolto alcune considerazioni sull'evoluzione digitale del terrorismo jihadista e sulla conseguente moltiplicazione del numero, delle forme e dell'entità dei rischi connessi all'attività dei gruppi islamisti: propaganda, addestramento e finanziamento online, infatti, hanno rappresentato e rappresentano una seria minaccia per la sicurezza pubblica[20].

In particolare, la propaganda jihadista online è diventata un «catalizzatore di radicalizzazione»[21] in grado di ispirare attacchi terroristici e provocare «gravi conseguenze negative per gli utilizzatori, i cittadini e la società in generale»[22]: lo dimostrano i tanti attacchi di *lone wolves* in Europa; lo ribadiscono, ove fosse necessario, i più recenti casi richiamati nell'*EU Terrorism Situation & Trend Report* (TE-SAT 2023) di Europol, relativi all'arresto, in Italia, di un uomo che diffondeva online materiale propagandistico e istruzioni per condurre attacchi terroristici e all'arresto, in Spagna, di due individui accusati di diffondere online materiale dell'IS per indottrinare, reclutare e istigare atti di violenza in nome dell'organizzazione jihadista; gli arrestati, si legge nel rapporto, avrebbero organizzato incontri offline per approfondire l'opera di radicalizzazione dei giovani reclutati[23]. Vale ricordare incidentalmente che anche in Africa e Medioriente, regioni in cui si osserva un'età media dei combattenti dell'ISIS tra i 18 e i 25 anni, i gruppi terroristici hanno sfruttato la progressiva diffusione dei dispositivi digitali per radicalizzare e indottrinare i più giovani[24].

[19] Nostra traduzione. National Public Radio, *The story behind the Osama bin Laden videos on TikTok*, liberamente consultabile su www.*npr.org*, 17 novembre 2023.

[20] Per considerazioni più analitiche, ci sia consentito di rinviare ad A. Casiere, *Il jihadismo digitale. Libertà religiosa, sicurezza, democrazia*, in *Stato, Chiese e pluralismo confessionale*, Rivista telematica (*www.statoechiese.it*), fascicolo n. 7 del 2023.

[21] Regolamento (UE) 2021/784, relativo al contrasto della diffusione di contenuti terroristici online, considerando n. 5.

[22] *Ibidem*.

[23] Cfr. Europol, *European Union Terrorism Situation and Trend report 2023 (TE-SAT)*, 26 ottobre 2023.

[24] Cfr. G. Sönmez, *Online Visibility And Radicalization: Concepts, Contextualization, And Cases*, in *Adam Alemi*, numero 1 del 2023, pp. 133, 134.

Negli ultimi anni, alcuni fattori hanno concorso al rallentamento dell'avanzata terrorista online: a) la sconfitta dello Stato islamico, che ha ridotto sensibilmente la propria comunicazione dagli «oltre 200 contenuti propagandistici a settimana» del 2015 agli «appena 20 output per settimana» del 2017; b) le operazioni coordinate da Europol, Eurojust e dalle omologhe agenzie statunitensi e c) le campagne di moderazione di contenuti promosse dalle piattaforme digitali[25]. Ciononostante, il modello comunicativo di maggior successo, quello dell'IS, continua ad ispirare l'azione di propaganda svolta da gruppi e individui, molti dei quali dimostrano una «impressionante curva di apprendimento» e una notevole capacità di adattamento ai meccanismi di censura digitale[26].

