

Piattaforme digitali e comunicazione politica tra regole ordinarie e disciplina elettorale: sviluppi della libertà di espressione in India

di Davide Ragone

Abstract: The essay analyzes the contemporary regulation of freedom of expression in India with particular attention to the digital sphere and electoral communication. While the constitutional framework of Article 19(1) provides the background, the focus is on recent regulatory developments. Central to the analysis are the Information Technology Act and, above all, the IT Rules 2021, which impose strict obligations on intermediaries, digital media and OTT platforms, creating new mechanisms of governmental oversight. A central role is played by the Indian Election Commission, a key regulator entrusted with supervising online campaigning and ensuring electoral fairness. The essay explores the normative responses to emerging phenomena such as deepfakes, the activity of influencers in political campaigns, paid advertising on digital platforms and the controversial practice of “paid news.” A dedicated section addresses the pervasive use of messaging services – particularly WhatsApp – as primary tools of political mobilization and disinformation. Considerable attention is paid as well to judicial review, pending cases before the Supreme Court and the role of jurisprudence in shaping the limits of state intervention. Finally, the analysis covers the use of official social media accounts by public office holders, who are simultaneously political figures. Overall, the paper identifies patterns of both convergence and divergence between State control and free expression, between innovation and accountability and between transparency and manipulation of the digital public sphere.

Keywords: India; Freedom of expression; Social regulation; Political communication; Digital sovereignty

1527

1. Un primo inquadramento: India e UE a confronto

Il presente saggio affronta il tema della regolazione della comunicazione politica e della libertà di espressione nell’India contemporanea ¹,

¹ L’eccezionalità dell’ordinamento indiano è da tempo al centro dell’interesse della comunità scientifica. Si vedano, *ex aliis*, D. Amirante, *The Indian Constitution in defence of democracy and multiculturalism: Pragmatism, flexibility and hybridisation*, in *Rivista di Diritti Comparati*, spec. VI (2024); D.D. Basu, *Introduction to the Constitution of India*, Gurgaon, 26th ed., 2022; C. Jaffrelot, *Modi’s India: Hindu Nationalism and the Rise of Ethnic Democracy*, Princeton, 2021; M. Khosla, *India’s Founding Moment: The Constitution of a Most Surprising Democracy*, Cambridge (Mass.), 2020; P. Viola, *Costituzionalismo autoctono. Pluralismo culturale e trapianti giuridici nel subcontinente indiano*, Bologna, 2020; D. Amirante, *La Costituzione più lunga del mondo. Elementi di base e struttura organizzativa*, in Id. (cur.), *I sistemi costituzionali dell’Asia meridionale*, Milano, 2019; D. Amirante, *La democrazia dei superlativi. Il sistema costituzionale*

concentrandosi sugli aspetti relativi alle piattaforme digitali e ai *social media*. La scelta di concentrare l'analisi sul contesto indiano risponde all'esigenza di indagare un ordinamento che, pur avendo una solida base costituzionale in materia di diritti fondamentali, si colloca oggi tra i sistemi più pervasivi al mondo per quanto riguarda l'intervento statale nello spazio digitale. Per comprendere pienamente la portata delle dinamiche in atto nell'ordinamento indiano, l'analisi prende avvio da un breve confronto con il modello regolativo dell'Unione europea (UE), che rappresenta oggi uno dei sistemi più articolati e strutturati in materia di piattaforme digitali e comunicazione politica *online*. Questa prima comparazione consente di far emergere fin dall'inizio le differenze strutturali e le tensioni profonde, che caratterizzano il bilanciamento tra libertà di espressione, poteri pubblici ed effettività dell'apparato regolatorio.

In Europa, e in particolare in Italia, la disciplina della comunicazione politica sui *social media* si inserisce, infatti, in un quadro giuridico relativamente chiaro e centralizzato, che può essere assunto come riferimento euristico. Da un lato, operano autorità indipendenti che presidiano il rispetto delle regole, come l'Autorità Garante delle Comunicazioni in Italia (AGCOM) o i garanti per la protezione dei dati personali nei diversi Stati membri; dall'altro, la cornice normativa europea offre strumenti sofisticati di regolazione, come il *General Data Protection Regulation* (GDPR)² e, più recentemente, il *Digital Services Act* (DSA)³ e la

dell'India contemporanea, Napoli, 2019; P. Viola, *Stato, Sistema di governo, Diritti e doveri nello sviluppo costituzionale indiano*, in D. Amirante (cur.), *I sistemi costituzionali dell'Asia meridionale*, cit.; R. Sharma, *No Country for Strongmen: How India's Democracy Constrains Modi*, in 98 *Foreign Affairs* 2 (2019); G. Austin, *The Indian Constitution: Cornerstone of a Nation*, Oxford-New Delhi, 2018 (1st ed. 1966); A.K. Thiruvengadam, *The Constitution of India: a contextual analysis*, Oxford, 2017; M. Vaishnav, *When Crime Pays: Money and Muscle in Indian Politics*, New Haven, 2017; S. Choudhry, M. Khosla, P.B. Mehta (eds), *The Oxford Handbook of the Indian Constitution*, Oxford, 2016; D. Amirante, *Lo stato multiculturale. Contributo alla teoria dello Stato dalla prospettiva dell'Unione indiana*, Bologna, 2014; D. Amirante, C. Decaro, E. Pföstel (cur.), *La Costituzione dell'Unione indiana. Profili introduttivi*, Torino, 2013; D. Francavilla, *Il diritto nell'India contemporanea. Sistemi tradizionali, modelli occidentali e globalizzazione*, Torino, 2011; N.G. Jayal, P.B. Mehta (eds), *The Oxford Companion to Politics in India*, Oxford, 2010; H.M. Seervai, *Constitutional Law of India*, 3 vol., New Delhi, 4th ed., 2005; S. Corbridge, J. Harris, *Reinventing India. Liberalization, Hindu Nationalism and Popular Democracy*, Cambridge, 2000; G. Austin, *Working a Democratic Constitution: A History of the Indian Experience*, Oxford-New Delhi, 1999.

