

Access denied: gli *Internet shutdowns* alla prova del diritto. Spunti di riflessione a partire dalla giurisprudenza della *Supreme Court* indiana

di Giulia Formici

Abstract: *Access Denied: The Test of Law for Internet Shutdown. Food for Thought Starting from the Indian Supreme Court Case-Law* – Internet shutdowns are escalating worldwide. These instruments, increasingly employed by public authorities to – at least formally – guarantee public order and national security, severely affect fundamental rights, in particular freedom of expression and assembly. The paper provides an overview of Internet shutdowns and their effects, focusing on the public and legal debate concerning this vast and indiscriminate censoring practice. The analysis of the relevant Indian Supreme Court case-law will lead to conclusive remarks on the need to ensure a careful proportionality test on Internet shutdown’s legitimacy, in order to avoid the rise of digital authoritarian instruments able to jeopardize democratic values.

Keywords: Internet Shutdown; Freedom of Speech; Indian Supreme Court; Internet Governance; Online Censorship.

1. Il controllo di Internet come sfida emergente: il caso degli *Internet shutdowns* quale osservatorio privilegiato

Nel febbraio 2007, durante accese proteste popolari avverso le discusse scelte politiche dell’allora Capo di Stato della Repubblica di Guinea, Lansana Conté, quest’ultimo ordinò l’interruzione totale di Internet e delle comunicazioni elettroniche sull’intero territorio nazionale, imponendo ai quattro maggiori *Internet Service Providers* (ISPs) di sospendere la fornitura dei propri servizi¹. È il primo caso noto di *Internet shutdown*² ovvero di un blocco esteso, generalizzato ed intenzionale della rete Internet, che può utilmente essere definito come l’insieme delle misure “taken by a government, or on behalf of a government, to intentionally disrupt access to, and the use of, information and communications systems online. They include actions that limit the ability of a large number of people to use online communications tools, either by restricting Internet connectivity at large or

¹ Si rinvia, per maggiori dettagli, a J. Rydzak, M. Karanja, N. Opiyo, *Dissent Does Not Die in Darkness: Network Shutdowns and Collective Action in African Countries*, in *Int J of Communication*, 14, 2020, 4264–4287.

² Altri termini sovente impiegati per identificare tali strumenti sono: “Internet blackouts”, “network shutdown”, “digital curfews” o “Internet kill switches”.

by obscuring the accessibility and usability of services that are necessary for interactive communications, such as social media and messaging services”³.

Il caso guineano non è tuttavia rimasto a lungo isolato: lo strumento impiegato nel 2007 ha infatti conosciuto una rapida diffusione, principalmente – ma non solo, come si avrà modo di vedere – in Stati del Continente africano e del Sud-Est asiatico, registrando un aumento esponenziale, nell’ultimo decennio, in termini di frequenza, durata e livello di sofisticazione.

La richiamata espansione degli *Internet shutdowns* non è però passata inosservata, avviando un intenso dibattito nella società civile, nella dottrina, nonché nelle istituzioni nazionali e internazionali e nelle corti. Da un lato, le autorità governative hanno sovente giustificato e motivato il ricorso a tali strumenti facendo riferimento ad esigenze di garanzia dell’ordine pubblico e della sicurezza nazionale; dall’altro, l’utilizzo degli *Internet shutdowns* in occasione di manifestazioni – digitali o “fisiche” – di dissenso avverso il potere costituito o determinate decisioni governative, nonché durante o immediatamente dopo importanti appuntamenti elettorali, ha ben presto rivelato un significativo impatto sui diritti fondamentali, tra cui sono certamente da indicare le libertà di espressione e riunione. L’ormai riconosciuto stretto legame tra queste ultime e la dimensione digitale⁴ ha allora aperto ad importanti interrogativi quanto alla legittimità e compatibilità con le carte costituzionali del blocco totale o parziale di Internet.

Simili quesiti, che divengono sempre più indifferibili e seri, si inseriscono poi nel vasto e complesso ambito della *governance* di Internet⁵. In un contesto in cui persino la partecipazione politica passa e si realizza attraverso la rete⁶, così che “technology governance can become a tool of

³ Questa la chiara definizione proposta dal United Nations Human Rights Council nel Report of the Office of the UN High Commissioner for Human Rights, *Internet Shutdowns: Trends, Causes, Legal Implications and Impacts on a Range of Human Rights*, A/HRC/50/55, 13 maggio 2022.

⁴ Tra la sconfinata bibliografia sul rapporto tra rete e diritti fondamentali, si legga: I. Hartmann, *A Right to Free Internet: On Internet Access and Social Rights*, in *J. High. Tech. L.*, 13, 2013; G. De Minico, *Libertà in rete. Libertà dalla rete*, Torino, 2020, ma anche UN Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, A/HRC/47/L.22, 13 luglio 2021.

⁵ Ai fini di questo contributo, con il termine *Internet governance* o “governo di Internet” si intende far riferimento alla disciplina della rete nella sua complessità, con riguardo dunque non solo alla regolazione tecnica dei sistemi di connessione bensì anche alla gestione di “tutta una serie di altri aspetti correlati, quali ad esempio: la neutralità della Rete, il diritto ed i costi di accesso, il rispetto delle libertà fondamentali sulla gestione dei contenuti, la tutela della proprietà intellettuale, le politiche fiscali, la sicurezza, l’individuazione di ciò che è reato e la correlata punibilità o repressione e via discorrendo”, A. Nicotra, *L’Internet governance in Italia*, in *Informatica e diritto*, 1, 2009, 63. Per approfondimenti sul concetto di *Internet governance* e sul suo stretto legame con i diritti fondamentali, si leggano, tra i tanti: R. Radu, J-M. Chenou, R. Weber (eds), *The Evolution of Global Internet Governance*, Berlino, 2014, 57-78; L. Abba, A. Lazzaroni, M. Pietrangelo (a cura di), *Fascicolo Monografico. La Internet governance e le sfide della trasformazione digitale*, in *Rivista Italiana di Informatica e Diritto*, 1, 2022.

⁶ Per riflessioni sul legame tra Internet e partecipazione democratica, si rinvia al *Il Forum: Le sfide della democrazia digitale*, in *Rivista del Gruppo di Pisa*, 3, 2019, 231-284.

political control”⁷, si afferma cioè la necessità di superare quell’originaria concezione di Internet quale “free marketplace of ideas”⁸, caratterizzata da una ottimistica – e forse ingenua – fiducia nella autodisciplina della rete e nell’esclusione dei pubblici poteri da qualsiasi intervento⁹. Tale visione deve ormai lasciare spazio ad una profonda discussione – ancora lontana dall’aver raggiunto un punto di arrivo – sulla regolamentazione – *governance* appunto – di Internet, sull’intreccio spesso confuso tra intervento dei pubblici poteri e responsabilizzazione dei privati e, in particolare, sulle possibili restrizioni alla libertà d’espressione e di accesso alle informazioni¹⁰. Una discussione, questa, che – anche nelle democrazie stabilizzate – contribuisce a complicare il già problematico e antico rapporto tra potere e libertà, trasponendolo in una realtà digitale che, proprio per la sua intrinseca struttura, è in grado di moltiplicare opportunità ma anche rischi¹¹.

In tale panorama, gli *Internet shutdowns*, realizzandosi in limitazioni volontarie e intenzionali della disponibilità della rete su ordine delle autorità pubbliche e dunque andando ben oltre il controllo dei singoli contenuti pubblicati online¹², divengono chiave di lettura ed osservatorio privilegiato per promuovere una riflessione più articolata sulla realizzazione di vecchie – e nuove – forme di protezione dei diritti nel mondo dei *bit* e sulla regolamentazione dello stesso. Un simile sforzo regolatorio emerge infatti in tutta la sua urgenza e rilevanza dinnanzi al concreto rischio che strumenti quali gli *Internet shutdowns*, assumendo le dimensioni di una “online censorship” tra le più “invasive and blunt”¹³, si tramutino infine in illimitate ed insidiose forme di repressione dei diritti e delle libertà capaci, insieme a mezzi sempre più diffusi di sorveglianza digitale, di determinare una deriva verso ciò che taluni studiosi hanno definito “digital authoritarianism”¹⁴.

⁷ N. Mulani, *The Politics of Internet Shutdown. Governance Lessons from Kashmir’s Internet Shutdowns*, in *Verfassungsblog*, 20 dicembre 2022.

⁸ Questa espressione, che trova radici nel concetto di “free trade in ideas”, coniato in una datata *dissenting opinion* dal Justice Holmes (caso *Abrams v. United States*, 250 U.S. 616, 630 (1919)), si è successivamente sviluppata, soprattutto con la pronuncia *Reno v. American Civil Liberties Union* 521 U.S.844 1997, così da essere impiegata anche con riferimento al contesto digitale.

⁹ O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?*, Oxford, 2021, 96; ma anche S. Rodotà, *Una Costituzione per Internet?*, in *Politica del diritto*, 3, 2010, 337-351; P. Passaglia, *Fake news e fake democracy*, in *Federalismi.it*, 11, 2020, 126-139.

¹⁰ Sul punto G. Azzariti, *Internet e costituzione*, in *Politica del diritto*, 3, 2011, 367-378; ma anche S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma, 2014; R.F. Jorgensen, *A Human Rights-Based Approach to Social Media Platforms*, in *Berkley Forum*, 26 febbraio 2021.

¹¹ Con riferimento a tali profili si rimanda, *ex multis*, a M. Bassini, *Internet e libertà di espressione. Prospettive costituzionali e sovranazionali*, Napoli, 2019; P. Falletta, *Controlli e responsabilità dei social network sui discorsi d’odio online*, in *MediaLaws*, 1, 2020, 147 ss.

¹² Sul rapporto tra misure di *content moderation* e controllo dei contenuti in Internet, da un lato, e gli *Internet shutdowns* e dunque forme di controllo generalizzato della rete, si dirà più ampiamente nelle conclusioni di questo lavoro.

¹³ G. De Gregorio, N. Stremlau, *Internet Shutdowns and the Limits of Law*, in *Int. J. of Communication*, 14, 2020, 4227.

¹⁴ Così A. Polyakova e C. Meserole in *Exporting Digital Authoritarianism: The Russian and Chinese models*, che intendono definire con tale termine “the use of digital information technology (..) to surveil, repress and manipulate domestic and foreign

Il presente contributo intende pertanto esaminare gli importanti quesiti giuridici posti dagli *Internet shutdowns*, riconducendoli entro il più ampio contesto appena delineato. Dopo un primo paragrafo volto a contestualizzare lo strumento del blocco della rete, fornendo alcune imprescindibili coordinate sulla posizione emersa da taluni studi promossi da società civile e organizzazioni internazionali, il lavoro si concentrerà sul rilevante apporto delle corti; nonostante diversi giudici – anche costituzionali – siano stati, negli ultimi anni, chiamati a pronunciarsi sugli *Internet shutdowns*, il terzo paragrafo intende porre attenzione alla giurisprudenza indiana, con particolare riguardo alle decisioni della Corte suprema.

Questa scelta risulta motivata sotto diversi profili: innanzitutto l'India detiene ad oggi il primato mondiale quanto a numero di *Orders* adottati al fine di bloccare la rete¹⁵, così che la casistica con cui anche le corti si sono confrontate appare differenziata e particolarmente variegata. La *case-law* in materia di *Internet shutdown* in tale ordinamento si inserisce, inoltre, a pieno titolo, in un più esteso ed interessante filone giurisprudenziale entro cui rientrano diverse pronunce della *Supreme Court* aventi ad oggetto la legittimità costituzionale di normative regolanti l'impiego di innovativi sistemi tecnologici o sofisticati strumenti di Intelligenza artificiale da parte delle autorità pubbliche; in tutti questi casi la corte apicale indiana è intervenuta con sentenze di forte rilievo – anche in ottica comparata – e molto discusse, in grado di indurre sovente gli organi legislativo o esecutivo ad adottare disposizioni maggiormente garantiste dei diritti fondamentali¹⁶.

populations”, in *Democracy & Disorder*, Brookings Institution, 2019, 1. Feldstein, in *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics & Resistance*, Oxford, 2021, parla di *digital repression* con riferimento all'utilizzo “of information and communications technology to surveil, coerce, or manipulate individuals or groups in order to deter specific activities or beliefs that challenge the state”; è proprio in questa categoria che vengono inseriti anche gli *Internet shutdowns* (e similmente, Rydzak, Karanja, Opiyo, *Dissent Does Not Die in Darkness*, cit.). B. Wagner (*Understanding Internet Shutdowns: A Case Study from Pakistan*, in *Int. J. of Communication*, 12, 2018, 3932) descrive invece gli *Internet shutdown* come “authoritarian practice”, cioè “strategic measure to prevent mobilization, as well as a disciplinary measure to prevent marginalized others from taking part in the national political debate and documenting their grievances”.

¹⁵ Per un'analisi dei dati, K. Ruijgrok, *Understanding India's Troubling Rise in Internet Shutdowns. A Qualitative and Quantitative Analysis*, Amsterdam, 2021.

¹⁶ Si pensi, in tale ambito, alle note vicende giudiziarie relative al c.d. progetto *Aadhaar* di riconoscimento biometrico (L. Scaffardi, *Dati genetici e biometrici: nuove frontiere per le attività investigative* in L. Scaffardi (a cura di), *I 'profili' del diritto. Regole, rischi e opportunità nell'era digitale*, Torino, 2018, 37-64; sia consentito poi il rinvio a G. Formici, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i legislatori e le corti*, in questa Rivista, 2, 2019, 1107-1132). Testimonianza dell'attivismo della Corte suprema indiana nell'ambito delle nuove tecnologie è anche la sentenza *Manohar v. Union of India*, No. 314/2021, 27 ottobre 2021, avente ad oggetto la legittimità delle operazioni di raccolta, trattamento e conservazione di dati – anche personali – svolte mediante lo *spyware* Pegasus. Su tale pronuncia, G. Kumar, *An Analysis of the Pegasus Spyware Issue in Light of Surveillance Laws and the Right to Privacy in India*, in *Law J.*, 2, 2021-2022, 394; S. Shrivastava, M. Kejriwal, *Pegasus Spyware: Evaluating the Need for Surveillance Reform and Introduction of Data Protection Bill*, in *Nirma University Law J.*, 11, 2021-2022, 67-78.

Infine, sotto il profilo metodologico, in India è possibile rinvenire, nonostante alcune criticità accentuatesi negli ultimi decenni¹⁷, un'esperienza di costituzionalismo maturo¹⁸. La decisione di analizzare la giurisprudenza indiana consente quindi di non relegare lo studio delle questioni giuridiche attinenti all'impiego di *Internet shutdowns* unicamente a regimi autocratici o in ordinamenti nei quali troviamo “processi di transizione e significativi rischi per la stabilità e la tenuta democratica”¹⁹, che pure sono stati teatro di numerose vicende giudiziarie in materia. Fare riferimento ad un ordinamento nel quale la questione di legittimità del controllo di Internet è filtrata dai meccanismi propri del costituzionalismo permette di aprire la prospettiva di analisi e di promuovere, infine, più articolate riflessioni conclusive che coinvolgono e ben possono essere utili anche per gli ordinamenti nostrani, in un ambito – quello ampio e frastagliato della *governance* della rete e delle nuove tecnologie – che pone ancora non pochi quesiti persino nelle democrazie stabilizzate²⁰.