Più di recente, secondo uno studio pubblicato nell'ambito del *Program on Extremism* della George Washington University, si è assistito ad una forma di "*post affiliation jihadism*", ossia un jihadismo ispirato da propaganda generica e priva di affiliazione a gruppi specifici, in grado provocare attacchi sempre «più comuni man mano che le idee estremiste vengono diluite e rese disponibili su più piattaforme, spesso presentate come contenuti islamici generici». Al classico panorama del jihadismo digitale di al-Qaeda e dell'IS, si sono aggiunti individui e organizzazioni privi di collegamenti ufficiali come *Hurras al-Tawheed* (*HAT*, "Guardians of Monotheism"), un network gemmato dalla galassia qaedista di Rocket.Chat, che produce il magazine online *O Mujahideen in the West*. Tra le altre cose, *O Mujahideen in the West* promuove l'unificazione della causa dei seguaci di al-Qaeda e dell'IS attraverso il superamento della *fitna* (divisione) in nome della lotta ai *kuffar* (infedeli) occidentali; in proposito, è stata osservato come la qualità della rivista sia significativamente inferiore rispetto ad altre esperienze, anche a causa della scelta di pubblicare articoli brevi e citazionistici, scelta spiegata, espressamente, «dall'adattamento della *Dawah* (proselitismo) ai bisogni dei giovani d'oggi che sono abituati ad una "informazione breve e veloce" e sono ispirati dalla popolarità dei brevi video di TikTok e degli shorts di Youtube»[27].

[25] Cfr. A. Meleagrou-Hitchens, J. Bellaiche, *Maintaining the Movement: ISIS Outreach to Westerners in the Post-Caliphate Era, in Program on Extremism, The George Washington University and National Counterterrorism Innovation, Technology and Education Center. Reports Projects, and research*, aprile 2023, pp. 7, 8.

[26] Cfr. G. Sönmez, *Online Visibility And Radicalization*, cit., p. 136.

[27] Nostra traduzione. A. Meleagrou-Hitchens, J. Bellaiche, *Maintaining the Movement*, cit, p. 15 ss.

Quanto alle tendenze relative ai media di IS e al-Qaeda, invece, i primi sembrano puntare sull'attività di traduzione dei contenuti, considerata «la spina dorsale della strategia di comunicazione» che consente «di abbattere le barriere linguistiche e raggiungere i simpatizzanti di tutto il mondo», i secondi sono impegnati nel rinnovamento e nell'intensificazione della propaganda su Telegram, Rocket.Chat, Chirpwire e sulla creazione di nuove risorse web, con archivi contenenti dichiarazioni, fotografie e video[28].

Il fenomeno del terrorismo jihadista online, dunque, lungi dall'essere sconfitto, sembra piuttosto attraversare una fase di riorganizzazione ideologica e infrastrutturale; nel frattempo, però, esso resta in grado di provocare significative conseguenze negative, come dimostra il recente attentato di Bruxelles del 16 ottobre 2023, condotto da un lupo solitario probabilmente auto-radicalizzato ed auto-addestrato attraverso canali digitali[29].

3. … e autoritarismo digitale e capitalismo di sorveglianza

Il modello securitario, diffusosi a partire dal 9/11 in risposta alle azioni del terrorismo religioso internazionale, considera la sicurezza e la libertà religiosa come conflittuali se non, addirittura, inversamente proporzionali[30]: come evidenziato da Pasquale Annicchino, a far data dagli attacchi del 2001, il rapporto tra diritto e religione è stato dominato da uno spirito di securitizzazione ben riassunto da Jeroen Temperman ha ben descritto come segue: «diritti e libertà sono buoni e giusti, ma se non controllate, le libertà possono attentare ad un altro importante bene pubblico, la sicurezza»[31].

In questa prospettiva, la tecnologia digitale è stata impiegata per «prevenire e reprimere le attività terroristiche che si consumano su Internet» e per «contrastare le condotte criminali che non avvengono online»[32]; ciò ha prodotto non solo condotte «potenzialmente foriere di violazioni di diritti quali *privacy*, *data*

[28] Cfr. Europol, *European Union Terrorism Situation and Trend*, cit.

[29] Cfr. N. Scheirlinckx, *Pourquoi Abdessalem Lassoued est-il passé à l'acte? «On dirait qu'il n'avait pas prévu l'après». Le point avec Thomas Renard, directeur du Centre international de lutte contre le terrorisme (ICCT)*, in *Le Vif* (www. levif.be), 20 ottobre 2023.