² Reg. UE n. 2016/679 del P.E. e del Cons. del 27-4-2016. Il regolamento è entrato in vigore il 24 maggio 2016 ed è divenuto pienamente applicabile a partire dal 25 maggio 2018. Il GDPR ha introdotto un quadro uniforme e direttamente applicabile in tutti gli Stati membri in materia di protezione dei dati personali, rafforzando i diritti degli interessati e imponendo obblighi stringenti ai titolari del trattamento, anche con riferimento all'uso dei dati per finalità politiche e di profilazione (art. 22 GDPR). Sebbene non sia una regolazione settoriale, il GDPR stabilisce all'art. 9 il divieto di trattamento per una serie di categorie particolari di dati personali (par. 1), tra cui include le opinioni politiche, e individua una serie di casi in cui si deroga a questa applicazione (par. 2), tra cui l'esplicita prestazione del consenso. Si segnala anche, alla luce dell'analisi che seguirà del caso indiano, il *Considerando n. 56*, secondo il quale «se, nel corso di attività elettorali, il funzionamento del sistema democratico presuppone, in uno Stato membro, che i partiti politici raccolgano dati

Regulation on the transparency and targeting of political advertising (TTPA)⁴. Questo impianto si traduce in obblighi stringenti di trasparenza per gli annunci politici, in regole puntuali contro la disinformazione e in sistemi di tutela dei dati personali: almeno in linea teorica, l'assetto europeo affida poi l'*enforcement* a meccanismi non direttamente dipendenti dal potere esecutivo, privilegiando l'intervento di organismi autonomi. Le difficoltà maggiori non derivano, dunque, dalla mancanza di regole, quanto piuttosto dalla necessità di rendere effettivamente uniforme la loro applicazione e maggiormente omogenee le sanzioni nei diversi Stati membri.

La situazione indiana si presenta radicalmente diversa: pur esistendo un fondamento costituzionale in materia di libertà di espressione, il legislatore e l'esecutivo dispongono di ampi margini per imporre restrizioni in un contesto caratterizzato dall'assenza di un'autorità indipendente paragonabile a quelle europee. In tale quadro, il cuore della disciplina è rappresentato dall'*Information Technology Act* (IT Act) e dalle IT Rules del 2021, che conferiscono al governo un ruolo diretto nella supervisione dei contenuti *online*. Queste regole attribuiscono, infatti, all'esecutivo la possibilità di ordinare la rimozione di contenuti, imporre obblighi procedurali stringenti alle piattaforme digitali e richiedere forme di tracciabilità degli utenti. Questo assetto ha alimentato fenomeni di

personali sulle opinioni politiche delle persone, può esserne consentito il trattamento di tali dati per motivi di interesse pubblico, purché siano predisposte garanzie adeguate».

³ *Reg. UE n. 2022/2065 del P.E. e del Cons. del 19-10-2022*. Il regolamento è entrato in vigore il 16 novembre 2022 ed è divenuto generalmente applicabile a partire dal 17 febbraio 2024, sebbene lo fosse già dal 25 agosto 2023 per le *Very Large Online Platforms* (VLOPs) e per i *Very Large Online Search Engines* (VLOSEs), cioè quelle piattaforme *online* e quei motori di ricerca *online*, che hanno un numero medio mensile di destinatari attivi del servizio nell'UE pari o superiore a 45 milioni (circa il 10% della popolazione UE), come, ad esempio, Facebook, Instagram o YouTube. Avendo questi strumenti un impatto enorme, sono stati, pertanto, soggetti a una disciplina più rapida e più intensa, con l'introduzione di obblighi specifici tra i quali, ad esempio, la valutazione da parte dei fornitori del rischio legato a «eventuali effetti negativi, attuali o prevedibili, sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica» (art. 34, par. 1, lett. c), formula che richiama quella ancora più estesa del *Considerando n. 82* («effetti negativi reali o prevedibili sui processi democratici, sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica»). Prima dell'approvazione del *Reg. UE n. 2024/900 del P.E. e del Cons. del 13-3-2024*, si segnala che, in generale, già l'art. 26 DSA poneva una serie di obblighi di trasparenza alla pubblicità *online*.