¹⁷ C. Petteruti, *Elezioni indiane 2019: la forma di governo parlamentare alla prova del fenomeno Modi*, in questa Rivista, 4, 2019, 2679-2697; A. Varshney, S. Ayyangar, S. Swaminathan, *Populism and Hindu Nationalism in India*, in *Studies in Comparative International Development*, 56, 2021, 197-222; A.R. Robledo, *India at the Crossroads: 75 Years of the World's Most Populous Democracy*, in *Diritti Comparati*, 5 ottobre 2022.

¹⁸ In questo senso D. Amirante (a cura di), *I sistemi costituzionali dell'Asia meridionale*, Milano, 2019, 11. Sul tema, l'Autore – in *Democrazie imperfette e «altre democrazie»? Costituzioni e qualità della democrazia nel sub-continente indiano*, in D. Amirante (a cura di), *«Altre» democrazie. Problemi e prospettive del consolidamento democratico nel sub-continente indiano*, Milano, 2010, 15-33 – parla di India come di una democrazia “altra” in cerca di consolidamento. Dello stesso Autore, si richiama *La democrazia dei superlativi. Il sistema costituzionale dell'India contemporanea*, Napoli, 2019. Per D'Ignazio, l'India rientra in un gruppo di Paesi (tra cui USA, Brasile e Russia con riferimento alla situazione politica del 2020) governati da leader populistici, che hanno provato “prima della pandemia e con diversa intensità, a caratterizzare in senso illiberale i rispettivi ordinamenti o, almeno, a introdurre in essi elementi di illiberalità”, G. D'Ignazio, *Le democrazie illiberali in prospettiva comparata: verso una nuova forma di Stato? Alcune considerazioni introduttive*, in questa Rivista, 3, 2020, 3870.

¹⁹ Amirante, *I sistemi costituzionali dell'Asia meridionale*, cit., 11.

²⁰ Si vuole premettere, sotto il profilo metodologico, la scelta di non osservare, nel presente contributo, il vasto e ancora acceso dibattito circa la qualificazione dell'“accesso ad Internet” quale diritto fondamentale a sé stante. Tale tematica, peraltro rivitalizzata a seguito dell'emergenza pandemica, è sicuramente di estremo rilievo ed attualità ma, come si vedrà anche nella giurisprudenza indiana analizzata nonché in altre pronunce richiamate, non è stata affrontata dalle corti come determinante e necessaria al vaglio di legittimità costituzionale degli *Internet shutdowns*. Volendo dunque concentrarsi in questa sede sulle sfide poste dall'impiego di forme di controllo della rete e sul percorso argomentativo seguito dai giudici indiani, si rinvia per approfondimenti sulla natura del diritto all'accesso ad Internet – da tenere distinto rispetto alla libertà di accesso alla rete – all'ampia dottrina che si è occupata del tema: tra i molti, per il profilo nazionale, M. Pietrangelo (a cura di), *Il diritto di accesso a Internet*, Napoli, 2011 e in tale volume T.E. Frosini, *Il diritto costituzionale di accesso a Internet*, 23-43; P. Costanzo, *Miti e realtà dell'accesso ad Internet (una prospettiva costituzionalistica)*, in *ConsultaOnline*, 2012, 1-14; L. Cuocolo, *La qualificazione giuridica dell'accesso a Internet tra retoriche globali e dimensione sociale*, in *Politica del Diritto*, 2-3, 2012, 263-288; M. Nisticò, P. Passaglia (a cura di), *Internet e Costituzione*, Torino, 2014; Rodotà, *Una Costituzione per Internet?*, cit.; M.R. Allegri, G. d'Ippolito (a cura di), *Accesso a Internet e neutralità della Rete, fra principi costituzionali e regole europee*, Roma, 2018; C.

2. La censura *della* rete: le coordinate di un vasto dibattito

Per comprendere la complessità delle sfide poste dall'impiego di *Internet shutdowns*, pare necessario fornire alcune coordinate di riferimento, così da comprendere al meglio le cause che hanno portato le autorità pubbliche ad adottare tali strumenti e le conseguenze che essi provocano rispetto alla tutela dei diritti fondamentali.

Come anticipato, il carattere generalizzato, indiscriminato – cioè atto a colpire tutti gli utenti di un dato territorio – e volontario degli *Internet shutdowns* consente di distinguere tale fenomeno da altre attività di controllo nel web: “Unlike ongoing filtering activities, shutdowns include fixed beginning and endpoints. Shutdowns are therefore characterized by their alteration of an existing operating state of the Internet. Experts identify six categories of Internet disruption related to scope: national Internet shutdowns, subnational Internet shutdowns, national mobile shutdowns, subnational mobile shutdowns, national shutdowns of apps/services, and subnational shutdowns of app/services (including VoIP like Skype)”²¹. Pur senza entrare in complessi tecnicismi, è importante evidenziare come gli *shutdowns* possano assumere forme disparate, differenziandosi per estensione territoriale, mezzo di comunicazione colpito dalla misura restrittiva²² e potendo anche realizzarsi mediante “targeted blocking of communication platforms”, cioè limitando il “blackout” di rete unicamente a determinate piattaforme, tra cui Facebook, Twitter, Whatsapp, Instagram e Telegram, sempre più impiegate come mezzi di scambio di informazioni e ritenute centrali per l'organizzazione di manifestazioni pubbliche. Anche in questo caso, però, diversamente dalla censura ed eliminazione di singoli post (controllo *nella* rete), il blocco così targettizzato implica l'impossibilità per qualunque utente di accedere a qualsiasi contenuto o di ricevere qualsiasi comunicazione, producendo quindi effetti generalizzati ed indiscriminati.

Il livello di sofisticazione degli strumenti descritti, tuttavia, non si esemplifica solamente nel livello di targhettizzazione dei servizi o delle aree geografiche colpite bensì anche nel tipo di blocco effettuato: il *throttling* – letteralmente “strozzatura” – indica una particolare tecnica di *shutdown* che si concretizza nel rallentamento, imposto ed intenzionale, della connessione.

Lotta, *Un nuovo diritto al tempo del Covid-19? Accesso a Internet e digital divide*, in *Rivista del Gruppo di Pisa*, 1, 2020, 61-71; con riferimento agli studi di diritto internazionale: F. Borgia, *Riflessioni sull'accesso ad Internet come diritto umano*, in *Comun. intern.*, 3, 2010, 395-414; G.M. Ruotolo, *Internet (Diritto internazionale)*, in *Enciclopedia del Diritto*, Milano, 2014, 545-567; S. Tully, *A Human Right to Access the Internet? Problems and Prospects*, in *Human Rights Law Review*, 2, 2014, 175-195; K. Sangsuvan, *Balancing Freedom of Speech on the Internet under International Law*, in *North Carolina J of Int. L and Commercial R*, 3, 2014, 701-756; O. Pollicino, *Right to Internet Access: Quo Iuris?*, in A. von Arnould et al. (eds), *The Cambridge Handbook of New Human Rights*, Cambridge, 2020, 263-275.

²¹ Feldstein, *The Rise of Digital Repression*, cit., 34.

²² Merita rilevare come in Paesi in cui l'utilizzo di Internet è diffuso principalmente mediante servizi di telefonia mobile, molto spesso lo *shutdown* colpisca unicamente la rete mobile. È da evidenziare comunque come “as technology develops, the modalities for disrupting access to, and the use of, online spaces will evolve, and the definition of shutdowns and responses to them must change as well”, UN High Commissioner for Human Rights, *Internet Shutdowns*, cit., 2-3.

Così “it appears as internet access or a platform or service is available, but the level of interference is enough to render the service or resource effectively useless”²³. Questa particolare forma di *Internet shutdown* interferisce, in particolare, con la possibilità di condividere video e foto o di svolgere comunicazioni o video in diretta, con un impatto facilmente intuibile su tutte quelle manifestazioni di piazza durante le quali spesso i partecipanti utilizzano servizi di *live stream* per documentare la portata degli eventi o la reazione delle forze dell’ordine.

Viste dunque le caratteristiche e le forme attraverso le quali lo strumento oggetto di indagine può realizzarsi, particolare attenzione merita ora la ricognizione dei motivi – quantomeno espressi – addotti dalle pubbliche autorità al fine di giustificare il ricorso alla censura *della rete*. Ebbene, nella maggior parte dei casi, i governi invocano la necessità di realizzare *Internet shutdowns* dinanzi a situazioni di pericolo, concreto o presunto, per l’ordine pubblico o la sicurezza nazionale determinate soprattutto da grandi movimenti di protesta, spesso frutto di momenti di forte tensione tra cittadini e potere costituito e che potrebbero rischiare di sfociare – a parere delle pubbliche autorità – nella violenza o, in taluni contesti, addirittura in atti di terrorismo.

Secondo gli studi e i dati raccolti dalla organizzazione Access Now, circa la metà degli *shutdowns* realizzati tra il 2016 e il 2021 sono avvenuti in occasione di proteste e agitazioni politiche²⁴, mentre un numero significativo di blocchi della rete è stato registrato in concomitanza con elezioni politiche o importanti votazioni popolari. È questo il caso degli *Internet shutdowns* verificatisi, ad esempio, in Uganda, Nigeria e Bielorussia²⁵, mentre emblematico dell’utilizzo di tali strumenti al fine di assicurare – secondo quanto sostenuto dalle autorità – il ripristino e la tutela della sicurezza pubblica e nazionale è certamente il blocco generalizzato della rete operato dal governo egiziano nel 2011 in occasione di quella che è stata poi definita la “Primavera araba”²⁶; o ancora quanto avvenuto in Myanmar, nel periodo successivo al colpo di stato militare che ha deposto il governo di Aung San Suu Kyi, o quello più recente messo in atto dal governo Iraniano con lo scopo di limitare l’impiego di canali digitali di comunicazione e impedire il diffondersi – anche all’estero – di notizie, video e immagini riguardanti le manifestazioni di piazza seguite alla morte della giovane Mahsa Amini²⁷.

²³ Access Now, *Report. The Return of Digital Authoritarianism. Internet Shutdowns in 2021*, aprile 2022, 28.

²⁴ UN High Commissioner for Human Rights, *Internet Shutdowns*, cit., 6.

²⁵ Dal 2019, “election-related internet shutdowns were documented in Benin, Belarus, the Democratic Republic of Congo, Malawi, Uganda, Kazakhstan, and other countries globally. For instance, Uganda implemented a country wide internet shutdown for 5 days (13-18 January 2021) before, during, and after their general elections (14 January 2021) to curtail knowledge of opposition arrests and to stifle any opposition against proclaimed results. The blackout followed several days of blocking social media and messaging apps”, UN High Commissioner for Human Rights, *Internet Shutdowns*, cit., 9. Per approfondimenti sugli *Internet shutdowns* operati nel Continente africano, si legga Rydzak, Karanja, Opiyo, *Dissent Does Not Die in Darkness*, cit.

²⁶ M. Aouragh, A. Alexander, *The Egyptian Experience: Sense and Nonsense of the Internet Revolution*, in *International Journal of Communication*, 5, 2011, 1344-1358.

²⁷ Per approfondimenti specifici sul caso Iraniano: M. Grinko, S. Qalandar, D. Randall, V. Wulf, *Nationalizing the Internet to Break a Protest Movement: Internet Shutdown and*

Internet shutdowns volti a garantire la sicurezza e l'ordine pubblico, però, si sono ravvisati anche in democrazie stabilizzate quali il Regno Unito e gli USA: in questi limitatissimi casi, tuttavia, il blocco della rete, durante proteste e dimostrazioni pubbliche, è risultato maggiormente limitato e circoscritto quanto a dimensioni e durata²⁸.

Ma vi sono ulteriori motivazioni dichiarate dai governi per legittimare l'impiego di *Internet shutdowns*: tra queste vi è sia la necessità di garantire il corretto e regolare svolgimento di esami o concorsi pubblici – di cui si dirà anche con riferimento al contesto indiano –, sia l'esigenza di controllare la diffusione di *fake news*, disinformazione e discorsi dell'odio; in questi casi, anziché intervenire in maniera mirata per eliminare eventuali specifici contenuti ritenuti illegittimi – per quanto persino tali pratiche non siano esenti da critiche, neppure nell'UE²⁹ –, si agisce in maniera generalizzata e indiscriminata operando non una censura *in rete* bensì una censura *della* rete, come avvenuto in Bielorussia, Congo, Etiopia e Myanmar, Indonesia³⁰.

L'ampliarsi degli interessi posti alla base dell'adozione di *Internet shutdowns*, unitamente all'aumento di questi ultimi non solo nel numero³¹ e

Counter-Appropriation in Iran of Late 2019, in AA.VV., *Proceedings of the ACM on Human-Computer Interaction*, 6, 2022, 1-21; V. Wulf, K. Aal, M. Rohde, *The Personal is Political: Internet Filtering and Counter Appropriation in the Islamic Republic of Iran*, in *Computer Supported Cooperative Work*, 31, 2022, 373-409. Per un'analisi della delicata situazione politico-istituzionale entro cui l'adozione di *Internet shutdowns* si inserisce, si rimanda a C. Sbaillò, *Iran: un terremoto nella Umma, che avrà conseguenze anche nei rapporti tra democrazie e autocrazie*, in questa Rivista, 4, 2022, XI-XIX. Sul blocco di Internet in Myanmar, invece: M. Ryan, M.V. Tran, *Democratic Backsliding Disrupted: The Role of Digitalized Resistance in Myanmar*, in *Asian J of Comparative Politics*, 0, 2022.

²⁸ In particolare, "in 2019, British police shut down the public's access to the Internet on the London underground to tackle planned protests by climate protesters. A similar tactic had been already implemented in the epitome of technological liberalism, San Francisco, in 2011, where mobile-Internet and phone services were shut down to control a protest in the subway", De Gregorio, Stremlau, *Internet Shutdowns and the Limits of Law*, cit., 4225; con riferimento al caso inglese, è stato sottolineato come "even though this did not have much effect on the ability for citizens to connect to the internet through other networks, it stands as an example of liberal democracies practicing a mass censorship measure to stop protests", N. Joshi, *Internet Shutdowns During Protests: A Practice in Digital Authoritarianism*, Dublino, 2020, 11. Su tali casi, si vedano anche M. Yang, *The Collision of Social Media and Social Unrest: Why Shutting Down Social Media Is the Wrong Response*, in *Northwestern J of Tech. and Intellectual Property*, 7, 2013, 707-728; P. Vargas-Leon, *Tracking Internet Shutdown Practices: Democracies and Hybrid Regimes*, in F. Musiani et al. (eds), *The Turn to Infrastructure in Internet Governance*, New York, 2016, 167-188.

²⁹ Si rimanda sul punto *infra* para. 4.

³⁰ UN Human Rights Council, *Disinformation and Freedom of Opinion and Expression. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Irene Khan, A/HRC/47/25*, 13 aprile 2021, 10. Sul tema, anche, S. Jamil, *The Rise of Digital Authoritarianism: Evolving Threats to Media and Internet Freedoms in Pakistan*, in *World of Media*, 3, 2021; R.A. Rahman, S. Tang, *Fake News and Internet Shutdowns in Indonesia: Symptoms of Failure to Uphold Democracy*, in *Constitutional Review*, 1, 2022, 151-183.