[30] Sul punto, cfr. R. Mazzola, *Recensione a G. Fattori (a cura di), Libertà religiosa e sicurezza. prima traduzione delle Linee Guida OSCE 2019*, cit., in *Diritto e Religioni*, n. 1 del 2021, p. 869.

[31] Nostra traduzione. P. Annicchino, *Comprehensive security and religion*, cit.

[32] A. Vedaschi, *Sicurezza e diritti nella digital age*, cit., p. 528.

protection e libertà di espressione», ma anche condotte lesive della presunzione di innocenza quante volte coinvolgano la «generalità degli individui, anziché focalizzarsi unicamente su coloro nei cui confronti esiste almeno un sospetto»[33].

La digitalizzazione, dunque, ha «aumenta[to] la superficie d'attacco disponibile»[34]: lo dimostra plasticamente il caso cinese dello Xinjiang[35]. La regione autonoma uigura dello Xinjiang (XUAR), abitata in maggioranza dall'etnia musulmana degli uiguri (una minoranza in Cina), è ritenuta un «caso limite persino per il sistema di sorveglianza cinese»: qui, per ragioni di contrasto al terrorismo, le autorità avrebbero installato oltre 9000 hub di sorveglianza (*People's Convenience Police Stations*) e migliaia di *face-scan* e *phone-scan checkpoints*; inoltre, gli apparati di pubblica sicurezza sarebbero in possesso dei dati biometrici di quasi tutti i residenti, raccolti nel corso di una campagna globale di salute pubblica. Grazie alla complessa e integrata rete di tecnologie digitali e algoritmi, le forze dell'ordine sarebbero in grado di comparare rapidamente centinaia di milioni di immagini, localizzare gli individui, tracciare le attività (digitali e non), analizzare dialoghi, effettuare riconoscimenti facciali e molto altro[36].

Altrove, all'inverso, è stata la difesa della religione, quindi la sicurezza della religione, a costituire il movente per conculcare diritti individuali e delle minoranze attraverso operazioni di sorveglianza e controllo digitale legittimate da cornici normative *ad hoc*, approvate nell'ambito di politiche di sicurezza e cyber-sicurezza nazionale. In particolare, si è osservato che alcuni governi hanno impiegato «le tecnologie digitali per violare i diritti umani, specialmente la libertà di espressione, l'accesso all'informazione e la privacy», con una in-

[33] *Ibidem*..

[34] P. Annicchino, *Se la religione diventa un laboratorio per la sorveglianza digitale*, cit.

[35] Per un primo approfondimento, si veda P. Annicchino, *La minoranza musulmana e lo stato nazionale di sorveglianza cinese*, cit.

[36] D. Byler, *Surveillance, data police, and digital enclosure in Xinjiang's "Safe Cities"*, in D. Byler, I. Franceschini, N. Loubere (a cura di), *Xinjiang Year Zero*, The National University – Canberra, 2022, p. 186. Si veda anche K. Strittmatter, *Stato di Sorveglianza. La vita in Cina ai tempi del controllo di massa*, LUISS University Press, Roma, 2022. Il 15 dicembre 2022, il Parlamento europeo ha nuovamente condannato «l'ampio ricorso alla sorveglianza di massa e l'attuale censura dei social network» da parte di Pechino e ha esortato «le autorità cinesi a cessare tali violazioni dei diritti fondamentali alla vita privata e alla libertà di espressione e la manipolazione delle informazioni sui social network». Parlamento Europeo, *Risoluzione sulla repressione delle proteste pacifiche nella Repubblica popolare cinese da parte del governo cinese*, 15 dicembre 2022.

tensità tale da far temere la degenerazione in «una sorveglianza permanente dei cittadini da parte del governo»[37]. India, Indonesia, Pakistan, Turchia, Malesia e Iran, secondo un nutrito gruppo di studiosi e osservatori, sfrutterebbero le risorse digitali contro minoranze, dissidenti, oppositori e attivisti. Nella classifica dei censori, l'Iran occuperebbe il secondo posto, con la ripetuta globale disabilitazione dell'accesso a Internet, alle piattaforme social e alla rete dati mobile, dispiegata per arginare le proteste e il dissenso[38].