⁴ *Reg. UE n. 2024/900 del P.E. e del Cons. del 13-3-2024*. Il regolamento è entrato in vigore il 9 aprile 2024 ed è divenuto pienamente applicabile a partire dal 10 ottobre 2025. La disciplina introduce un quadro armonizzato di trasparenza per la pubblicità politica *online*, imponendo obblighi di etichettatura degli annunci, l'indicazione del soggetto finanziatore e delle risorse economiche impiegate, nonché specifiche limitazioni all'uso dei dati personali per finalità di *targeting* politico e obblighi informativi sulle modalità di diffusione e amplificazione dei messaggi politici. L'intervento normativo è finalizzato a contrastare la manipolazione elettorale, la disinformazione e le interferenze nei processi elettorali, rafforzando l'integrità del dibattito pubblico e la trasparenza delle campagne politiche digitali.

censura quasi “istituzionalizzata”, con l’India che negli ultimi anni ha registrato il primato mondiale per numero di *Internet shutdowns*⁵.

Anche sul piano della comunicazione politica emergono profonde differenze rispetto al modello europeo: laddove l’UE si è orientata verso un regime di trasparenza progressivamente più severo (si pensi, ad esempio, alla previsione delle etichette obbligatorie per gli annunci politici da parte di Meta)⁶, in India vige un sistema di pre-certificazione delle inserzioni elettorali, meccanismo rigoroso nelle intenzioni, ma spesso aggirato attraverso la pratica delle *paid news*, cioè la pubblicazione di articoli e servizi giornalistici a pagamento camuffati da notizie imparziali. Non meno rilevante è il fatto che le stesse piattaforme abbiano approvato inserzioni contenenti messaggi manipolatori o violenti, a testimonianza di un controllo più debole e frammentario rispetto a quello europeo.

Un ulteriore punto di divergenza riguarda l’uso dei servizi di messaggistica: anche in Europa strumenti come WhatsApp o Telegram sono largamente diffusi in ambito politico, ma non hanno raggiunto la rilevanza sistemica, che hanno conquistato in India. Nel contesto indiano, infatti, WhatsApp rappresenta il cuore della mobilitazione elettorale e costituisce un canale primario di propaganda e di disinformazione, sfuggendo a un controllo efficace e restando difficilmente monitorabile dalle autorità. Infine, va considerata la questione dell’uso dei *social media* da parte dei titolari di cariche pubbliche: l’Europa è sensibile alla distinzione tra comunicazione istituzionale e propaganda politica, tentando

⁵ L’India ha detenuto a lungo il primato mondiale per numero di ordini di *Internet shutdowns*, con almeno 116 casi documentati nel 2023 e un ruolo dominante anche negli anni precedenti. Sulla base del *Report* di F. Anthonio, Z. Rosson, KeepItOn, *Emboldened Offenders, Endangered Communities – Internet Shutdowns in 2024*, feb. 2025, a livello globale, nel 2024 sono stati registrati almeno 296 *shutdowns* in 54 paesi e l’India ha imposto 84 interruzioni («41 *shutdowns* were related to protests and 23 were related to communal violence», 20), risultando il Paese con più *shutdowns* tra le democrazie, seconda complessivamente solo a Myanmar (85) sulla cui vicenda si veda M. Ryan, M.V. Tran, *Democratic backsliding disrupted: The role of digitalized resistance in Myanmar*, in 9 *Asian Journal of Comparative Politics* 1 (2024). Per una riflessione sull’India, si vedano P. Prakash, *Internet blocking and shutdowns in India and international human rights law*, in 5 *Indian Public Policy Review* 3 (2024); G. Formici, *Access denied: gli Internet shutdowns alla prova del diritto. Spunti di riflessione a partire dalla giurisprudenza della Supreme Court indiana*, in *DPCE Online*, 1 (2023), spec. 116-128; K. Ruijgrok, *The authoritarian practice of issuing internet shutdowns in India: the Bharatiya Janata Party’s direct and indirect responsibility*, in 29 *Democratization* 4 (2022); N. Shah, *(Dis)information Blackouts: Politics and Practices of Internet Shutdowns*, in *International Journal of Communication*, 15 (2021); T. Singh, A. Mishra, K. Bapat, *Why Don’t They Just Stop Stopping the Internet? The Curious Case of India’s Internet Shutdowns*, in *VerfBlog* (26 Oct. 2021).

⁶ In un post ufficiale Meta ha affermato che la TTPA «introduces significant operational challenges and legal uncertainties» per gli inserzionisti e le piattaforme, rendendo impossibile offrire tali annunci nell’UE. A partire dal 6 ottobre 2025, gli annunci «political, electoral and social issue adverts are no longer able to be delivered in the EU» su Facebook e Instagram, sebbene la società abbia ribadito che gli utenti e i candidati possono continuare a pubblicare post e discutere di politica sulle piattaforme. Si veda *Ending Political, Electoral and Social Issue Advertising in the EU in Response to Incoming European Regulation*, blog ufficiale di Meta, 27 July 2025, disponibile su <https://www.facebook.com/government-nonprofits/blog/eu-announcement>.

formalmente di salvare questa distinzione con la fissazione di regole e principi di trasparenza, che cercano di separare i due ambiti⁷. In India, al contrario, la linea di confine appare decisamente più sfumata: Ministri, funzionari e titolari di incarichi pubblici tendono a utilizzare gli stessi canali digitali in maniera ibrida, sovrapponendo spesso ruoli istituzionali e attività politiche.