³¹ Per fornire, sinteticamente, alcuni dati tratti dai siti di AccessNow, Google Jigsaw e Internet Freedom Foundation, si evidenzia come dal 2016 al 2021 siano stati documentati 931 *Internet shutdowns* nel mondo, in 74 diversi Paesi, con un aumento esponenziale del 49% rispetto ai dati relativi all'intervallo di tempo 2012-2016.

nella durata³² ma anche nelle modalità di realizzazione via via sempre più sofisticate e targettizzate, hanno così recentemente portato allo sviluppo di un vivace ed attento dibattito nella società civile, grazie soprattutto all’operato di talune ONG o enti di ricerca³³, nonché in seno a governi, parlamenti, corti e dottrina. Ciò ha contribuito ad accendere i riflettori sulle delicate questioni giuridiche sottese nonché sui diritti fondamentali colpiti e limitati dal ricorso a simili strumenti.

Sotto tale rilevante profilo, infatti, le restrizioni della disponibilità di Internet hanno mostrato di avere un impatto significativo tanto sui diritti alla libertà di espressione e di riunione³⁴, come di grande evidenza, quanto sull’accesso alle informazioni – non a caso gli *shutdowns* sono stati anche definiti “systematic information blackout” – e, in ultima analisi, su quel *government by discussion* inteso come principio, “patrimonio genetico” delle democrazie, “secondo cui deve essere garantito un confronto pubblico e aperto tra idee diverse e confliggenti, che permetta a ogni cittadino di scegliere la verità. Di qui l’importanza della tutela del dissenso, che fa parte del regime costituzionale della libertà di informazione nelle democrazie pluralistiche, della garanzia di avere fori pubblici aperti alle discussioni dove possono essere esposte le idee più disparate (..), della tutela del pluralismo delle fonti di informazione”³⁵.

Anche gli effetti limitativi del blocco della rete rispetto ai diritti sociali e alle libertà economiche sono stati oggetto di attenzione: è stato infatti rilevato come gli *Internet shutdowns* provochino forti restrizioni al godimento di molteplici diritti sociali che ormai si esercitano anche – e in taluni casi, addirittura primariamente – tramite Internet³⁶; questa affermazione del resto è stata tragicamente confermata dall’esperienza pandemica, durante la quale i diritti all’educazione, al lavoro e alla salute hanno trovato nelle nuove tecnologie e in Internet un potente mezzo di garanzia³⁷.

³² Gli *Internet shutdowns*, infatti, possono durare poche ore, alcuni giorni oppure mesi e addirittura anni. Il blocco di Internet adottato in Myanmar nel febbraio 2021, nonché quello che ha colpito la popolazione anglofona del Cameroon o gli abitanti del territorio del Jammu e Kashmir in India, sono solo alcuni esempi di *Internet shutdowns* di durata estremamente estesa.

³³ Si pensi ad Access Now o Internet Freedom Foundation.

³⁴ Del resto, “solo chi è rimasto alla preistoria del diritto e si aggira ancora armato di clava, cercando di inventare la ruota, non si rende conto del passaggio epocale che si è verificato nelle società evolute in questi anni: la possibilità di accedere sempre, dovunque a tutta la conoscenza racchiusa in testi digitali; la possibilità di comunicazione sempre dovunque e a costi minimi con tutti; la possibilità di diffondere sempre e dovunque a tutto il mondo il proprio pensiero”, V. Zeno-Zencovich, *Perché occorre rifondare il significato della libertà di manifestazione del pensiero*, in *Percorsi costituzionali*, 1, 2017, 71, così che l’impatto di una restrizione dell’accesso ad Internet su tali diritti diviene lampante.

³⁵ G. Pitruzzella, *La libertà di informazione nell’era di Internet*, in *MediaLaws*, 1, 2018, 10.

³⁶ *Ex multis*, A. Morelli, *Il diritto alla salute nell’era digitale: profili costituzionalistici*, in *MediaLaws*, 1, 2012; G. Pesci, *Il digital divide, l’uguaglianza sostanziale e il diritto all’istruzione*, in *Rivista internazionale di informatica giuridica*, 2, 2021, 259-286.

³⁷ In questi termini E. Celeste, *Digital Constitutionalism. The Role of Internet Bills of Rights*, Abingdon, 2023, specialmente 30 ss.; ma anche M. Nisticò, P. Passaglia (a cura di), *Internet e Costituzione*, cit.; T.E. Frosini, O. Pollicino, E. Apa, M. Bassini (a cura di), *Diritti e libertà in Internet*, Milano, 2017.

Diversi studi hanno, inoltre, dimostrato le conseguenze degli *Internet shutdowns* sulla libertà di iniziativa economica, specialmente in settori ormai altamente digitalizzati (bancario, finanza, e-commerce, ma anche turismo e trasporti). La Brookings Institution, in particolare, ha documentato, tra il 2015 e il 2016, una perdita economica di circa “US\$ 2.4. billion in GDP globally” causata dal frequente blocco di Internet in 19 Paesi, mentre la World Bank ha calcolato una perdita di circa 2.8 miliardi \$ nel solo Myanmar a causa dello *shutdown* operato tra febbraio e dicembre 2021³⁸.

In sintesi, dunque, gli strumenti di blocco generalizzato di Internet sono “easy to enact, but as instruments of repression, they bring two significant disadvantages. First, they lead to outsized economic impacts: because shutdowns impact every citizen in the country, they effectively bring commerce to a halt, particularly in high- technology economies. Second, (...) over an extended period, such shutdowns can lead to significant blind spots for the government and precipitate regime turnover. Newer research also indicates that Internet shutdowns may lead to increased rates of violent mobilization among protesters during blackouts”³⁹.

Le significative e allarmanti conseguenze, qui richiamate, prodotte dagli *Internet shutdowns* in ambito economico e politico, insieme alle serie riflessioni sulla legittimità delle finalità perseguite e sulla proporzionalità delle restrizioni dei diritti fondamentali realizzate mediante il blocco della rete⁴⁰, sono state così ben presto evidenziate in diversi documenti a livello internazionale e sovranazionale, divenendo base importante per la promozione di una maggiore discussione sul tema da parte di cittadini, legislatori ma anche, indirettamente, corti.

Un primo chiaro esempio di tale sviluppo può essere individuato nella Risoluzione 73/173 adottata dalla UN General Assembly il 17 dicembre 2018, riguardante la “Promotion and Protection of Human Rights and Fundamental Freedoms, Including the Rights to Peaceful Assembly and Freedom of Association”, nella quale viene espressamente richiesto agli Stati di “ensure that the same rights that individuals have offline, including the rights to freedom of expression, of peaceful assembly and of association, are also fully protection online (...) particularly by refraining from Internet shutdown that violate international human rights law”⁴¹. Facendo riferimento ai diritti e principi sanciti sia nella *Universal Declaration of Human*

³⁸ World Bank, *Digital & Telecom. Myanmar Infrastructure Monitoring*, aprile 2022; D.M. West, *Internet Shutdowns Cost Countries \$2.4. Billion Last Year*, Center for Technology Innovation at Brookings, 2016.

³⁹ Feldstein, *The Rise of Digital Repression*, cit., 40.

⁴⁰ “Oggi, nella società dell’informazione o, se si preferisce, nell’era dell’accesso (secondo la definizione di J. Rifkin), non avere accesso a Internet, significa vedersi precluso l’esercizio della più parte dei diritti di cittadinanza”, T.E. Frosini, *Il diritto costituzionale di accesso ad Internet*, cit., 23.

⁴¹ Similmente, lo *Human Rights Council* e lo *Special Rapporteur on the rights to freedom of peaceful assembly and of association*, hanno affermato come “blanket Internet shutdowns and generic blocking and filtering of services are considered by UN human rights mechanisms to be in violation of international human rights law”, UN Human Rights Council, *Ending Internet Shutdowns: A Path Forward. Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association*, A/HRC/47/24/Add. 2, 15 giugno 2021, 5.

Rights, sia nell'*International Covenant on Civil and Political Rights*⁴², viene sottolineato come “shutting the Internet is an inherently disproportionate response, given the blanket nature of the act, which blocks multiple uses of the Internet. As such, it violates the requirement of necessity and proportionality set out in international human rights law”⁴³.

Dinnanzi a tali considerazioni, non stupisce come anche nell'UE siano sorti quesiti sull'impiego potenziale degli *Internet shutdowns*: a seguito del diffondersi di tali strumenti su vasta scala in Egitto e Tunisia nel 2011, una apposita *Parliamentary question* è stata avanzata alla Commissione europea. La preoccupazione che anche in ambito eurounitario si potesse ricorrere al blocco della rete, del resto, trovava fondamento in alcune disposizioni normative nazionali, tra cui ad esempio quelle dell'Austria, che non escludevano la possibilità per le pubbliche autorità di ricorrere, in caso di specifiche esigenze securitarie, ad una interruzione generalizzata e

⁴² In particolare, si fa riferimento all'art. 19 (2) del *Covenant*, che fa eco all'art. 19 della *Universal Declaration*.

⁴³ UN Human Rights Council, *Disinformation and Freedom of Opinion and Expression*, cit., 10. Sotto il profilo del diritto internazionale – cui si vuole in questa sede solo fare un breve rimando, ponendo attenzione principalmente al tema in ottica comparata –, una prima rilevante fonte che entra in gioco con riferimento al fenomeno degli *Internet shutdowns* è da rinvenirsi nell'art. 19 dell'*International Covenant* sopra richiamato: al co. 3, in particolare, viene ribadita la necessità di tre requisiti determinanti la legittimità di restrizioni alla libertà di espressione. Secondo l'interpretazione fornita di tali requisiti, applicati allo specifico strumento degli *Internet shutdowns* operante una evidente compressione della *freedom of expression*, tali limitazioni: i) devono essere espresse da legge, ii) devono essere precise e non vaghe o eccessivamente ampie “for example, a law referring to public order or national security that does not more specifically address the surrounding circumstances and conditions for Internet shutdowns is likely not sufficiently precise”; iii) le restrizioni devono perseguire un “legitimate goal” ed essere proporzionate e necessarie al perseguimento dello stesso. Sulla base di queste considerazioni emerge come “Internet shutdowns generally do not meet those requirements. Given their indiscriminate and widespread impacts, Internet shutdowns very rarely meet the proportionality test”, Report of the Office of the UN High Commissioner for Human Rights, *Internet Shutdowns*, cit., 3. Ulteriore fonte di riferimento a livello internazionale è rappresentata, poi, dal *Constitution of the International Telecommunication Union (ITU)*, ratificato ormai da quasi tutti gli Stati del mondo: tale trattato prevede il diritto delle autorità pubbliche statali di bloccare i servizi di telecomunicazione – cui pare potersi ricondurre anche Internet – unicamente qualora sussista un pericolo per la sicurezza dello Stato o una violazione dell'ordine pubblico o della “decency” (Art. 34, co. 2). Per una puntuale analisi del diritto internazionale applicabile alla materia in esame e alla sua interpretazione, si rinvia a De Gregorio, Stremlau, *Internet Shutdowns and the Limits of Law*, cit.; ma anche J. Goldsmith, T. Wu, *Who Controls the Internet? Illusions of a Borderless World*, Oxford, 2006; B. Joyce, *Internet Freedom and Human Rights*, in *The European J of International L*, 2, 2015, 493-514; J. Clark et al., *The Shifting Landscape of Global Internet Censorship*, Berkman Klein Center for Internet & Society Research Publication, <https://dash.harvard.edu/handle/1/33084425>, 2017; H. Moynihan, *The Application of International Law to State Cyberattacks Sovereignty and Non-Intervention*, Chatham, 2019; F. Delerue, *Cyber Operations and International Law*, Cambridge, 2020; D. B. Sander, *Freedom of Expression in the Age of Online Platforms*, in *Fordham International L J*, 2020, 43, 939-1006; H. Kaur, *Protection Internet Access: A Human Rights Treaty Approach*, in *Brooklyn J of International L*, 46, 2021, 767-799.

volontaria di Internet⁴⁴. In risposta, la Commissione “considers the security, stability and resilience of the Internet and of other electronic communication technologies is a fundamental building block in democracy”, così affermando come qualsiasi limitazione dei diritti fondamentali debba essere appropriata, proporzionata e necessaria in una società democratica, nonché accompagnata da adeguate salvaguardie procedurali, anche qualora la garanzia di interessi securitari sia in gioco.

È allora proprio da queste posizioni che un serio dibattito non solo dottrinale ma anche giurisprudenziale ha preso le mosse: riconosciuto “il ruolo importante” svolto dalle “consolidate tecniche di bilanciamento, proporzionalità e ragionevolezza” al fine di “contemperare i diritti e i loro limiti”⁴⁵, le corti chiamate a pronunciarsi in merito alla legittimità degli *Internet shutdowns* hanno contribuito – e contribuiscono – a determinare il futuro impiego di tali strumenti. La giurisprudenza in materia ha assunto pertanto particolare rilievo: in taluni casi, come in quello indiano, che ci si appresta ad esaminare, il vaglio giurisdizionale ha finito col rappresentare un intervento essenziale, a fronte dell’inerzia dei legislatori, al fine di arginare i rischi di “techno-political measures” e “digital governance practices” passibili di tramutarsi, qualora prive di adeguata regolamentazione, in invasivi mezzi di controllo *della* rete e di repressione delle libertà e dei diritti *in* Internet⁴⁶.

3. Il contributo della giurisprudenza: potenzialità e criticità delle pronunce dei giudici indiani in materia di *Internet shutdown*

I provvedimenti con cui gli *Internet shutdowns* vengono disposti sono dunque stati oggetto, negli ultimi anni, di numerosi interventi giurisprudenziali. Tali decisioni – spesso inserite, come anticipato, in contesti geo-politici ed istituzionali molto diversi tra loro – dimostrano una molteplicità di approcci in materia: talune pronunce sono infatti caratterizzate da un vaglio di proporzionalità e necessità limitato e meno rigoroso, sovente accompagnato tanto da una lettura estensiva delle esigenze securitarie atte a giustificare la limitazione della rete, quanto dalla rilevazione dell’inesistenza di misure meno invasive in grado di raggiungere l’obiettivo perseguito⁴⁷. In diversi

⁴⁴ Si fa riferimento alla *Parliamentary Question P-002322/2011* del 3 marzo 2011, nella quale si cita ad esempio il para. 89 del *Telecommunications Act* austriaco del 2003. Anche nel Regno Unito, a titolo esemplificativo, vi sono disposizioni normative che riconoscono la possibilità, in capo a determinate autorità pubbliche, di ordinare un blocco della rete: “the Section 132 of the Communications Act of 2003 grants special powers to the ‘independent regulator and competition authority for the United Kingdom communications industries’, known as OFCOM. According to Section 132 of the Act, OFCOM can request to any United Kingdom-based ISP the suspension of the service in order to preserve the ‘public order’ or in case of a massive cyber-attack. This situation is considered part of the national security strategy of the United Kingdom”, Vargan-Leon, *Tracking Internet Shutdown Practices*, cit., 177.

⁴⁵ M. Olivetti, *Diritti fondamentali e nuove tecnologie*, in *Revista Estudos Institucionais*, 2, 2020, 403.

⁴⁶ Joshi, *Internet Shutdowns During Protests*, cit., 1.

⁴⁷ Interessante, in questo senso, è la giurisprudenza della *Supreme Administrative Court* egiziana che, con decisione del 24 marzo 2018, ha ribaltato la pronuncia del giudice di

altri casi, invece, le Corti hanno svolto uno scrupoloso controllo di legittimità, determinando infine l'invalidità delle disposizioni determinanti gli *Internet shutdowns*, sebbene sulla base di valutazioni differenti⁴⁸.