Come abbiamo anticipato, tuttavia, gli attori pubblici non sono l'unica fonte di "pericolo digitale": in Occidente, infatti, c'è chi ritiene che «la principale minaccia per le democrazie costituzionali» provenga «da attori privati che amministrano gli spazi che sono formalmente privati, ma che esercitano in pratica, e senza alcun controllo, funzioni tradizionalmente attribuite ad autorità pubbliche»[39].

Il passaggio all'intelligenza artificiale ha amplificato la questione, poiché «uno degli impieghi più frequenti di questa nuova frontiera della tecnologia riguarda il riconoscimento di messaggi diffusi sulle piattaforme digitali e potenzialmente pericolosi, perché aventi una portata radicalizzante, anche quando non direttamente tesa al reclutamento del destinatario in organizzazioni terroristiche»; gli algoritmi destinati a questa funzione «vengono direttamente elaborati dalle medesime piattaforme digitali gestite dalle grandi società tecnologiche» con «non trascurabili problemi sotto il profilo della trasparenza dei sistemi»[40]. Inoltre, come già evidenziato[41], la concentrazione di poteri a rilevanza pubblicistica o quasi-pubblicistica nelle mani di pochi intermediari digitali alimenta una distorsione della sfera pubblica che si riflette sul «fun-

[37] Nostra traduzione. Cfr. I. Yilmaz, F. Yang, *Digital Authoritarianism, Religion and Future of Democracy*, in I. Yilmaz (a cura di), *Digital Authoritarianism and its Religious Legitimization. The Cases of Turkey, Indonesia, Malaysia, Pakistan and India*, Palgrave Macmillan, 2023, p. 153.

[38] Cfr. I. Yilmaz, F. Yang, *Digital Authoritarianism*, cit., L. Hashemi, *Threats to Iranian Instagram: Analyzing Iran's Internet Landscape*, in *www.washingtoninstitute.org* 24 novembre 2021; Al Arabiya English, *Iran second worst country for internet censorship in 2022 following protests: Report. By Jennifer Bell*, in *english.alarabiya.net*, 25 gennaio 2023, S. Shample, *Using digital tools, the IRGC strengthens its grip on power in Iran*, in *www.mei.edu*, 29 settembre 2020.

[39] Nostra traduzione. G. De Gregorio, *Digital Constitutionalism in Europe*, cit.

[40] A. Vedaschi, *Sicurezza e diritti nella digital age*, cit., p. 529 ss.

[41] Si veda A. Casiere, *Il jihadismo digitale. Libertà religiosa, sicurezza, democrazia*, cit.

zionamento dei processi democratici»: a guardiani privati, che promettono il mantenimento dell'ordine digitale, è consentito «sopprimere arbitrariamente certi punti di vista senza che ai soggetti colpiti sia data la possibilità di una qualche forma [effettiva] di ricorso», con ricadute significative sul diritto all'informazione e, più in generale, sui processi democratici ed elettorali, poiché «la sfera pubblica è il luogo dove si realizzano i valori della libertà di parola e di espressione. La libertà di parola è alla base della partecipazione democratica che contribuisce alla formazione dell'opinione pubblica»[42], un asset strategico che, per citare la Corte costituzionale, costituisce il «cardine di democrazia dell'ordinamento generale»[43].

Questo modello di amministrazione pubblico-privato dello spazio digitale ha certamente potenziato l'efficacia della lotta ai contenuti illeciti in generale e terroristici in particolare; tuttavia, non può sottacersi che, mentre il potere pubblico «ha l'obbligo positivo di proteggere i diritti umani e operare in modo trasparente, imparziale e nel pubblico interesse», gli operatori digitali non hanno «doveri di imparzialità, trasparenza o protezione dei diritti umani», ma rispondono solo all'esigenza di «massimizzare il profitto nell'interesse privato», circostanza che rende quantomeno «azzardato delegare simili poteri pubblici agli intermediari di Internet»[44].