Alla luce di questo primo inquadramento comparato, la struttura del saggio è costruita in modo da sviluppare in modo sistematico, attraverso l'analisi dell'ordinamento vigente in India, le medesime questioni accennate in questo confronto con il modello europeo. Partendo dall'illustrazione del fondamento costituzionale della libertà di espressione e delle fonti giuridiche che disciplinano gli ambiti più tradizionali della comunicazione, lo studio sviluppa un'analisi dell'evoluzione della regolazione dei *media* e delle piattaforme digitali, mantenendo lungo tutto il percorso una costante attenzione alla dimensione giurisprudenziale. I paragrafi successivi sono riservati alla regolazione specifica della comunicazione elettorale, dove vengono affrontati i temi più attuali: i *deepfake*, il ruolo degli *influencer* nelle campagne elettorali, le inserzioni pubblicitarie a pagamento e il fenomeno delle *paid news*. Ulteriori riflessioni riguardano poi l'utilizzo dei *social media* da parte dei titolari di incarichi pubblici, che sono al tempo stesso soggetti politici, e le ipotesi di riforma legislativa al vaglio, volte a colmare le lacune esistenti e a rafforzare gli strumenti di contrasto alla manipolazione digitale. In conclusione, l'analisi del caso indiano consente di osservare in forma particolarmente nitida alcune tendenze, che attraversano molte democrazie: l'espansione degli strumenti di intervento pubblico nello spazio *online*, il ricorso sempre più frequente a logiche di controllo preventivo e il rischio di una progressiva normalizzazione di pratiche di limitazione dell'accesso all'informazione e della circolazione dei contenuti. In questo senso, il presente contributo utilizza l'India come laboratorio per interrogarsi sulle tensioni strutturali tra libertà di espressione, processi democratici e governo della comunicazione digitale di massa in una sfera pubblica che si sposta sempre più verso l'*online*.

2. La libertà di espressione nella Costituzione indiana: riconoscimento e limiti

⁷ Nell'ordinamento dell'UE la questione dell'utilizzo dei *social media* da parte dei titolari di cariche pubbliche non è oggetto di una disciplina specifica, ma è affrontata in modo indiretto dalle norme della TTPA e da strumenti di *soft law*. In assenza di una regolazione settoriale, assumono rilievo i principi elaborati dalla Corte europea dei diritti dell'uomo in materia di comunicazione politica, pluralismo e neutralità delle autorità pubbliche, pur in controversie non riferite direttamente ai *social media* o all'uso di account istituzionali (si vedano EctHR, *Bowman c. United Kingdom*, ric. n. 24839/94, 19-2-1998, e EctHR, *Animal Defenders International c. United Kingdom*, ric. n. 48876/08, 22-4-2013). In Italia, invece, la comunicazione istituzionale è espressamente disciplinata dalla l. 22-2-2000 n. 28 (cd. *par condicio*) con il divieto per le pubbliche amministrazioni di svolgere attività di comunicazione in periodo elettorale, salvo quelle impersonali e indispensabili (art. 9), principio applicato anche ai contesti digitali e vigilato dall'AGCOM.

Nel sistema delle fonti indiane il principale riferimento sulla libertà di espressione è rappresentato dall'art. 19(1)(a) Cost., che afferma: «*all citizens shall have the right to freedom of speech and expression*». L'esercizio di questo diritto non può chiaramente essere assoluto e già all'art. 19(2) Cost. si stabilisce che la legge può individuare delle «*reasonable restrictions*» per limitarlo «*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*».

La tutela della sovranità e dell'integrità dell'India è uno dei motivi dove è evidentemente necessario restringere questa libertà per contrastare meglio minacce come secessione, ribellione armata o aggressioni esterne. Questo specifico riferimento è stato inserito nel 1963 con un emendamento costituzionale, approvato in risposta a tensioni separatiste, esplicitando nello *Statement of Objects* del testo, che lo scopo era quello di attribuire poteri adeguati per limitare invocazioni secessioniste o che, comunque, potessero compromettere l'unità nazionale. Il legislatore e la giurisprudenza hanno provato anche a definire meglio i confini con altri tipi di violazione: ad esempio, l'incitamento alla sovversione contro il governo o al tradimento del proprio Paese rientrano nella sicurezza dello Stato, mentre disordini minori senza presumibili implicazioni di vasta portata non giustificano di per sé la censura in nome della sicurezza nazionale.

Anche la necessità di preservare l'ordine pubblico non aveva inizialmente un fondamento costituzionale, che consentisse la limitazione di questo genere di discorso politico e mediatico. Le sentenze *Romesh Thappar v. State of Madras*, AIR 1950 SC 124, e *Brij Bhushan v. State of Delhi*, AIR 1950 SC 129, pronunciate entrambe il 26 maggio 1950 dalla Corte Suprema, rappresentano i primissimi casi indiani in materia di libertà di stampa e sono celebri proprio perché hanno evidenziato l'assenza nel testo costituzionale di un esplicito riferimento al *public order* come ragione per la sua compressione, decidendo per l'annullamento della censura preventiva di alcune pubblicazioni. In conseguenza di questi giudizi, il 18 giugno 1951 il Parlamento approvò il *Constitution (First Amendment) Act*, che inserì appunto all'art. 19(2) Cost. la clausola dell'ordine pubblico e operò altre due modifiche chirurgiche, aggiungendo l'aggettivo «*reasonable*» alle restrizioni e la formula «*in the interests of*» prima dell'elenco dei motivi che le giustificano.