In tale contesto – e rimandando anche alle considerazioni metodologiche esposte in apertura del presente lavoro –, la giurisprudenza indiana risulta certamente meritevole di particolare attenzione e analisi, distinguendosi per numero di pronunce in materia, per rilevanza e spessore delle decisioni adottate e per accuratezza del vaglio di legittimità svolto, non a caso richiamato – in ottica comparata – anche dai giudici della Corte costituzionale ugandese in una più recente pronuncia del 27 aprile 2021⁴⁹.

Del resto, considerando il già citato primato mondiale per numero di interruzioni volontarie della rete detenuto dall'India⁵⁰, non stupisce che

primo grado che aveva condannato il precedente Presidente Mubarak e gli ex Primo Ministro Ahmed Nazif e Ministero dell'Interno Habib Al-Adly per aver illegittimamente imposto il primo *Internet shutdown* massivo e totale nel territorio egiziano, nelle date dal 28 gennaio al 2 febbraio 2011, in occasione delle rivolte di piazza che avevano dato vita alla c.d. “Primavera araba”. Diversamente dalla corte di prima istanza, i giudici di appello hanno ritenuto il blocco della rete conforme alla legge e giustificato da esigenze di tutela della sicurezza nazionale e di integrità del territorio. Sul punto si veda *The Case of Communications Suspension and Internet Shutdown During the 2011 Egyptian Revolution*, in *Global Freedom of Expression*, Columbia University, <https://globalfreedomofexpression.columbia.edu/cases/communications-suspension-and-internet-shutdown-case-during-the-2011-egyptian-revolution/>. Più complesse sono invece le considerazioni da sviluppare con riferimento alla sentenza del 25 giugno 2020 della Corte di giustizia della Comunità economica degli Stati dell'Africa occidentale (Corte dell'ECOWAS) avente ad oggetto la legittimità dell'*Internet shutdown* disposto in Togo: da un lato, infatti, i giudici hanno riconosciuto la legittimità, necessità e proporzionalità del blocco di Internet; dall'altro lato, invece, il provvedimento impugnato è stato censurato poiché assunto in assenza di una normativa chiara e precisa disciplinante l'adozione di simili strumenti (su tale pronuncia, F. Vona, *Internet shutdown: la Corte di giustizia dell'ECOWAS configura l'accesso ad Internet come una componente essenziale della libertà di espressione nel caso Amnesty International Togo et al. c. Repubblica Togolese*, in *Federalismi.it*, Focus Africa, 3, 2020). In altri casi, invece, i ricorsi contestanti la legittimità degli *Internet shutdowns* sono stati respinti sotto profili meramente formali: ne sono esempio la decisione del *Constitutional Council of Cameroon* (*Global Concern Cameroon v. Ministry of Posts and Telecommunications et al.*, 001/G/SCT/CC/2018, del 30 luglio 2018) o il caso deciso dalla Corte costituzionale ugandese *Unwanted Witness-Uganda v. Attorney General*, No. 0016/2017, 27 aprile 2021.

⁴⁸ Si richiamano in questo senso le decisioni: *CM Pak Limited v. The Pakistan Telecommunication Authority*, 42/2016, pronunciata dalla *High Court of Islamabad* (Pakistan) il 26 febbraio 2018; *Alliance of Independent Journalists v. Minister of Communication*, 230/G/TF/2019/PTUN-JKT, decisa dalla *Jakarta State Administrative Court* il 3 giugno 2020 (Indonesia); *Zimbabwe Lawyers for Human Rights and Media Institute of Southern Africa v. The Minister of State in the President's Office et al.*, Case No. *High Court* dello Zimbabwe, 265/19, del 21 gennaio 2021; *Chapter One Foundation v. Communications Technology Authority, High Court for Zambia*, 2021/HP/0955, del 17 marzo 2022.

⁴⁹ Nonostante il già indicato esito della pronuncia *Unwanted Witness-Uganda v. Attorney General*, i giudici non hanno mancato di rinviare, in quel caso, alla sentenza *Bhasin*, che verrà a breve analizzata, definendola “a good starting point to determine whether the shutdown of the internet during and after the 2016 General and Local Government Elections was consistent with the Constitution of Uganda”, p. 18.

⁵⁰ Basti pensare che nel 2019, ben 121 dei 213 *Internet shutdowns* registrati a livello globale hanno avuto luogo in India (Report di Access Now).

proprio qui la società civile si sia più volte attivata non solo ricorrendo a proteste e manifestazioni avverso gli *Internet shutdowns* ma anche richiedendo l'intervento dei giudici statali e federali, sino a promuovere l'intervento della Corte Suprema, mediante ricorso sancito dall'art. 32 Cost. Tale disposizione stabilisce il diritto "di investire la Corte suprema delle questioni riguardanti l'esercizio dei diritti conferiti dalla Parte III. In merito ai diritti fondamentali, la Suprema corte ha il potere di emettere ordinanze e provvedimenti, nonché atti di *habeas corpus*, *mandamus*, divieto, *quo warrant* e *certiorari* per l'esecuzione di uno qualsiasi dei diritti fondamentali"⁵¹.

E proprio da taluni ricorsi *ex art. 32 Cost.* ha avuto origine uno dei casi più noti e di maggior portata in materia di *Internet shutdown*: si tratta della sentenza *Anuradha Bhasin v. Union of India* (No. 1031/2019), del 10 gennaio 2020, nella quale, per la prima volta, la Corte Suprema si è confrontata con il delicato controllo di legittimità degli strumenti di blocco della rete.

Per cogliere appieno l'importanza di questa pronuncia, nonché del complesso contesto politico-sociale entro cui essa si inserisce, pare necessario svolgere alcune preliminari precisazioni sui fatti alla base del ricorso. Nel caso *Bhasin*, infatti, la decisione del governo federale di instaurare un *Internet shutdown* totale e generale nel *Jammu and Kashmir* (d'ora in avanti J&K) affonda le proprie radici nella situazione di forte tensione tra le autorità governative – locali e centrali – e la popolazione di quel territorio. Quest'ultimo, infatti, è stato per decenni oggetto di accesa contesa tra l'India e il confinante Pakistan, divenendo così drammaticamente teatro di scontri, anche sanguinosi. Proprio per tali articolate vicende storico-politiche, il J&K ha visto riconoscersi, sin dalla Costituzione indiana del 1950, uno *status* speciale rispetto agli altri stati federati, determinante la concessione di una propria costituzione e di specifiche autonomie sancite nell'art. 370 Cost. Questa disposizione delineava appunto il particolare rapporto tra J&K e l'Unione, tanto da essere considerata la più chiara dimostrazione della peculiare "costruzione federale indiana"⁵². Nel 2019, tuttavia, con l'emanazione del *Jammu and Kashmir Reorganization Act (Constitution Application to Jammu and Kashmir Order 2019)*, lo Stato federale

⁵¹ P. Viola, *Stato, sistema di governo, diritti e doveri nello sviluppo costituzionale indiano*, in D. Amirante (a cura di), *I sistemi costituzionali dell'Asia meridionale*, Milano, 2019, 97 ma anche M. Caielli, *Governo debole, giudiziario forte: alcune riflessioni sull'azione di pubblico interesse in India*, in *Forum di Quaderni costituzionali*, 2 novembre 2021. Sul ruolo della Corte suprema, si veda M.S. Bussi, *Il 'governo' della Magistratura e l'indipendenza del potere giudiziario in India*, in questa Rivista, 4, 2020, 5061-5077. Per approfondimenti sul ruolo della Corte suprema con riferimento alla tutela dei diritti fondamentali e alla *social action litigation*, si rimanda alla dottrina di U. Baxi, *Taking Suffering Seriously: Social Action Litigation in the Supreme Court of India*, in *Third World Legal Stud.*, 1985, 107-132; M.P. Jain, *Law and the Poor: Some Recent Developments in India*, in *J. of Malaysian and Comparative Law*, 13, 1986, 23-104; B. Baar, *Social Action Litigation in India: The Operation and Limitations of the World's Most Active Judiciary*, in *Policy Studies J.*, 1, 1990, 140-141; S. Deva, *Public Interest Litigation in India: A Critical Review*, in *Civil Justice Quarterly*, 28, 2009, 19-40; G. Gill, *The Social Justice Bench of the Supreme Court of India: A New Development*, in *Public Law*, 2, 2016, 392-401.

⁵² Viola, *Stato, sistema di governo, diritti e doveri nello sviluppo costituzionale indiano*, cit., 72. Sul punto, più specificamente, si legga anche A.G. Noorani, *Article 370. A Constitutional History of Jammu and Kashmir*, Oxford, 2011; A.S. Anand, *The Constitution of Jammu and Kashmir, Its Developments and Comments*, New Delhi, 2013.

ha deciso di revocare l'autonomia storicamente e costituzionalmente attribuita a tale territorio, riaccendendo peraltro mai sopite e profonde contese religiose, etniche e politiche con il confinante Stato del Pakistan. Il citato *Order* può certamente essere letto quale riflesso della politica fortemente nazionalista del Presidente Modi, che ha motivato tale intervento normativo sulla base della presunta pericolosità della concessa autonomia, ritenuta un'arma in grado di favorire il terrorismo musulmano⁵³.

Come prevedibile, questa controversa decisione ha scatenato non pochi dubbi e opposizioni sia nella dottrina⁵⁴, sia nella società civile, così che alcune proteste, in gran parte pacifiche, hanno portato i cittadini del territorio a riversarsi nelle strade e nelle piazze per esprimere il proprio dissenso⁵⁵. Allo scopo di sedare una situazione estremamente tesa e potenzialmente esplosiva, le autorità statali e federali hanno quindi rapidamente adottato stringenti misure di sicurezza, comprensive di un rigido coprifuoco e di restrizioni alla libertà di spostamento, nonché di limitazioni di Internet realizzate mediante il ricorso ad *Internet shutdowns* estremamente lunghi nel tempo, protrattisi addirittura per più di 500 giorni, tra il 2019 e il 2021⁵⁶.

Dinnanzi a tali misure, diversi ricorrenti hanno adito la Corte Suprema allo scopo di “seek issuance of an appropriate writ for setting aside or quashing any and all order(s), notification(s), direction(s) and/or circular(s) issued by the respondents [in questo caso il governo federale] under which any/all modes of communication including Internet, mobile and fixed line telecommunication services have been shut down or suspended or in any way made inaccessible or unavailable in any locality. Further the Petitioners sought the issuance of an appropriate writ or direction directing Respondents to immediately restore all modes of communication including mobile, internet and landline services”⁵⁷.

⁵³ Mulani, *The Politics of Internet Shutdowns*, cit.

⁵⁴ In dottrina taluni hanno ritenuto il decreto presidenziale illegittimo in quanto non in grado, da solo, di modificare una disposizione del testo costituzionale e rendendosi in questo caso piuttosto necessaria una procedura di revisione costituzionale. Per una ricostruzione del tema, T. Amico di Meane, *Una fina annunciata? La revoca dell'autonomia del Kashmir nel fragile federalismo indiano*, in *DPCE*, 1, 2020, 85-115; W. Menski, M. Yousuf (eds), *Kashmir After 2019: Completing the Partition*, New Delhi, 2021; D. Parth, *The De-Operationalization of Article 370 of the Indian Constitution*, in *Minnesota J of Int L*, 1, 2022, 259-280.

⁵⁵ Sul complesso argomento delle tensioni in quei territori, legate anche a delicati fattori religiosi, si legga L. Colella, *Fattore religioso, diritto e normazione in India, Pakistan e Bangladesh*, in questa Rivista, n. Sp. 2021, 1675-1698.

⁵⁶ Mulani (in *The Politics of Internet Shutdowns*, cit.) parla di un *Internet shutdown* di 552 giorni tra agosto 2019 e febbraio 2021; questo è stato pertanto definito “the longest shutdown in the history of Internet shutdown”, S. Moinuddin, *Digital Shutdowns and Social Media*, Berlino, 2021, in particolare nel capitolo “Spatial Mapping of Digital Shutdown in India”.

⁵⁷ Para. 5 della sentenza. Secondo i *Petitioners* – tra cui Anuradha Bhasin, editor del *Kashmir Times Srinagar Edition* – il ricorso ad uno *shutdown* generalizzato ed integrale non risulta proporzionato: nonostante la *Section 5* dell'*Indian Telegraph Act*, 1885 preveda la possibilità di promuovere restrizioni delle comunicazioni, secondo i *Petitioners* “there can be no blanket orders, as it would amount to a complete ban. (...) The least restrictive option must be put in place. (...) The State needs to balance the safety of the people with their lawful exercise of their fundamental rights”, para. B, p. 11.

La Corte, dunque, in una lunga e articolata pronuncia, ha innanzitutto riportato la questione sottoposta entro i confini del complesso rapporto tra garanzia delle libertà ed esigenze securitarie, manifestatosi nel caso concreto nella contrapposizione tra, da un lato, tutela della libertà di espressione⁵⁸, in primis, nonché di altri diritti costituzionalmente riconosciuti tra cui “freedom of movement, right to free trade and avocation”, e dall’altro la garanzia della sicurezza nazionale e dell’ordine pubblico dinnanzi a potenziali disordini e violenze foriere anche di una possibile infiltrazione di terroristi in zone già scenario di cruenti scontri tra musulmani e induisti.

Pur dando atto, come sostenuto dai *Respondents*, della impossibilità tecnica di distinguere i potenziali terroristi o i “troublemakers” dai cittadini che intendono manifestare il proprio pensiero in rete o mediante riunioni pubbliche (para. 17), nonché della pericolosità dei social media che possono facilmente essere impiegati quali mezzi per incitare alla violenza⁵⁹, la Corte si è posta quale principale quesito quello di determinare la legittimità delle limitazioni dei diritti fondamentali motivate da esigenze securitarie.

Per fare ciò, i giudici hanno fornito alcune utili coordinate sulla portata della “freedom of expression over the medium of internet”: se, al giorno d’oggi, Internet rappresenta il mezzo più accessibile e maggiormente impiegato per lo scambio di informazioni (para. 22)⁶⁰, diviene allora importante distinguere “between internet as a tool and the freedom of expression through the internet” (para. 25). Ecco, quindi, che il diritto alla libertà di espressione, anche qualora esercitato nel contesto digitale e dunque mediante Internet, diviene “integral part of Art. 19(1)(a) and accordingly, any restriction on the same must be in accordance with Article 19(2) of the Constitution”⁶¹ (para. 26); sempre sotto l’ombrello di tale disposizione costituzionale sono fatti rientrare anche “the freedom of trade and commerce through the medium of the Internet (art. 19(1)(g))” e il “right to disseminate information” (para. 27). La Corte, dunque, riconduce la dimensione digitale del diritto alla libertà di espressione alla tutela costituzionale già riconosciuta nella dimensione “analogica”, senza spingersi a vagliare la spinosa e dibattuta questione – che nessuna delle parti in giudizio aveva peraltro promosso – relativa alla natura di diritto fondamentale a sé stante dell’accesso ad Internet. Facendo riferimento sempre all’art. 19, la Corte ha poi stabilito come i diritti in esso sanciti possano essere sottoposti a

⁵⁸ Si fa riferimento all’art. 19, para. 1, della Costituzione Indiana.