[42] 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. 826 ss.

[43] Secondo. D. Caccioppo, la «sentenza della Corte costituzionale n. 126 del 1986 definendo la libertà di espressione come «cardine di democrazia dell'ordinamento generale» ha ribadito «la rilevanza centrale […] che la libertà di manifestazione del pensiero, anche e soprattutto in forma collettiva, assume ai fini dell'attuazione del principio democratico». La Corte ha utilizzato questo metodo interpretativo in molte pronunce riguardanti per la maggior parte l'area dell'informazione (in altri termini la libertà di espressione del pensiero impiegata a fini informativi), riconducendo il diritto di informare all'area tematica della tutela della libertà costituzionale di manifestazione del pensiero, sulla base della considerazione che le notizie, così come le opinioni, sono espressioni del pensiero (Corte cost., 14.4.1965, n. 24, Corte cost., 10.3.1996, n. 18, Corte cost., 9.7.1970, n. 122, Corte cost., 14.7.1971, n. 1975, Corte cost., 15.6.1972, n.105, Corte cost., 23.4.1974, n. 113, Corte cost., 10.2.1981, 26, Corte cost., 10.2.1981, 18, Corte cost. 23.3.1983, n. 73)». Cfr Id., *Osservazioni in chiave pubblicistica sui provvedimenti restrittivi delle piattaforme digitali*, in *NGCC*, numero 4 del 2023, pp. 817-823.

[44] Nostra traduzione. L. Belli, C. Sappa, *The Intermediary Conundrum*, cit., p. 185.

4. Conclusioni

«Penso che stiamo per scontrarci con una rivoluzione che farà sembrare quello che ha fatto Gutenberg come una tranquilla passeggiata pomeridiana». Con queste parole, nel 1986, lo storico della scienza James Burke commentava il futuro dell'*electronic revolution*, rispondendo a Benjamin Dunlap nel corso di una serie di brevi conversazioni, "After Words", trasmesse dalla PBS in appendice agli episodi del documentario "The Day the Universe Changed". Quello che Burke non poteva allora prevedere è che, in quel futuro, uno strumento di libertà e sviluppo come la tecnologia digitale, avrebbe costituito altresì una potente arma nelle mani di terrorismo e regimi autoritari.

Il terrorismo jihadista è uno dei pericoli avvertiti con maggiore preoccupazione dall'opinione pubblica ed è, nel quadro della sicurezza nazionale, tra i migliori argomenti per la limitazione della *privacy*, della libertà religiosa e della manifestazione del pensiero attraverso gli strumenti digitali: bilanciare «il bisogno di *cybersecurity* con le preoccupazioni per la *privacy*, la libertà di espressione e di credo è un problema complesso che richiede attenta valutazione» finalizzata ad evitare da un lato che «vincoli legali e burocratici possono ostacolare la capacità dello stato di intervenire rapidamente contro i gruppi estremisti»[45] e, dall'altro, che si sacrifichino le garanzie in materia di libertà, producendo l'insicurezza (o incertezza) dei diritti fondamentali.

Adattare la sofisticata architettura dello Stato di diritto al mondo digitale appare assai complessa: anzitutto, perché la tecnologia digitale è caratterizzata da una rapidità di sviluppo che impone una navigazione a vista, con cambi repentini di rotta; in secondo luogo, perché l'estensione quali-quantitativa del rischio e del danno, potenzialmente catastrofico, sembra invocare il superamento di alcune garanzie costituzionali sacrificate sull'altare dell'efficacia e dell'effettività; infine, perché questa dinamica si inserisce nel più ampio processo di securitizzazione caratterizzato da un clima in cui «in nome di un'assoluta ed oltranzistica difesa di questo genere di sicurezza possono essere compromessi i diritti individuali costituzionalmente riconosciuti in una sorta di collettiva "ansia che cancella i diritti"»[46].