La celebre sentenza *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, pronunciata il 24 marzo 2015, è stata decisiva per definire in modo più puntuale il concetto di ordine pubblico, spiegando che «*mere discussion or even advocacy of a particular cause howsoever unpopular is at the heart of Article 19(1)(a). It is only when such discussion or advocacy reaches the level of incitement that Article 19(2) kicks in*». Sostanzialmente, quindi, l'ordinamento tutela anche i toni aspri o satirici nel dibattito pubblico, mentre, al contrario, la restrizione deve scattare se si tratta di «*“incitement”, specifically incitement which has a proximate relation to public disorder*» e con «*an imminent causal connection with public disorder*», allo scopo di reprimere rivolte, tumulti o crimini di massa, come, ad esempio, fermare discorsi che esortino alla violenza etnica. Si tratta di indicazioni fondamentali, perché in democrazia

l'ordine pubblico non può essere mai invocato alla stregua di un alibi strumentale per ottenere il silenziamento di critiche politiche espresse in modo pacifico⁸.

Un ulteriore limite riguarda la moralità pubblica e il buon costume, motivi che consentono di circoscrivere la libertà di espressione, al fine di impedire la diffusione di materiale osceno o gravemente offensivo del comune senso del pudore. La formulazione «*decency or morality*» dell'art. 19(2) Cost. è eccessivamente vaga e ha sollevato spesso critiche, perché apre potenzialmente a censure arbitrarie, come dimostrano i casi in cui autorità pubbliche o gruppi di pressione hanno invocato la moralità per boicottare e ostacolare la diffusione di idee progressiste o secolarizzate nei *media* e nel cinema⁹: gli autori e i responsabili di alcuni film con scene di amore interreligioso o tematiche LGBT hanno subito pressioni e minacce da parte di gruppi conservatori, e sono stati costretti a tagli o rinvii (si veda il § 6). A integrazione dei generici termini previsti in Costituzione, sono intervenuti, da una parte, il legislatore (artt. 292-294 del Codice penale indiano), che ha vietato, ad esempio, la vendita o l'esibizione pubblica di contenuti osceni, e, dall'altra, i Tribunali, che hanno elaborato parametri più moderni, basati sugli *standard* sociali contemporanei¹⁰, implicando, ad

⁸ Questa interpretazione si pone in continuità con l'orientamento della Corte Suprema indiana già espresso in *S. Rangarajan v. P. Jagjivan Ram*, (1989) 2 SCC 574, pronunciata il 22 marzo 1989, dove si affermava che «*our commitment to freedom of expression demands that it cannot be suppressed unless the situation created by allowing the freedom is pressing and the community interest is endangered [...] The anticipated danger should not be remote, conjectural or far-fetched*», nel contesto delle limitazioni previste dall'art. 19(2) Cost.

⁹ Nella stessa logica, anche libri di divulgazione su sessualità o diritti civili e opere cinematografiche sono stati sequestrati o ostacolati in alcuni Stati in nome della morale pubblica. Casi emblematici sono rappresentati dal film *Fire* (regia di Deepa Mehta, 1996) su una relazione omosessuale femminile, che è stato oggetto di proteste dei nazionalisti hindu con danneggiamenti alle sale cinematografiche e sospensioni delle proiezioni, e da *Lipstick Under My Burkha* (regia di Alankrita Shrivastava, 2016), inizialmente vietato dalla *Central Board of Film Certification* (CBFC) per violazione della *decency and morality* e poi distribuito solo per adulti, dopo la decisione del *Film Certification Appellate Tribunal* (FCAT). Questi episodi dimostrano come la vaghezza dell'art. 19(2) Cost. consenta forme di *moral policing* nei confronti di espressioni artistiche e culturali non conformi a visioni tradizionali.

¹⁰ Nella sentenza *Ranjit D. Udeshi v. State of Maharashtra*, AIR 1965 SC 881, pronunciata il 19 agosto 1964, la Corte Suprema afferma che «*where, obscenity and art are mixed, art must so preponderate as to throw the obscenity into a shadow or the obscenity so trivial and insignificant that it can have no effect and may be overlooked*», ma soprattutto questa decisione, dedicata al giudizio di libri o film controversi, esprimeva l'esigenza di tener conto dei costumi contemporanei e degli standard nazionali: «*in this connection the interests of our contemporary society [...] must not be overlooked [...] treating with sex [...] judged of by our national standards [...] must determine the result*». Cinquant'anni più tardi, la Corte Suprema è ritornata sul concetto degli standard contemporanei con piccole variazioni: in *Aveek Sarkar & Anr v. State of West Bengal and Anr*, (2014) 4 SCC 257, pronunciata il 3 febbraio 2014, sostiene che «*only those sex-related materials which have a tendency of exciting lustful thoughts can be held to be obscene, but the obscenity has to be judged from the point of view of an average person, by applying contemporary community standards*», mentre nella successiva *Devidas Ramachandra Tuljapurkar v. State of Maharashtra*, (2015) 6 SCC 1, pronunciata il 14 maggio 2015, spiega che «*while judging a particular photograph [...] as obscene in 2014, regard must be had to the contemporary*

esempio, che un contenuto “audace”, ma con chiaro valore artistico o sociale non possa essere censurato *a priori*, ma debba essere piuttosto apprezzato nel contesto complessivo dell’opera¹¹ e alla luce dei cambiamenti valoriali in atto nella società.