⁵⁹ “The purpose of the limited and restricted use of internet is to ensure that the situation on the ground would not be aggravated by targeted messages from outside the country. Further, the Internet allows for the transmission of false news or fake images, which are then used to spread violence. The dark web allows individuals to purchase weapons and illegal substances easily”, para. 18.

⁶⁰ I giudici svolgono alcune interessanti considerazioni anche sul rapporto tra diritto e nuove tecnologie, assimilati, questi ultimi, ad elementi che “seldom mix, like oil and water. There is a consistent criticism that the development of technology is not met by equivalent movement in the law”, para. 24.

⁶¹ L’art. 19, para. 2, prevede la possibilità di comprimere il diritto alla libertà di espressione qualora ciò sia previsto da una legge e “in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub-clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence”.

limitazioni purché queste, come previsto dal secondo comma, siano “sanctioned by law”, “reasonable”, e adottate al fine di tutelare “interests of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence”.

Dinnanzi a queste preliminari considerazioni, i giudici si sono pertanto apprestati a valutare prima la sussistenza e il rispetto dei requisiti di legittimità e poi un attento vaglio di proporzionalità⁶² finalizzato a garantire che le restrizioni dei diritti fondamentali non siano arbitrarie o eccessive, “beyond what is required in the interests of the public” (para. 53)⁶³.

A tal fine, la Corte ha proposto una preliminare efficace sintesi del test di proporzionalità, frutto anche di una vasta analisi comparata⁶⁴ e che merita qui di essere riportata in tutta la sua ampiezza: “the possible goal of such a measure intended at imposing restrictions must be determined and legitimate”; “the authorities must assess the existence of any alternative mechanism in furtherance of the aforesaid goal. (...) Only the least restrictive measure can be resorted to by the State, taking into consideration the facts and circumstances”; il provvedimento (nel caso specifico l’*Order*) che dispone la limitazione dei diritti fondamentali deve inoltre essere “supported by sufficient material and should be amenable to judicial review”; “the degree of restriction and the scope of the same, both territorially and temporally, must stand in relation to what is actually necessary to combat an emergent situation” (para. 71).

Procedendo allora a valutare la legittimità dell’obiettivo perseguito, i giudici ravvisano nell’esigenza di tutelare la sicurezza e l’ordine pubblico un motivo sufficiente a giustificare il ricorso a misure restrittive delle libertà dei cittadini (para. 76). Ciò considerando anche la storia del martoriato territorio del J&K, definito “a hot bed of terrorist insurgencies for many years” (para. 35), nonché riconoscendo il ruolo di Internet nello sviluppo del terrorismo moderno⁶⁵.

Il rispetto però degli altri requisiti di proporzionalità e necessità risulta determinante per lo svolgimento della pronuncia: a tal fine, in particolare, vengono esaminate le normative, pur non unicamente e specificamente riferite agli *Internet shutdowns*, che costituiscono base giuridica per l’emanazione di *Orders* di interruzione della connessione. Esse sono

⁶² “Proportionality is an essential facet of the guarantee against arbitrary State action because it ensures that the nature and quality of the encroachment on the right is not disproportionate to the purpose of the law”, para. 47.

⁶³ Richiamando la pronuncia *Modern Dental College & Research Centre v. State of Madhya Pradesh*, 2016, 7 SCC 353, viene stabilito come nessun diritto abbia natura assoluta, essendo quindi passibile di limitazioni.

⁶⁴ La Corte ricostruisce il vaglio di proporzionalità come definito non solo dalla *case-law* indiana ma anche – come spesso accade – in ottica comparata, richiamando peraltro il simpatico aforisma di Lord Diplock “you must not use a steam hammer to crack a nut, if a nutcracker would do”, così ritenendo che “proportionality is all about means and ends” (para. 50). In questo senso la Corte riconosce che “a proper balancing of the competing principles (...) is one of the expressions of the multi-faceted nature of democracy”, para. 55.

⁶⁵ “Being used to support fallacious proxy wars by raising money, recruiting and spreading propaganda/ideologies. The prevalence of the Internet provides an easy inroad to young impressionable minds”, para. 36.

identificate in tre fonti: l'*Information Technology Act, 2000*, la *Section 144* del Codice di procedura penale⁶⁶ e la *Section 7* (c.d. *Suspension Rules*) del *Telegraph Act*. Sulla base di tali disposizioni, misure determinanti il blocco dei servizi Internet possono essere attivate dalle pubbliche autorità⁶⁷ solo qualora si verifichi una “public emergency” o un “interest of public safety”, che devono tuttavia risultare di “serious nature and need to be determined on a case by case basis” (para. 93).

Esaminando poi, più nel dettaglio, le condizioni stabilite dalle *Suspension Rules*, emerge la necessità che gli *Orders* adottati sulla base delle *Suspension Rules* siano liberamente accessibili, e vengano dunque notificati e messi a conoscenza dell'intera cittadinanza, anche allo scopo – di estremo rilievo – di consentire il ricorso a meccanismi di *judicial review* e a strumenti di garanzia che risulterebbero impossibili da attivare qualora nessuna informazione sui provvedimenti, sulla loro esistenza e sul loro contenuto, venisse messa a disposizione.

Riconoscendo che “complete broad suspension of telecom services, be it the Internet or otherwise, being a drastic measure, must be considered by the State only if necessary and unavoidable” (para. 99), i giudici hanno affermato di conseguenza come gli *Internet shutdowns* adottati sulla base delle *Suspension Rules* debbano risultare limitati nel tempo (così che un ordine determinante una sospensione indefinita e illimitata dei servizi Internet è da ritenersi vietato, para. 100) e accompagnati da adeguate salvaguardie procedurali tali da limitare il rischio di abusi da parte delle pubbliche autorità. In questo senso, il *Review Committee*, già previsto dalla normativa in esame e composto da *Senior State Officials*, viene inteso quale organo qualificato a svolgere un controllo sulla proporzionalità – anche sul fronte della durata – della misura restrittiva adottata.

Con riferimento invece alla *Section 144* C.p.p., tale previsione stabilisce la possibilità per lo Stato di ricorrere, anche preventivamente, a misure volte a mantenere la pace pubblica e ad affrontare imminenti minacce alla sicurezza⁶⁸. Simili misure, tuttavia, non possono assumere il carattere di un “blanket order”, ma, al contrario, devono indicare, in forma scritta, i fatti materiali che costituiscono fondamento dell'*Order* restrittivo, precisandone anche i limiti temporali che per legge non possono essere superiori a 2 mesi, estensibili però per ulteriori 6 mesi. La lettura interpretativa della disposizione normativa richiamata, fornita dalla Corte alla luce del principio di proporzionalità, riconosce poi l'illegittimità di misure dal carattere

⁶⁶ Questa disposizione, in particolare, è stata oggetto di attenzione da parte della dottrina, che ha rilevato come l'ampiezza e vaghezza del dettato normativo di tale *Section* apra a possibili abusi di potere: “Section 144 is a useful instrument when dealing with emergencies. However, in absence of a lucid definition, the unrestricted and extraordinary power this provision vests with the Executive, coupled with limited judicial oversight, makes it highly susceptible to misuse by the ruling government”, R. Agarwal, *Section 144: A Contemporary Analysis Questioning the Arbitrary Imposition of Internet Shutdown in India*, in *Jus Corpus Law Journal*, 2, 2021, 42.

⁶⁷ Nello specifico: “Secretary to the Government of India in the Ministry of Home Affairs, in the case of Government of India or the Secretary to the State Government in-charge of the Home Department in the case of a State Government”, para. 84.

⁶⁸ Per un'analisi di tale disposizione, N. Nayak, *The Legal Disconnect: An Analysis of India's Internet Shutdown Laws*, in *IFF Working Paper*, 1, 2018, 1-22.

illimitato e arbitrario (para. 109) o impiegate per fronteggiare un pericolo meramente eventuale (si parla in questo caso di “likelihood” e di “mere tendency”, para. 109).

Sulla base di queste premesse, la Corte ha conseguentemente mosso considerazioni di primario rilievo sulla legittimità del ricorso a strumenti di limitazione della rete. Le parole impiegate dai giudici sono quantomai significative: “the power under *Section 144* cannot be used as a tool to prevent the legitimate expression of opinion or grievance or exercise of any democratic rights. Our Constitution protects the expression of divergent views, legitimate expression and disapproval, and this cannot be the basis for invocation of *Section 144*, unless there is sufficient material to show that there is likely to be an incitement to violence or threat to public safety or danger” (para. 118). Non viene, pertanto, esclusa *in toto* la possibilità di ricorrere ad *Internet shutdowns* generalizzati, cioè volti a colpire l'intera popolazione di un territorio: questo perché in taluni casi è concretamente impossibile distinguere tra “the subject of protection under these orders and the individuals against whom these prohibitory orders are required to be passed” (para. 124). Nondimeno, riconoscendo il reale pericolo che simili strumenti sfocino in una seria lesione sproporzionata e illegittima dei diritti fondamentali, i giudici hanno dichiarato come “orders passed mechanically or in acryptic manner cannot be said to be orders passed in accordance with law” (para. 134). Viene evidenziato quindi come gli *Orders* in materia non possano essere impiegati “in a casual and cavalier manner”, inverandosi in disposizioni “unreasoned” e “un-notified” (para. 129) che finirebbero, in ultima istanza, con l'impedire ai cittadini di poter portare le proprie doglianze dinnanzi al *Review Committee* o alle Corti (in primis la High Court).

Al termine della ricca disamina delle disposizioni previste dall'ordinamento indiano atte a consentire il blocco della rete nonché delle condizioni di legittimità stabilite dalle stesse, la Corte ha utilmente indicato i requisiti specifici che devono sussistere ed essere rispettati ogniqualvolta venga stabilito un *Internet shutdown*, al fine di considerare tali misure proporzionate e necessarie. Innanzitutto, sia con riferimento alle *Suspension Rules* sia alla *Section 144* C.p.p., è richiesta la presenza di un pericolo e di una situazione emergenziale non meramente potenziale; tali strumenti non possono in nessun caso essere utilizzati per sopprimere o limitare il legittimo esercizio della libertà di espressione, del dissenso o di altri “democratic rights”. I *material facts* sulla cui base si fonda il ricorso a tali restrizioni della rete devono essere indicati con precisione; tra tutte le possibili limitazioni della connessione, in termini di estensione, dovrà essere scelta la misura meno intrusiva e invasiva dei diritti fondamentali; sotto il profilo temporale, “repetitive orders would be an abuse of power”, determinando quindi la necessaria temporaneità – specificamente dettagliata e precisata nell'atto stesso – degli *Internet shutdowns*; tutti gli *Orders* adottati devono essere poi poter essere soggetti a *judicial review*; l'apposito *Review Committee* invece deve svolgere revisioni periodiche al fine di verificare la persistenza dei requisiti di legittimità.

Sulla base di tali considerazioni e requisiti, estremamente precisi, la Corte ha quindi, infine, rinvenuto significative lacune nei provvedimenti oggetto di ricorso nel caso concreto. Da qui l'ordine ai *Respondents* non solo di revisionare tutti gli atti adottati alla luce dei principi e delle condizioni di

legittimità sanciti nella pronuncia stessa, ma anche di revocare gli *Orders* eventualmente considerati illegittimi. La Corte ha inoltre stabilito che “the State/concerned authorities are directed to consider forthwith allowing government websites, localized/limited e-banking facilities, hospital services and other essential services, in those regions, wherein the internet services are not likely to be restored immediately” (para. 152), senza tuttavia aggiungere alcun riferimento alle possibili difficoltà tecniche di realizzazione di tale specifica tutela.

La dettagliata analisi, qui proposta, è parsa necessaria ed imprescindibile per comprendere appieno il portato della lunga sentenza della Corte suprema, chiamata ad affrontare per la prima volta il tema, di estrema delicatezza e rilievo, della legittimità degli *Internet shutdowns*⁶⁹. L’approccio attento dei giudici è stato accolto con favore dai ricorrenti e dalla società civile, sia per l’importante affermazione della tutela costituzionale della libertà di espressione e dell’accesso alle informazioni anche qualora essi siano esercitati in Internet, sia per la determinazione di criteri e requisiti di proporzionalità e necessità che hanno – quantomeno in parte – sopperito alla vaghezza e generalità delle disposizioni normative in materia. “The verdict established the law on Internet shutdowns, placing a strong focus on the principles of proportionality, necessity and reasonableness (...). Furthermore, the Court emphasized citizens’ rights to know about government actions and stuck a balance between citizens’ liberties and security”⁷⁰: in tale ottica, i requisiti⁷¹ della conoscibilità, della temporaneità e determinatezza delle restrizioni della rete, nonché la predisposizione di chiari elementi di fatto alla base del ricorso a simili strumenti, insieme alla dichiarata illegittimità di *Orders* aventi natura “unreasoned”, “indefinite” e “repetitive”, rappresentano solidi confini entro cui l’intervento delle autorità governative deve necessariamente muoversi per considerarsi legittimo. La previsione di una maggiore trasparenza e chiarezza degli *Orders*, la possibilità di ricorrere al meccanismo di *judicial review* e l’istituzione di apposite autorità di controllo, contribuiscono inoltre a limitare la discrezionalità dei poteri pubblici e, dunque, il pericolo di abusi.

Se, sotto i profili evidenziati, la pronuncia pare assolutamente andare nella direzione di una più solida garanzia dei diritti fondamentali, essa non è stata comunque esente da osservazioni critiche⁷². I giudici, infatti, non sono giunti ad escludere *in toto* la legittimità degli *shutdowns* generalizzati, di ampia portata e indirizzati all’intera cittadinanza di vasti territori; hanno piuttosto indicato dei paletti di legittimità, da taluni considerati però eccessivamente vaghi e forieri di interpretazioni anche meno garantiste da parte delle pubbliche autorità. In altre parole, se viene riconosciuta

⁶⁹ Merita evidenziare come “the decision was given by a three-judge bench of the Supreme Court. Therefore, it establishes a binding precedent on all Courts within its jurisdiction, unless overruled by a larger bench of the Supreme Court”, Global Freedom of Expression, Columbia University, <https://globalfreedomofexpression.columbia.edu/cases/bhasin-v-union-of-india/>.

⁷⁰ C.V. Sarma, *Case Commentary Anuradha Bhasin*, in *Indian J of Legal Rev*, 5, 2022, 3.

⁷¹ Parla di “guidelines” Sarma, *Case Commentary*, cit., 5.

⁷² Si veda in particolare lo studio della pronuncia da parte di Global Freedom of Expression, Columbia University, <https://globalfreedomofexpression.columbia.edu/cases/bhasin-v-union-of-india/>.

l'illegittimità di qualsiasi blocco della connessione volto a limitare l'esercizio libero e pacifico di diritti costituzionalmente riconosciuti (di espressione e di riunione in particolare), non risulta invece del tutto chiaro il confine – e la possibilità di stabilirlo con chiarezza – tra giustificata esigenza di garanzia della sicurezza, da un lato, e intenzionale limitazione “of any democratic rights” dall'altro. Insomma, la determinazione della sussistenza di una reale emergenza – e non di un potenziale timore che legittime manifestazioni di dissenso possano tramutarsi in disordini violenti o possano mettere in discussione il potere costituito⁷³ – pare suscettibile, sotto questi profili, di un margine di discrezionalità che rischia di minare la portata concreta dei requisiti stabiliti nella sentenza. Infine, la decisione di non provvedere ad un ordine di ripristino della connessione bensì di rimettere alle autorità governative la valutazione circa la sussistenza delle condizioni indicate e del vaglio di proporzionalità dettagliato dai giudici, è parsa criticabile da chi avrebbe voluto una posizione finale più netta e precisa da parte della Corte⁷⁴.