[45] Nostra traduzione. G. Sönmez, *Online Visibility And Radicalization*, cit.

[46] N. Colaianni, *Il disagio della libertà*, in F. Alicino (a cura di), *Terrorismo di ispirazione religiosa. Prevenzione e deradicalizzazione nello Stato laico*, Editrice Apes, Roma, 2019, p. 18 ss.

Invece, il fine dell'ordine pubblico materiale, che certamente è causa efficiente e finale dell'ordinamento e interesse costituzionalmente rilevante alla pacifica convivenza e al libero godimento dei diritti, deve essere perseguito all'interno del perimetro di regole e principi che legittimano l'azione pubblica, specie nell'interazione con i diritti fondamentali. Fermo restando che non esiste il «diritto soggettivo "alla" sicurezza pubblica», è pacifico invece che la Costituzione conferisce rilievo all'interesse collettivo all'*ordre dans la rue* attraverso un'attribuzione diffusa di competenze di sicurezza alle autorità pubbliche che possono adottare provvedimenti «anche in limitazione di diritti costituzionalmente previsti purché la Costituzione lo consenta espressamente oppure ne riservi la previsione alla legge»[47].

I diritti fondamentali, che «non [sono] mai affermati in termini assoluti», sono inseriti «in una complessa trama costituzionale in cui la loro portata può essere limitata da altri diritti e interessi tutelati», tra cui la sicurezza. Se quest'ultima «può essere motivo di limitazione dei diritti», i diritti fungono a loro volta «da invalicabile argine contro derive securitarie», onde impedire che essa, svuotandoli di contenuto, renda impossibile «godere delle libertà garantite costituzionalmente e, di riflesso, lo sviluppo della persona umana e della sua dignità»[48]. Il funzionamento di questo complesso meccanismo circolare è assicurato, dagli strumenti costituzionali che misurano il rapporto tra autorità e libertà nella democrazia liberale e cioè dai principi di ragionevolezza, di presunzione di non colpevolezza, di riserva di legge, di riserva di giurisdizione, di legalità e proporzionalità e dai rispettivi corollari.

Tutti questi principi dovrebbero giocare un ruolo fondamentale nella regolazione della sfera pubblica e della tecnologia digitale, in quanto, permettendo l'azione pubblica nel rispetto delle libertà fondamentali, individuano il limite alle interferenze illecite nella vita privata e alla censura (specie preventiva); tuttavia, essi appaiono gravemente depotenziati dall'attuale statuto privatisti-

[47] Cfr. A. Pace, *La sicurezza pubblica nella legalità costituzionale*, in *Rivista AIC*, numero 1 del 2015 e R. Niro, *Il "posto" di sicurezza e ordine pubblico nella costituzione italiana, nel pensiero di Alessandro Pace. Nel segno del costituzionalismo garantista*, in *Giurisprudenza costituzionale*, n. 6 del 2019.
[48] A. Negri, *Radicalizzazione religiosa e de-radicalizzazione laica. Sfide giuridiche per l'ordinamento* democratico, Carocci editore, Roma, 2022, p. 42 ss.

co della sfera pubblica digitale[49], pensato in un'epoca in cui quegli strumenti non erano in grado di produrre effetti negativi di questa portata.

Si tratta, dunque, non solo di ripensare il delicato bilanciamento di interessi e diritti in gioco, ma soprattutto di individuare un modello normativo in grado di influenzare positivamente il futuro dei diritti umani e della democrazia. Resistere alla tentazione di sacrificare la libertà, in cambio di uno spazio digitale addirittura più sicuro di quello tradizionale, consente di sbarrare la strada a forme di autoritarismo digitale sul modello orientale o ad un capitalismo di sorveglianza con potenziali proiezioni orwelliane.

[49] A. Casiere, *Il jihadismo digitale. Libertà religiosa, sicurezza, democrazia*, cit.