Anche la reputazione individuale è protetta dalla legge e in India la diffamazione rappresenta sia illecito civile che reato. La Corte Suprema ha reiteratamente confermato la legittimità costituzionale delle disposizioni penali sulla diffamazione (artt. 499-500 del Codice penale indiano), e, in particolare nella sentenza *Subramanian Swamy v. Union of India*, (2016) 7 SCC 221, pronunciata il 13 maggio 2016, i giudici hanno respinto integralmente le censure, ribadendo che il diritto alla reputazione è parte dell’interesse pubblico e, quindi, una limitazione dello *speech* intesa a proteggerlo è costituzionalmente valida¹². Per quanto attiene alla sfera della comunicazione politica, giornalisti e attivisti possono, dunque, criticare figure pubbliche anche duramente, ma non possono diffondere consapevolmente falsità lesive dell’altrui onorabilità. Si tratta di un freno che opera, peraltro, sia verso i *media* che verso gli stessi politici: accuse infondate o attacchi personali eccessivi possono sfociare in cause di diffamazione che i Tribunali valutano alla luce del bilanciamento tra diritto di critica e tutela della dignità personale.

In sintesi, la libertà di espressione in India, pur garantita dall’art. 19(1)(a) Cost., è circondata da una serie di limitazioni, che riflettono un’esigenza di equilibrio con altri diritti costituzionali di pari rilievo. La giurisprudenza ha progressivamente chiarito che le restrizioni sono legittime solo se ragionevoli, proporzionate e fondate su una connessione effettiva e prossima con i rischi che intendono prevenire. Allo stesso tempo, i giudici hanno ribadito che la critica politica, la battuta satirica e l’opera artistica – anche quando scomode o provocatorie – restano al cuore di questo diritto. Emerge già da queste prime riflessioni una dinamica, che riconosce il valore della libera espressione quale fondamento della democrazia, ma non trascura la necessità di preservare coesione nazionale, dignità della persona e ordine sociale.

mores and the national standards and not the standards of a group of susceptible or sensitive persons».

¹¹ La giurisprudenza indiana ha riconosciuto nella sentenza *K.A. Abbas v. Union of India & Anr*, (1971) 2 SCC 446, pronunciata il 24 settembre 1970, che «*a film must be taken as a whole, evaluated as a single integrated work of art or entertainment. If, in telling the story, it is logical, relevant or necessary to depict a passionate kiss or a nude human figure, there should be no question of excluding the shot, provided the theme is handled with delicacy and feeling, aiming at aesthetic expression and avoiding all suggestion of prurience or lasciviousness*». Sul tema i giudici sono tornati anche con la sentenza *Samaresh Bose v. Amal Mitra*, (1985) 4 SCC 289, pronunciata il 24 settembre 1985, in cui hanno esplicitato che «*an overall view of the obscene matter in the setting of the whole work would, of course, be necessary, but the obscene matter must be considered by itself and separately to find out whether it is so gross*».

¹² La Corte Suprema richiede un’applicazione equilibrata della disposizione, rifiutando un uso strumentale della norma e chiarendo che la tutela della reputazione non può neanche tradursi in un mezzo di compressione indebita del dissenso politico o della critica pubblica, essendo compito dei giudici effettuare una valutazione attenta del contesto, dell’interesse pubblico coinvolto e della proporzionalità dell’intervento repressivo.

3) L'accesso a Internet come diritto fondamentale

La giurisprudenza indiana ha storicamente svolto un ruolo cruciale nel bilanciare la libertà di espressione con altre esigenze costituzionali, svolgendo una funzione di arbitro nei casi di censura, regolamentazione dei media e accesso a Internet¹³. Negli ultimi anni, con l'ascesa del digitale, le Corti sono state chiamate non solo a interpretare la normativa tradizionale alla luce dei nuovi mezzi, ma anche a riconoscere nuovi diritti impliciti (come quello all'accesso alla rete), derivanti dai diritti fondamentali esistenti. Nel complesso, l'orientamento emerso è sufficientemente garantista verso le libertà civili in rete, pur riconoscendo la legittimità di restrizioni mirate per la sicurezza e l'ordine pubblico.