Proprio tali ultime critiche – in parte peraltro confermate dal persistente vasto ricorso agli *Internet shutdowns*⁷⁵ successivo alla decisione esaminata – sono state riproposte e riaffermate anche dinnanzi ad una ulteriore pronuncia della Corte suprema, giunta a distanza di pochi mesi dal caso *Bhasin*: nella decisione *Foundation for Media Professionals v. Union Territory of Jammu and Kashmir*, No. 10817/2020 dell'11 maggio 2020, infatti, i giudici, dopo aver ripercorso i tratti salienti e i principi sanciti nella precedente sentenza in materia, hanno ordinato l'istituzione di uno *Special Committee* col compito di riconsiderare la legittimità delle continue restrizioni della connessione nel territorio del J&K, nel quale Internet era stato da ultimo oggetto non di un totale blocco bensì di un rallentamento a 2G.

In questo caso i giudici, pur rilevando che i *Suspension Orders* adottati non risultavano adeguatamente motivati – essendo privi di indicazioni quanto ai *material facts* comprovanti la necessità di uno *shutdown* generalizzato⁷⁶ –, hanno nondimeno individuato la sussistenza, in quelle

⁷³ Del resto anche la *High Court* di Calcutta, in *Sanmay Banerjee v. State of West Bengal et al.*, WP 21526/2019 ha affermato come “even the Judiciary and the Legislature are not exempt from fair criticism. This is what the freedom of speech and expression, as enshrined in the Constitution is all about. It is the criticism which helps in good governance and keeps a leash on public functionaries, providing a touchstone for the Executive to test the worth of their public endeavors”. Ancora, in *Kishori Mohan v. State of West Bengal* AIR 1972 SC 1749, la Corte suprema aveva stabilito come “mere criticism of the government does not tantamount to public disorder”.

⁷⁴ Sul punto Agarwal, *Section 144*, cit., e Global Freedom of Expression, Columbia University, <https://globalfreedomofexpression.columbia.edu/cases/bhasin-v-union-of-india/>.

⁷⁵ “Kris Ruijgrok’s study observes that these guidelines [adottate nella sentenza *Bhasin*] are not being followed by state officials across India. Reasons for this weak enforceability could include overly broad legal terminology (when is or isn’t a security issue a “public emergency”?) and a lack of public transparency (the proceedings and consequences of the shutdown Review Committee meetings are unknown to the public), each of which makes it difficult for the public to hold officials accountable for abuses of power”, Mulani, *The Politics of Internet Shutdowns*, cit.

⁷⁶ “Our attention is drawn to the fact that blanket orders have been passed for the entire territory rather than for specific affected areas”, para. 18.

zone, di “compelling circumstances of cross border terrorism” (para. 19)⁷⁷ tali da dimostrare l’esistenza di potenziali pericoli per la sicurezza nazionale e l’ordine pubblico. Le valutazioni sulla concretezza o fondatezza delle possibili minacce non vengono però ulteriormente approfondite dalla Corte: quest’ultima attribuisce piuttosto ad uno *Special Committee*, appositamente istituito, la valutazione della necessità e proporzionalità degli *Orders* adottati. Tale commissione, guidata dall’*Indian Home Secretary* e composta da “Secretaries at national as well as State level”, viene altresì chiamata ad esaminare la sussistenza ed appropriatezza di alternativi strumenti, suggeriti dai *Petitioners* e determinanti restrizioni meno invasive (para. 24). Pur riconoscendo come l’ampliamento della disponibilità di Internet mobile a velocità 4G sia certamente “desirable and convenient”, i giudici affermano parimenti la legittima esigenza di reprimere le minacce alla sicurezza derivanti da coloro che cercano di infiltrarsi nel territorio indiano e destabilizzare l’integrità della nazione; esigenza, questa, peraltro estremamente sentita dinnanzi a numerosi tragici avvenimenti che avevano portato alla morte di cittadini e forze dell’ordine (para. 14).

In questo senso, ancora una volta, la posizione dei giudici è stata oggetto di critiche. Ciò non solo per le problematiche già evidenziate con riferimento alla decisione *Bhasin* – e quindi la vaghezza di alcuni concetti stabiliti e la mancata valutazione della necessità delle misure adottate –, ma anche per la specifica composizione del *Committee* istituito, che vede al suo interno membri dell’esecutivo, appartenenti quindi alla stessa autorità che ha adottato, in prima istanza, le restrizioni: la mancanza di quei fondamentali caratteri di terzietà ed indipendenza degli organi di controllo è stata ritenuta in grado di limitare fortemente l’efficacia del vaglio operato e dunque la garanzia offerta⁷⁸.

Nonostante le criticità emerse e i limiti evidenziati nella richiamata giurisprudenza della Corte suprema⁷⁹, non può non rilevarsi come la sentenza *Bhasin* abbia portato, in diversi casi successivi decisi da altre corti indiane, ad un attento controllo di legittimità e ad una censura di *Orders* determinanti *Internet shutdowns* ritenuti in violazione dei principi di proporzionalità e necessità. E’ il caso della pronuncia della *High Court* di Calcutta, del 18 luglio 2022 (*Ashlesh Biradar v. State of West Bengali*, WPA/104/2022), nella quale il *vademecum* determinato dalla *Supreme Court* nel precedente del 2020 è stato utilizzato e seguito dai giudici di Calcutta; questi hanno dichiarato la violazione degli artt. 19(1)(a) e 21 della

⁷⁷ “The Respondent has submitted that continuous infiltration, foreign influence, violent extremism and issues of national integrity are prevalent in the Union Territory of Jammu and Kashmir, which are serious issues”, para. 21.

⁷⁸ Si veda sul punto l’analisi di Global Freedom of Expression, Columbia University, <https://globalfreedomofexpression.columbia.edu/cases/foundation-for-media-professionals-v-union-territory-of-jammu-and-kashmir-anr/>.

⁷⁹ Ciò, del resto, trova un interessante parallelismo nella già citata pronuncia nel c.d. caso *Aadhaar*, nella quale la posizione di maggioranza dei giudici della Corte suprema è stata positivamente accolta sotto determinati profili, in particolare nella parte in cui dettagliate linee guida quanto alla legittimità del sistema di riconoscimento e del trattamento dei dati biometrici vengono determinate; nonostante ciò, critiche sul test di proporzionalità, svolto rispetto a taluni interessanti aspetti, sono state comunque avanzate, come emerge anche nella nota *Dissenting opinion* del Justice Chandrachud.

Costituzione ad opera di un *Suspension Order* ritenuto arbitrario, “unreasonable” e adottato per il perseguimento di uno scopo illegittimo, non sussistendo una situazione di “public emergency”, come richiesto dalla *Section 144* C.p.p. e come interpretata dalla Corte suprema⁸⁰. In questa controversia, in particolare, il blocco della rete era stato avviato sulla base di un *intelligence report* che aveva evidenziato rischi di attività illecite nei giorni di un esame scolastico (*Madhyamil Pariksha*): applicando il test di proporzionalità già indicato in *Bhasin*, la Corte di Calcutta ha riconosciuto la possibilità, da parte dello Stato, di adottare mezzi meno invasivi e lesivi dei diritti fondamentali per raggiungere l’obiettivo di prevenire brogli e irregolarità durante le prove scolastiche⁸¹.

L’indirizzo giurisprudenziale e, dunque, il vaglio svolto dalle corti sulla base dei criteri individuati nelle sentenze della Corte suprema, tuttavia, non conosce, al momento, piena coerenza, forse proprio a causa di quelle debolezze, sopra rilevate, che lasciano spazio a diverse interpretazioni ed applicazioni. La sentenza della *High Court of Gauhati* (Stato di Assam) del 26 agosto 2022 (*Raju Prosad Sarma v. State of Assam*, WPC/5527/2022) è calzante esemplificazione di tale disomogeneità: questa pronuncia assume un tenore differente rispetto a quanto emerso nella sentenza *Biradar* appena analizzata. Similmente a quel caso, anche la *High Court of Gauhati* era stata infatti chiamata a pronunciarsi sul *Suspension Order* adottato dal *Principal Secretary to the Government of Assam* e volto a sospendere Internet (“including broadband, leased line, mobile data and 2G/3G/4G”) al fine di impedire ai candidati di un concorso pubblico di accedere alla rete durante l’esame. Nonostante l’istanza del *Secondary Education Board of Assam* richiedesse alle pubbliche autorità una valutazione quanto alla possibilità di disabilitare la connessione nel solo luogo del concorso e dunque con una estensione territoriale estremamente limitata, il blocco della rete previsto dall’*Order* in oggetto aveva investito invece l’intero territorio di Assam.

Secondo il ricorrente – che ha peraltro richiamato un importante report intitolato “Suspension of Telecom Services/Internet and its Impact” e pubblicato nel 2021 dal *Parliamentary Standing Committee on Communications and Information Technology* indiano –, la prevenzione di brogli durante esami o concorsi non rientrava tra le motivazioni di “public emergency” legittimanti il ricorso ad una limitazione generalizzata ed indifferenziata di Internet. L’*Advocate General*, al contrario, ha evidenziato come il blocco di Internet, operato in misura circoscritta ai soli telefoni e non anche alla rete fissa e ristretto temporalmente alla sola durata dell’esame, fosse misura necessaria data l’impossibilità di adottare mezzi alternativi per evitare pratiche vietate, già ampiamente verificatisi in passato. In questo caso, allora, il fine ultimo della misura è stato individuato nell’interesse ad “instill public faith and confidence and also ensure a free, fair and malpractice-free recruitment process” (p. 3). Ebbene, diversamente dalla pronuncia della Corte di Calcutta, nella sentenza in esame l’*Order* non è stato sospeso: una

⁸⁰ Il caso ha ad oggetto il *Suspension Order* adottato dal *Department of State of West Bengal*, nel marzo 2022.

⁸¹ Del tutto similmente viene risolto il caso, precedente a quello analizzato, *Dhirendra Singh Rajpurohit v. State of Rajasthan*, D.B. Civil Writ Petition No. 10304/2018, del 28 novembre 2018.

simile decisione avrebbe potuto – a parare dei giudici – incidere negativamente sugli ulteriori esami all’epoca imminenti e già programmati; inoltre, il *Counsel for the Government of Assam* aveva assicurato che nessun *Internet shutdowns* sarebbe stato posto in essere in occasione dei successi concorsi previsti nel mese di settembre⁸².

Non è stata presa, quindi, in questo caso, una posizione da parte dei giudici quanto alla legittimità dell’*Order* disposto per una finalità evidentemente differente dalla tutela della sicurezza venuta in gioco nei casi *Bhasin* e *Foundation for Media Professionals*. E così, dinnanzi a questa diversità di approcci e decisioni in merito all’utilizzo degli *Internet shutdowns* quale strumento di prevenzione di brogli durante esami o concorsi pubblici, un’interessante controversia è ad oggi pendente dinnanzi alla Corte suprema⁸³, a dimostrazione non solo di quanto la questione sulla legittimità del blocco di Internet sia aperta, ma anche di come i principi e criteri determinati dalla Corte suprema nel 2020 non possano certamente essere considerati risolutivi.

La ricca giurisprudenza indiana, tanto della Corte suprema quanto di corti statali, aiuta, in conclusione, a comprendere la complessità dell’intervento giurisdizionale in tale ambito: se la sentenza *Bhasin* rappresenta senza dubbio un significativo intervento a tutela dei diritti fondamentali esercitati nel contesto digitale, la *case-law* indiana dimostra altresì l’indeterminatezza del vaglio di proporzionalità promosso e, in particolare, la difficoltà di accertare la necessità del provvedimento adottato. La determinazione della reale e concreta presenza di una “public emergency” risulta un nodo centrale assai difficile da sciogliere al fine di assicurare la compatibilità di strumenti restrittivi della rete con le tutele costituzionali, così come resta da stabilire con chiarezza se ed in quale misura la targhettizzazione degli *shutdowns* a specifici territori e la loro breve durata siano in grado di legittimare il ricorso a tali strumenti anche per scopi legati alla sola garanzia della regolarità e affidabilità di procedure concorsuali pubbliche o esami scolastici.

4. Alcune – provvisorie – conclusioni: la sterilità del dibattito “*keep it on/shut it off*” e la necessità di una riflessione sulla proporzionalità degli strumenti di controllo di Internet

La disamina della giurisprudenza indiana in materia di *Internet shutdown* consente di muovere ora alcune considerazioni finali: queste, lungi dal porsi a chiusura di un dibattito ancora estremamente aperto, spingono a riflettere sul più ampio contesto della regolamentazione di Internet e sulle complesse

⁸² “Since the next examination is scheduled on 28.8.22, which is just two days away and (..) also keeping in mind that the disruption that may be caused in the holding of the examination fixed on 28.8 if an interim order is passed at this stage suspending the impugned notification, I am not inclined to pass any interim order”, para. 5.

⁸³ Si tratta del caso *Software Freedom Law Center, India v. State of Arunachal Pradesh et al.*, No. 314/2022, che ha conosciuto il 9 settembre 2022 una prima evoluzione: la Corte suprema ha emesso un *Order* diretto al *Ministry of Electronics and Information Technology* volto a richiedere a quest’ultimo di dimostrare l’esistenza di uno *Standard Protocol* per l’adozione di *Internet shutdowns* durante gli esami.

ed irrisolte sfide che il controllo della rete da parte di soggetti pubblici – o privati, se si pensa ai gestori delle piattaforme online – pone rispetto alla tutela dei diritti fondamentali e, in ultima analisi, alla garanzia di libertà fondanti il concetto stesso di democrazia.

Partendo da tale consapevolezza, la prima osservazione che si intende formulare attiene al riconoscimento del ruolo essenziale giocato dal formante giurisprudenziale nella determinazione – dai tratti ancora in parte sfumati – dei limiti di legittimità e dei contorni del vaglio di proporzionalità in materia di restrizioni della disponibilità di Internet. La Corte suprema indiana, infatti, si trova a riconoscere come l’articolato legame tra luoghi virtuali e luoghi reali, tra partecipazione offline e online, non possa che approdare “inevitabilmente a una richiesta di riconoscimento di diritti”⁸⁴. Ciò emerge con estrema evidenza nel caso *Bhasin*, in cui le esigenze securitarie e di mantenimento dell’ordine pubblico si scontrano con la delicata garanzia di una libertà di espressione nel mondo dei *bit* capace di produrre effetti anche fuori dallo schermo dei nostri cellulari o computer e di rivelarsi mezzo di partecipazione politica e di manifestazione – democraticamente “salutare” – di dissenso.

Le normative indiane che consentono l’adozione di *Internet shutdowns*, dunque, sono apparse in tutta la loro inadeguatezza e incapacità di regolare uno strumento dai così ampi risvolti. La vaghezza del dettato normativo e degli *Orders* adottati su tale base, nonché la mancata predisposizione di specifiche salvaguardie e limiti, sono foriere di possibili abusi da parte delle autorità pubbliche, così da richiedere un test di proporzionalità dettagliato, un attento vaglio da parte di organi appositamente istituiti ma anche la precisazione, di fondamentale rilievo, che gli *Internet shutdowns* “cannot be used as a tool to prevent the legitimate expression of opinion or grievance or exercise of any democratic rights”, comprensivi della “expression of divergent views, legitimate expression and disapproval”⁸⁵.