Concentrandoci in questo paragrafo sul filone giurisprudenziale relativo al riconoscimento dell'accesso a Internet¹⁴, è necessario partire dalla sentenza *Faheema Shirin R.K. v. State of Kerala*, AIR 2020 Ker 35, pronunciata il 19 settembre 2019 dalla *Kerala High Court*, che ha inserito il diritto ad avere accesso alla rete nella sfera dei diritti fondamentali garantiti dalla Costituzione. Il caso era nato dal ricorso di una studentessa espulsa da un convitto femminile per aver usato il cellulare oltre l'orario consentito. La giovane sosteneva che il regolamento dell'ostello, vietando l'uso serale di Internet, violasse i suoi diritti allo studio e alla *privacy*. I giudici del Kerala le diedero ragione con argomentazioni forti, dichiarando che la connessione alla rete deve ormai essere considerata una parte integrante sia del diritto all'istruzione, sia del diritto alla *privacy*, tutelati in India dall'art. 21 Cost. (diritto alla vita e libertà personale). La Corte osservò che in un'epoca digitale negare a un adulto l'uso di Internet equivale a privarlo di uno strumento essenziale di conoscenza e affermò che «*l'enforcement of discipline shall not be by blocking the ways and means of the students to acquire knowledge*». Dopo avere enfatizzato che anche l'ONU da anni considera il *right to Internet access* come un diritto umano fondamentale, la *Kerala High Court* ha riconosciuto, dunque, il diritto a Internet come

¹³ P. Passaglia, *La problematica definizione dell'accesso a Internet e le sue ricadute su esclusioni sociali e potenziali discriminazioni*, in *MediaLaws*, 3 (2021), 13-15.

¹⁴ Sul tema generale, si vedano, *ex aliis*, M. Reglitz, *Free Internet Access as a Human Right*, Cambridge, 2024; C.L. Alvarez, J.M.S. Díez, *The Content of the Right to Internet Access*, in 15 *Law, State & Telecommunications Review* 1 (2023); O. Pollicino, *The Right to Internet Access. A Comparative Constitutional Legal Framework*, in M. Ienca, O. Pollicino, L. Liguori, E. Stefanini, R. Andorno (eds), *The Cambridge Handbook of Information Technology, Life Sciences and Human Rights*, Cambridge, 2022; M.R. Allegri, *Il diritto di accesso a Internet: profili costituzionali*, in *MediaLaws* 1, 57 ss (2021); A.M. Gambino, R. Giarda, *L'accesso ad Internet come diritto*, *ivi*, 103 ss.; P. Tanzarella, *L'accesso a Internet è fondamentale, ma è davvero un diritto (fondamentale)?*, *ivi*, 39 ss.; B. Çalı, *The Case for the Right to Meaningful Access to the Internet as a Human Right in International Law*, in A. von Arnould, K. von der Decken, M. Susi (eds), *The Cambridge Handbook on New Human Rights. Recognition, Novelty, Rhetoric*, Cambridge, 2020, 276 ss.; O. Pollicino, *The Right to Internet Access: Quid Iuris?*, *ivi*, 263 ss.; T.E. Frosini, *Liberté égalité Internet*, Napoli, 2^a ed., 2019; S. Tully, *A Human Right to Access the Internet? Problems and Prospects*, in 14 *Human Rights Law Review* 2 (2014); L. Cuocolo, *La qualificazione giuridica dell'accesso a Internet, tra retoriche globali e dimensione sociale*, in *Politica del diritto*, 2-3 (2012); T.E. Frosini, *Il diritto costituzionale di accesso a internet*, in *Rivista AIC*, 1 (2011).

elemento del diritto alla vita, perché funzionale all'istruzione e al libero sviluppo della personalità, nonché come aspetto della libertà di espressione (art. 19(1)(a) Cost.), perché Internet è un mezzo di informazione e di dialogo pubblico. La dimensione del diritto alla *privacy* viene in rilievo in quanto la restrizione si riferiva soprattutto a studentesse, impattando sulla loro autonomia personale: la Corte affermò che un'adulta ha il diritto di decidere come usare il cellulare e un divieto generalizzato in nome della moralità era da considerare ingiustificato e discriminatorio. Questo giudizio rappresenta la prima sentenza del suo genere ed è un precedente importante, spesso utilizzato come prova che in India l'accesso a Internet non può essere interdetto arbitrariamente e senza una motivazione valida né dallo Stato, ma neanche da soggetti privati (come, ad esempio, istituzioni educative)¹⁵.

Sulla portata del diritto a Internet e sui limiti delle sue restrizioni, la Corte suprema si è espressa la prima volta con la sentenza *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637, pronunciata il 10 gennaio 2020. Questo caso riguardava il *blackout* totale delle comunicazioni imposto nel *Jammu & Kashmir* nell'agosto 2019, contestualmente alla revoca dell'autonomia speciale della regione (art. 370 Cost.). Una giornalista (Anuradha Bhasin) e altri ricorrenti contestarono che la prolungata sospensione di Internet violasse i loro diritti fondamentali, impedendo alla stampa locale di operare e ai cittadini di essere informati, di esprimersi o anche di svolgere alcune attività lavorative. Pur senza dichiarare un diritto illimitato a Internet¹⁶, la sentenza stabilisce alcuni principi chiave, a partire dall'affermazione che la libertà di espressione tramite Internet è protetta dalla Costituzione al pari di quella esercitata su altre piattaforme tradizionali e, pertanto, pubblicare idee *online* rientra nel perimetro dell'art. 19(1)(a) Cost. e fare *business* su Internet in quello dell'art. 19(1)(g) sulla libertà di commercio: eventuali restrizioni devono, quindi, superare il vaglio di ragionevolezza *ex* art. 19(2) Cost. La Corte Suprema ha anche stabilito l'illegalità della sospensione a tempo indeterminato di Internet: i provvedimenti devono avere un arco temporale preciso ed essere periodicamente riesaminati, perché un *blackout* permanente è sproporzionato rispetto a qualsiasi obiettivo di ordine pubblico. I giudici hanno, infine, imposto al governo l'obbligo di pubblicare e motivare per iscritto qualunque ordine di *shutdown* o limitazione.