Se “Internet shutdown have a different intent than does Internet censorship, as their focus is not on a specific piece of content but rather on the act of communication itself”⁸⁶, allora il blocco della rete deve essere inteso quale mezzo estremo di *governance* di Internet e, più in generale, dei canali di comunicazione e informazione⁸⁷. Dinnanzi a mancanti o solo succinte disposizioni normative e provvedimenti attuativi – come rilevato

⁸⁴ Rodotà, *Il mondo nella rete*, cit., 10.

⁸⁵ Sentenza *Bhasin*, para. 118.

⁸⁶ Wagner, *Understanding Internet Shutdown*, cit., 3921. Non a caso questa forma estremamente evidente e ampia di blocco di Internet è stata ben presto evitata – anche per i pericolosi effetti sull’economia nazionale – da taluni ordinamenti che hanno prediletto l’adozione di altri strumenti di censura e controllo di Internet più sofisticati e mirati: “In contrast, the use of internet shutdowns and blackouts to curtail freedom of expression online – a rising trend in illiberal regimes around the world – is less prevalent in China. The government’s more advanced and sophisticated system of internet control and censorship reduces the need for such a blunt tool. Nonetheless, there continue to be sporadic media blackouts in China, including in relation to protests in Hong Kong”, H. Moynihan, C. Patel, *Restrictions on Online Freedom of Expression in China. The Domestic, Regional and International Implications of China’s Policies and Practices*, Chatham House Papers, 2021, 5.

⁸⁷ Pollicino definisce gli *Internet shutdown* come “major censorship measures”, in Pollicino, *Judicial Protection of Fundamental Rights on the Internet*, cit.

anche in diversi casi giurisprudenziali richiamati, tra cui quello deciso dalla Corte ECOWAS⁸⁸ –, il ruolo delle Corti diviene cruciale per fornire quelle che sono state definite vere e proprie linee guida sul ricorso agli *Internet shutdowns*⁸⁹, capaci di determinare anche tutele specifiche quali la necessità di enucleare precondizioni di fatto motivate e circostanziate, la predisposizione di un organo di riesame apposito o ancora la garanzia del mantenimento della connessione per la fruizione di servizi essenziali tra cui quelli ospedalieri o bancari o relativi all'accesso a siti governativi.

Nonostante il significativo apporto delle pronunce esaminate in questo contributo, il dibattito sugli *Internet shutdowns* e sulla loro legittimità non può tuttavia dirsi giunto ad un approdo conclusivo: come emerge dai diversi casi ancora pendenti dinnanzi alle Corti indiane e dal vasto numero di blocchi della rete ancora realizzati, il vaglio di proporzionalità è reso spesso arduo dinnanzi alla mancata trasparenza dei pubblici poteri⁹⁰ e all'assenza di informazioni precise sulle reali o potenziali minacce alla sicurezza – rappresentate anche dalla diffusione di disinformazione e *fake news* –. In questi casi, stabilire i confini tra legittime esigenze emergenziali, da un lato, e repressione di forme di opposizione online e offline rispetto al potere costituito o specifiche decisioni politiche, dall'altro, diviene estremamente difficile. Altri strumenti di tutela determinati in tale ambito, anche mediante il descritto intervento giurisprudenziale, sono poi oggetto di discussione: dalla composizione dei *Committees* e alla loro effettiva capacità di riesame delle decisioni governative sino alla fattibilità tecnica della preservazione della connessione per determinati soggetti o enti, al fine di assicurare servizi fondamentali.

La complessità di tali quesiti – che senza dubbio la giurisprudenza, più che il legislatore, ha contribuito a determinare e ha tentato, seppure in un processo ancora *in fieri*, di affrontare – permette di comprendere come l'ancora aperto dibattito sulla legittimità degli *Internet shutdowns* non possa essere semplicisticamente ridotto alla limitante opposizione tra *keep it on* e *shut it off*⁹¹. Una simile lettura impedisce di cogliere appieno le articolate problematiche giuridiche sottese e rende difficile ricondurre queste ultime entro la più vasta sfida, che tanto impegna anche corti, legislatori e giuristi

⁸⁸ Vedi *supra* nota 47.

⁸⁹ In questo senso T. Singh, A. Mishra, K. Bapat, *Why Don't They Just Stop Stopping the Internet? The Curious Case of India's Internet Shutdowns*, in *Verfassungsblog*, 26 ottobre 2021.

⁹⁰ “Although democratic states are usually inclined to provide a higher degree of transparency and accountability about the reasons behind Internet shutdowns, the general absence of government transparency makes the entire situation extremely opaque because information about Internet shutdowns comes primarily from the same officials who have been responsible for the shutdown. As a result, understanding the true reasons and consequences of Internet shutdowns and, in particular, how and to what extent human rights are affected, is not usually an easy task”, De Gregorio, Stremlau, *Internet Shutdowns and the Limits of Law*, cit., 4229. Ciò comporta, inevitabilmente, la difficoltà, per i cittadini colpiti da tali misure, di ricorrere all'intervento di apposite autorità di controllo o degli organi giurisdizionali, non avendo modo di conoscere e dunque di riflettere sulla legittimità e proporzionalità dello strumento impiegato rispetto alla finalità perseguita e all'interesse/diritto da tutelare.

⁹¹ In questo senso si legga De Gregorio, Stremlau, *Internet Shutdowns and the Limits of Law*, cit.

nelle democrazie occidentali, della regolamentazione del rapporto tra controllo – pubblico o privato – della rete e salvaguardia dei diritti fondamentali. Come affermato da Mounk, la rivoluzione tecnologica e l'avvento della rete hanno portato “nei paesi autoritari l'opposizione democratica (ad avere) molti più strumenti per rovesciare un dittatore al potere da lungo tempo. Tuttavia, per lo stesso motivo, anche i fomentatori dell'odio e i mercanti della menzogna possono minare le democrazie liberali molto più facilmente”⁹². Sebbene in contesti e con fondamenti differenti, dunque, le riflessioni sui limiti e le condizioni del controllo della rete e su un suo eventuale blocco e restrizione da parte delle pubbliche autorità, diventano sempre più urgenti, a qualsiasi latitudine.

Nel panorama giuridico nostrano, infatti, il ricorso a taluni strumenti di *governance* di Internet, pur certamente differenti per dimensioni e impatto rispetto al blocco generalizzato della rete, ha iniziato a porre quesiti che, sotto molteplici profili, si rivelano identici e convergenti con quelli già sopra individuati con riferimento agli *Internet shutdowns*. Pensiamo al *deplatforming* – ovvero l'inibizione all'accesso ad un servizio digitale, quale una piattaforma, nei confronti di un determinato utente –, o al divieto, disposto avverso taluni soggetti, di accedere ad Internet *tout court* o a determinati siti; o ancora consideriamo l'obbligo di chiusura di interi siti o profili *social*. Pur non discutendosi di misure paragonabili ad una restrizione generalizzata della disponibilità della rete, riguardante cioè la totalità degli utenti, non può non evidenziarsi come anche in tutti questi casi ad essere colpiti non sono i singoli contenuti presenti online bensì la vera e propria capacità di un dato soggetto di accedere *in toto* al servizio o al social. Diversamente dalla censura di un singolo post o di una immagine ma similmente a quanto avviene in occasione di *Internet shutdown*, l'effetto prodotto dai citati strumenti è quindi quello di limitare, nei confronti di determinati soggetti, la partecipazione alla “piazza digitale”, l'accesso alle informazioni reperibili online e la possibilità di esprimere la propria opinione in rete. E pure le questioni giuridiche sottese sono le medesime già viste per il blocco generalizzato di Internet: entro quali limiti simili restrizioni della rete sono da ritenersi proporzionate al fine perseguito, spesso legato alla garanzia della sicurezza? Come rilevato, “la privazione della possibilità di accesso ai social network determina inevitabilmente, nell'odierna società dell'informazione, quantomeno un depotenziamento (ma anche un vero e proprio impedimento, a seconda dei casi) nell'esercizio della libertà di espressione”⁹³: quali possono essere, allora, gli interessi confliggenti tali da giustificare la necessità e proporzionalità della misura di blocco dell'impiego di una app o social network o sito nei confronti di un utente?

Ecco allora che, sulla base di tali interrogativi, del tutto simili a quelli posti dalla Corte suprema indiana nei casi sopra analizzati, sono sorte anche alle nostre latitudini talune controversie di rilievo: pensiamo all'intervento, nel contesto europeo, della Corte europea dei diritti dell'uomo (Corte EDU) che si è pronunciata, in diversi casi, sulla conformità rispetto all'art. 10 della

⁹² Y. Mounk, *Popolo v. democrazia. Dalla cittadinanza alla dittatura elettorale*, Milano, 2018, 333.

⁹³ M. Bassini, *Libertà di espressione e social network, tra nuovi “spazi pubblici” e “poteri privati”*. *Spunti di comparazione*, in *MediaLaws*, 2, 2021, 76.

Convenzione EDU di misure determinanti il blocco di siti, social o altri servizi online e stabilite da pubblici poteri, ai danni di singoli cittadini. È questo il caso *OOO Flarus et al. v. Russia* (Applications 12468/15, 23489/15 e 19074/16) deciso con sentenza del 16 novembre 2020: i tre ricorrenti, cittadini russi gestori di pagine web, blog o riviste online, denunciavano la violazione della libertà di espressione ad opera del *Prosecutor General* che aveva ordinato agli ISPs il blocco dei loro account, ritenuti portatori di “calls for extremist activities”⁹⁴. Anziché provvedere ad un ordine di rimozione dello specifico contenuto ritenuto illegittimo o pericoloso, le autorità russe avevano quindi adottato un blocco ben più invasivo e “generalizzato”, stabilendo la chiusura dei siti *in toto*. Mancando di motivare tale provvedimento, il *Prosecutor* aveva oltretutto impedito ai ricorrenti di “taking down or modifying the specific content and formulating a legal objection” (para. 32). Alla luce di queste considerazioni e per quanto maggiormente interessa in questa sede, i giudici di Strasburgo hanno dunque affermato come “wholesale blocking of access to a website is an extreme measure which has been compared to banning a newspaper or television station. Such a measure (..) renders inaccessible large amount of content which has not been identified as illegal” (para. 37). Di conseguenza, “any indiscriminate blocking measure which interferes with lawful content or websites as a collateral effect of a measure aimed at illegal content or websites amounts to arbitrary interference with the rights of the owners of such websites. (..) The applicants’ claim that the true objective of the Russian authorities was to suppress access to the opposition media outlets gives rise to serious concern”⁹⁵ (para. 38). In queste parole non possono che rivenirsi forti somiglianze con quanto affermato dalla Corte suprema indiana nel caso *Bhasin*; somiglianze, queste, che si accompagnano peraltro alle valutazioni proposte dalla Corte EDU quanto alla mancata previsione, nella normativa russa di riferimento, sia di un preventivo vaglio di necessità e proporzionalità delle misure “censorie” generalizzate, sia di un obbligo di motivazione dettagliata delle misure adottate, tale da consentire agli interessati di adire organi di controllo o giurisdizionali (para. 40). Anche in questa pronuncia, che pure attiene ad un caso molto più limitato – quanto ad estensione – rispetto agli *Internet shutdowns*, emergono nondimeno quelle condizioni e requisiti che la Corte indiana ha elencato con riferimento al blocco generalizzato della rete.

⁹⁴ Il *Russian Information Act*, emendato nel 2013, “empower the Prosecutor General to identify and submit a blocking request directly to the telecoms regulator against websites containing calls for mass disorder, extremist activities, or participation in unauthorised mass gatherings”, senza il previo intervento di autorità giurisdizionali (para. 5). Nel caso in esame, i siti dei ricorrenti erano stati oscurati e bloccati in quanto contenenti incitazioni alla protesta avverso il governo russo, soprattutto a seguito della repressione delle manifestazioni di piazza Bolotnaya e di quelle contro l’occupazione russa in Crimea. I ricorrenti, già dinnanzi alle corti russe, avevano ritenuto che “the indiscriminate blocking of access to the entire websites (..) prevented the applicants from restoring access to their websites by removing the offending material”, para. 8.

⁹⁵ Inoltre “The UN Human Rights Committee and Special Rapporteurs have emphasized that targeting online media or websites with blocking measures because they are critical of the government or political system can never be considered a necessary restriction on freedom of expression”, para. 38.

Del resto, i giudici di Strasburgo si sono pronunciati in maniera simile anche in decisioni ben più risalenti nel tempo, tra cui il caso *Ahmet Yildirim v. Turkey* (Application n. 3111/10, decisa con sentenza del 18 dicembre 2012) avente ad oggetto il blocco all'accesso a qualsiasi Google Sites⁹⁶. In particolare, la *Denizli Criminal Court*, su indicazione del *Telecommunications and Information Technology Directorate*, anziché bloccare un singolo sito gestito da un cittadino turco colpevole di aver insultato la memoria di Atatürk, aveva operato una restrizione all'accesso “to all content on the Internet domain concerned”, così che “domain such as (...) Google Groups, myspace.com and youtube.com have been subject of blocking orders over long periods of time because of the websites which they host” (para. 17). Questa misura aveva finito col rappresentare non “a wholesale ban but rather a restriction on Internet access. (...) Nevertheless, the fact that the effects of the restriction in issue were limited does not diminish its significance, especially since the Internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information, providing as it does essential tools for participation in activities and discussion concerning political issues and issues of general interest” (para. 54). Tali affermazioni, estremamente significative, richiamano quindi l'irrilevanza dell'ampiezza delle restrizioni ai fini della verifica di legittimità e proporzionalità: anche nel caso di un blocco della disponibilità di singole tipologie di siti, viene così ribadita la necessità di prescrizioni normative precise e chiare; qualità, queste, non rilevate nella legge turca (Legge n. 5651, Sezione 8), che è stata ritenuta infine “in direct conflict with the wording under art. 10 [Convenzione EDU] and led to arbitrary effects”⁹⁷.

La distinzione tra blocco dell'accesso ad interi siti, a un gruppo di siti web o ancora alla rete nella sua totalità diviene così irrilevante e sfumata dinnanzi a questioni giuridiche ed effetti restrittivi di libertà e diritti che caratterizzano in modo del tutto simile tanto le controversie qui esaminate quanto quelle analizzate più sopra con riferimento agli *Internet shutdowns*, pur ovviamente coinvolgendo un numero di soggetti significativamente diverso – di gran lunga superiore nei casi indiani –. Tutti i casi sin qui esaminati impongono il medesimo test di proporzionalità e, qualora non regolamentati da norme precise, rischiano similmente di realizzarsi in abusi di potere da parte delle autorità pubbliche. Le misure di cui si è occupata la Corte EDU hanno infatti colpito, in un caso, utenti che non hanno realizzato nessuna violazione della legge, e nell'altro, contenuti che non potevano considerarsi illeciti. La possibilità di ricorrere ad una simile generalizzazione deve essere, allora, soggetta a stringenti controlli e valutazioni di proporzionalità e necessità, come affermato tanto nelle sentenze qui brevemente riportate dei giudici di Strasburgo, quanto nella giurisprudenza indiana più ampiamente presentata.

Ma il dibattito giurisdizionale in materia di restrizioni di Internet non interessa certamente solo il contesto europeo: anche oltreoceano, negli Stati

⁹⁶ D. Mburu Nyokabi et al., *The Right to Development and Internet Shutdowns: Assessing the Role of Information and Communications Technology in Democratic Development in Africa*, in *Global Campus Human Rights J*, 3, 2019, 147-172.

⁹⁷ *Ahmet Yildirim v. Turkey*, in *Global Freedom of Expression*, Columbia University, <https://globalfreedomofexpression.columbia.edu/cases/ahmed-yildirim-v-turkey/>.

Uniti d'America, la Corte suprema si è occupata della legittimità di una legge del North Carolina che aveva introdotto, nei confronti di tutti i condannati di reati sessuali, un divieto generalizzato di accesso a qualsiasi “commercial social networking Website (..) where the sex offender knows that the site permits minor children to become members or to create or maintain personal webpages”⁹⁸. In estrema sintesi, Justice Kennedy, che ha redatto la pronuncia, ha descritto tale disposizione come “a prohibition unprecedented in the scope of First Amendment speech it burdens”⁹⁹. Pur riconoscendo l’interesse legittimo perseguito dalla legge statale così come la tendenza dei criminali a sfruttare tali innovazioni tecnologiche, l’interdizione indiscriminata dell’accesso alla rete viene definita come “a complete bar to the exercise of First Amendment rights on websites integral to the fabric of our modern society and culture”¹⁰⁰. La misura è parsa dunque realizzare una restrizione sproporzionata della libertà di espressione, anche considerando la possibilità di adottare misure meno invasive rispetto ad un utilizzo dei social media considerati peraltro “the most powerful mechanisms available to a private citizen to make his or her voice heard”¹⁰¹. Al netto delle pur interessanti discussioni sull’utilizzo del parallelismo tra Internet e la piazza pubblica (*public forum*) e delle sue ripercussioni sull’interpretazione del Primo Emendamento¹⁰², la pronuncia richiamata rivela ancora una volta l’importanza di un vaglio attento di proporzionalità¹⁰³, della presenza di un interesse legittimo e di una valutazione circa la sussistenza di possibili misure alternative determinanti una minore limitazione dei diritti, affermando così la significativa invasività di più ampi strumenti di divieto e impedimento dell’accesso a social network o siti¹⁰⁴.

Certo merita segnalare come operazioni di esclusione dalla rete o da determinati servizi web siano poste in essere non solo da autorità pubbliche,

⁹⁸ North Carolina Gen. Stat. 14-202.5(a) (2015).

⁹⁹ *Packingham*, 137 S. Ct., 1737.

¹⁰⁰ *Ibidem*, 1738.

¹⁰¹ *Id.*

¹⁰² Bassini, *Libertà di espressione e social network*, cit. ma anche O. Soldatov, *The Transformative Effects of Social Media: Preliminary Lessons from the Supreme Court Argument in Packingham v. North Carolina*, in questa Rivista, 2, 2017, 417-420; E. Celeste, *Digital Punishment: Social Media Exclusion and the Constitutionalising Role of National Courts*, in *International Review of Law, Computers & Technology*, 2, 2021, 162-184;

¹⁰³ In questo caso, tale vaglio viene svolto tra libertà di espressione e interesse dello stato di proteggere i minori.

¹⁰⁴ “Recent US case law has imposed a series of obligations where phenomena of social media exclusion involved accounts of special categories of users, in particular politicians. The importance of introducing constitutional safeguards in these circumstances is apparent in light of the implications for other civil and political rights. Excluding individuals from accessing and interacting with content published by politicians on social media significantly restricts the enhanced possibility that online platforms offer citizens for engaging in the democratic life of their country”, E. Celeste, *Digital Punishment*, cit., 170. In questo contesto possono essere fatte rientrare pure le restrizioni e il blocco di diversi siti ad opera del governo spagnolo in occasione del contestato referendum in Catalogna (come documentato dalla ONG Edri, *No Justification for Internet Censorship during Catalan Referendum*, 4 ottobre 2017, <https://edri.org/our-work/no-justification-for-internet-censorship-during-catalan-referendum/>).

sulla base di disposizioni normative, bensì anche da soggetti privati, con particolare riferimento ai gestori di grandi piattaforme e social network: casi arcinoti possono essere identificati nella *deplatforming* dell'ex Presidente degli USA, Donald Trump, da Twitter¹⁰⁵ o ancora nella chiusura da parte di Facebook di profili appartenenti a forze politiche estremamente controverse nel contesto italiano, quali Forza Nuova e CasaPound¹⁰⁶. Qui la particolarità evidente e di rilievo è da rinvenirsi nell'intervento di soggetti privati e non di pubbliche autorità, come visto invece nei casi precedenti. Il potere di controllo assunto da gestori di piattaforme e social media apre necessariamente una serie aggiuntiva di interrogativi, profondi e complessi, sulla tutela orizzontale della libertà di espressione nel mondo digitale¹⁰⁷. Se

¹⁰⁵ Sul tema, *ex multis*, A. Fricano, *Prove tecniche di resilienza costituzionale: l'assalto a Capitol Hill e la censura mediatica di Donald Trump*, in *La Rivista del Gruppo di Pisa*, Quaderno n. 3, 2021, 733-744.

¹⁰⁶ Tra i tanti che hanno commentato le controverse pronunce del Tribunale di Roma, si rinvia a P. Falletta, *Controlli e responsabilità dei social network sui discorsi d'odio online*, cit.; R. Bin, *CasaPound vs Facebook: un'ordinanza che farà discutere*, in *lacostituzione.info*, 15 dicembre 2019; P. Zicchittu, *La libertà di espressione dei partiti politici nello spazio pubblico digitale: alcuni spunti di attualità*, 2, 2020, 81-94; C. Caruso, *La libertà di espressione presa sul serio. CasaPound c. Facebook, Atto I*, in *SidiBlog*, 20 gennaio 2020; ma anche, rispetto a simili decisioni, S. Thobani, *L'esclusione da Facebook tra lesione della libertà di espressione e diniego di accesso al mercato*, in *Persona e mercato*, 2, 2021, 427-429.

¹⁰⁷ In tali contesti, "Lo spazio pubblico si dilata considerevolmente fino a inglobare quegli attori privati che, in virtù di una loro posizione di fatto, incidono sull'esercizio dei diritti fondamentali. In maniera del tutto simmetrica, le garanzie costituzionali si espandono, democratizzando la regolazione privatistica della rete", Zicchittu, *La libertà di espressione dei partiti politici*, cit., 86. Il dibattito sul ruolo e la responsabilizzazione dei privati gestori di siti o piattaforme è ancora estremamente acceso ed articolato: "Proprio la 'privatizzazione della censura' è divenuta centrale nella riflessione sul ruolo della rete quale 'piazza virtuale', che dovrebbe garantire il massimo pluralismo, realizzando quello che Alain Touraine ha indicato come 'il ruolo positivo della tecnica': 'protegge(re) contro tutti i totalitarismi culturali'. La realtà dei fatti, invece, evidenzia una rete (o meglio delle *Internet Platforms*) che, seppur per fronteggiare reali abusi, selezionano ogni giorno i contenuti dell'agorà e gli stessi accessi ad essa", C. Bologna, *Libertà di espressione e riservatezza "nella rete"? Alcune osservazioni sul mercato delle idee nell'agorà digitale*, in *La Rivista del Gruppo di Pisa*, Quaderno n. 3, cit., 33; nella stessa rivista L. Rinaldi, *Le piattaforme tra diritto pubblico e diritto privato: libertà d'espressione, discorso politico e social network in alcuni casi recenti tra Italia e Stati Uniti*, 211-228; T. Wischmeyer, *Making Social Media an Instrument of Democracy*, in *European L J*, 2, 2019, 169-181; sul controverso e ancora ampiamente dibattuto tema della regolamentazione e lotta alla disinformazione, *fake news* e discorsi d'odio online, si rinvia, senza pretesa di completezza, a F. Pizzetti, *Fake news e allarme sociale: responsabilità, non censura*, in *MediaLaws*, 1, 2017, 49-59; C.R. Sunstein, *#Republic. La democrazia nell'epoca dei social media*, Bologna, 2017; M. Cuniberti, *Il contrasto alla disinformazione in rete tra logiche del mercato e (vecchie e nuove) velleità di controllo* e M. Bassini, G.E. Vigevani, *Prima appunti su fake news e dintorni*, tutti in *MediaLaws*, 1, 2017; G. Ziccardi, *La soluzione c'è: si chiama censura*, in *ilMulino*, 2, 2017, 226-234; T.E. Frosini, *No news is fake news*, in *DPCE*, 4, 2017, V-X; G. Pitruzzella, O. Pollicino, S. Quintarelli (a cura di), *Parole e potere. Libertà d'espressione, hate speech e fake news*, Milano, 2017; M. Cavino, *Il triceratopo di Spielberg. Fake news, diritto e politica* e G. Suffia, G. Ziccardi, *Fake news, guerra dell'informazione ed equilibri democratici*, tutti in *Federalismi.it*, 11, 2020; G.M. Ruotolo, *A little hate, worldwide! Di libertà d'opinione e discorsi politici d'odio on-line nel diritto internazionale ed europeo*, in *Diritti umani e diritto internazionale*, 2, 2020, 549-582. Più ampiamente, si

pure questo elemento determinante impone di distinguere tali casi – che quindi non si intende qui approfondire – da quelli previamente presentati, nondimeno un tratto comune è da individuarsi, ancora una volta, nel fatto che simili operazioni non consistono nella cancellazione o blocco di singoli contenuti (post) bensì nel divieto ed esclusione integrale di accesso – e dunque di espressione – all'interno dei social media o delle piattaforme.

Insomma, tutti gli esempi e gli interventi giurisprudenziali qui indicati con riferimento alla Corte EDU e alla Corte suprema americana, hanno interessato aree geografiche – e spesso anche forme di stato – diverse da quelle nelle quali il ricorso agli *Internet shutdowns* è maggiormente sviluppato. Nonostante ciò, tali decisioni consentono di comprendere come gli interrogativi sul rapporto tra tutela delle libertà in rete, da un lato, e potere pubblico – e privato – di esclusione da Internet, dall'altro, siano estremamente diffusi e si presentino in riferimento a diverse casistiche, con diverse dimensioni ed ampiezza di effetti. Pur concretizzandosi in restrizioni dalla portata più o meno ampia, la censura *della* rete o di parti di essa – interi social o siti – ha aperto un dibattito vasto. All'interno di esso, l'intervento delle Corti nei casi esaminati in questo lavoro pare accumulato dal riconoscimento dei pericoli per la libertà di espressione e di riunione nonché, in ultima istanza, per la garanzia di quella manifestazione – pacifica – del dissenso che è così cruciale per una società realmente democratica e che non può essere in ogni occasione compressa dinnanzi ad esigenze securitarie.

Ecco allora che, in un simile ampio panorama, lo studio della giurisprudenza e del dibattito politico, sociale e dottrinario in materia di *Internet shutdown* diviene di estrema utilità ed interesse anche per leggere quei fenomeni, sempre più frequenti alle nostre latitudini, di *deplatforming* o di limitazione – più o meno mirata – della disponibilità e libertà di accesso a porzioni della rete¹⁰⁸.

Promuovere un serio studio delle tutele costituzionali, dei limiti e del vaglio di proporzionalità da garantire dinnanzi a tutti questi strumenti si rivela allora uno sforzo imprescindibile per evitare le derive di un totalitarismo digitale¹⁰⁹, esercitato non solo mediante un vaglio dei contenuti (dunque un controllo *nella* rete) bensì attraverso la restrizione e il controllo *della* rete stessa – totale o parziale –.

leggano anche le riflessioni di P. Costanzo, *Internet*, in *Digesto delle discipline pubblicistiche*, Torino, 2000, 355 ss.

¹⁰⁸ Gli strumenti impiegati dalle pubbliche autorità per limitare l'accesso ad Internet sono del resto in continua evoluzione: si pensi, ad esempio, agli scenari di c.d. *splinternet*, cioè di frammentazione della rete, promossi non solo in Cina con il *Great Firewall*, ma anche in Russia, dove ha avuto luogo il tentativo di realizzazione di una *RuNet*, una rete nazionale indipendente dal *world wide web*, che sta trovando graduale attuazione tanto mediante l'attuazione della legge sulla sovranità di Internet del novembre 2019, quanto attraverso le diverse misure restrittive l'accesso a determinati social network disposte a seguito dell'invasione armata dell'Ucraina. Sul punto, A. Polyakova, C. Meserole, *Exporting Digital Authoritarianism: The Russian and Chinese Models*, cit.; S. Feldstein, *Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?*, Carnegie Working Paper, marzo 2022.

¹⁰⁹ R. Kant et al., *Internet Under Threat? The Politics of Online Censorship in the Pacific Islands*, in *Pacific Journalism Review*, 24, 2018, 64-83; L. Diamond, *The Road to Digital Unfreedom: The Threat of Postmodern Totalitarianism*, in *Journal of Democracy*, 1, 2019, 20-24.

Il rischio – già invernato in alcuni ordinamenti, come si è visto in questo contributo e come evidenziato dalle pronunce giurisprudenziali citate – è che tali forme di controllo di Internet finiscano col favorire pratiche di recessione democratica¹¹⁰, così da condurre ad uno scivolamento insidioso da *Internet shutdown* a *democracy shutdown*. Risulta quindi “più che mai necessaria una riflessione olistica sull’universo comunicativo, sulla sua configurazione e prevedibile sviluppo, sul suo governo che consideri insieme libertà e diritti, poteri e limiti, rimedi e procedure”¹¹¹. È su tali considerazioni e sulla capacità di legislatori e giudici di tramutarle in soluzioni normative e giurisprudenziali efficaci, che dovrà concentrarsi il dibattito giuridico, facendo perno sulla consapevolezza che è anche nel campo della tutela dei diritti nel mondo digitale che si gioca la delicata partita della regolamentazione del rapporto tra potere e libertà in una società democratica.

Giulia Formici
Dipartimento di Diritto Pubblico Italiano e Sovranazionale
Università degli Studi di Milano
giulia.formici@unimi.it

¹¹⁰ Come osservato dal UN Special Rapporteur on Rights to Freedom of Peaceful Assembly, Clement Voule (news.un.org/en/story/2021/07/1095142, 1 luglio 2021), “Shutdowns have been observed in long-established democracies and more recent democracies alike, in line with broader trends of democratic recession across the world”. Sul più vasto tema della recessione democratica, poi, si legga, *ex multis*, T.G. Daly, *The Democratic Recession and the “New” Public Law: Toward Systematic Analysis*, in *Int J Const L Blog*, 22 aprile 2016; A. Di Gregorio, *I fenomeni di degenerazione delle democrazie contemporanee: qualche spunto di riflessione sullo sfondo delle contrapposizioni dottrinali*, in *Nuovi Autoritarismi e Democrazie: Diritto, Istituzioni, Società*, 2, 2019, 1-29; L. Mezzetti, *Corrosione e declino della democrazia*, in *DPCE*, N. Speciale, 2019, 421-445; T. Groppi, *Dal costituzionalismo globale ai nuovi autoritarismi. Sfide per il diritto comparato*, in *Rivista AIC*, 4, 2022, 65-79.

¹¹¹ V. Zeno-Zencovich, *La disciplina della comunicazione in base al suo contenuto. Una proposta di inquadramento sistematico*, in *Il diritto dell’informazione e dell’informatica*, 3, 2020, 551.