Nel caso *Anuradha Bhasin*, la Corte Suprema non ha ordinato immediatamente di ristabilire Internet in *Kashmir*, ma ha rimandato al governo il riesame, dopo aver enunciato chiaramente che il *blackout* non può essere usato come misura ordinaria di controllo e repressione e che l'accesso a Internet risulta soggetto esclusivamente a eccezioni

¹⁵ Per un'analisi dettagliata della sentenza, si veda J. Preeti, *Faheema Shirin v. State of Kerala: In Light of Right to Internet*, in *ILI Law Review* (Summer 2020).

¹⁶ In G. Formici, *Access denied: gli Internet shutdowns alla prova del diritto. Spunti di riflessione a partire dalla giurisprudenza della Supreme Court indiana*, cit., 137, è stato evidenziato come pervasive «forme di controllo di Internet finiscano col favorire pratiche di recessione democratica, così da condurre ad uno scivolamento insidioso da *Internet shutdown* a *democracy shutdown*». Per una riflessione più ampia, si veda J. Thumfart, *Digital Rights and the State of Exception. Internet Shutdowns from the Perspective of Just Securitization Theory*, in *9 Journal of Global Security Studies* 1 (2024).

strettamente necessarie e proporzionate per la sicurezza nazionale e l'ordine pubblico. Questo verdetto è stato considerato tendenzialmente assai equilibrato¹⁷: viene riconosciuta la gravità dell'impatto di uno *shutdown*¹⁸, sottolineando che tali misure ostacolano istruzione, lavoro e servizi essenziali, ma allo stesso tempo si lascia spazio all'esecutivo per valutare blocchi mirati in situazioni di reale emergenza (ad esempio rivolte violente), sotto vincolo di stretta revisione e con durata temporanea e limitata al minimo indispensabile¹⁹.

Pochi mesi dopo, nella sentenza correlata *Foundation for Media Professionals v. Union Territory of Jammu & Kashmir*, WP (C) n. 10817/2020 SCC, pronunciata l'11 maggio 2020, la Corte Suprema ha dovuto affrontare la questione della riduzione del segnale Internet da 4G a 2G in *Kashmir*²⁰, che rendeva impossibile videochiamate, *streaming* di lezioni, etc. Pur non ripristinando immediatamente il 4G, i giudici hanno applicato i minimi standard, stabiliti nel caso *Anuradha Bhasin*, constatando che l'ordine non motivava adeguatamente il *downgrade*. Di conseguenza hanno richiesto la costituzione di uno *Special Committee* (guidato dal Ministro

¹⁷ Nel caso specifico, il 14 gennaio 2020, come conseguenza della sentenza, in Jammu e Kashmir è stato parzialmente ripristinato l'accesso alla rete, ma a bassa velocità (2G), in certi distretti della regione e riservato a telefoni post-paid e siti cd. *whitelisted* (banche, servizi governativi, etc.). Soltanto il successivo 4 marzo, dopo oltre 200 giorni, viene ripristinato l'accesso alla linea fissa di *Internet* nella valle del Kashmir.

¹⁸ Nel Rapporto di *Human Rights Watch* del 14 giugno 2023, dall'emblematico titolo *No Internet means no work, no pay, no food: Internet shutdowns deny access to basic rights in "digital India"*, è inserita, tra le Raccomandazioni finali al Parlamento indiano, quella di «*reject the Telecommunications Bill, 2022, which contravenes the Supreme Court judgment in Anuradha Bhasin v. Union of India and expands the powers of government officials to impose network disruptions at their discretion, without any meaningful safeguards, limitations, or remedies to ensure transparency, accountability, and redress*».

¹⁹ Per approfondimenti sulla sentenza *Anuradha Bhasin*, si vedano R.M. Deka, *Case Comment: Anuradha Bhasin v. Union of India*, in 2 *Journal of Legal Research and Juridical Sciences* 3 (2023); R. Juyal, *Constitutional Liberties and Cyberspace: Analysing the Anuradha Bhasin Case and Its Impact on Fundamental Rights*, in 23 *Legal Information Management* 4 (2023); P. Thakur, S. Choudhary, *Competing Concerns of Public Security and Individual Liberty: A Critique of The Supreme Court Judgement in Anuradha Bhasin v. Union of India*, in *HPNLU Law Journal* 1 (2020).

²⁰ In questo quadro, il caso dello Jammu e Kashmir assume un valore paradigmatico non solo per la frequenza e la durata degli *shutdowns*, ma perché mostra come la regolazione dell'accesso alla rete possa trasformarsi da misura eccezionale di sicurezza in tecnica ordinaria di governo di uno spazio politicamente conteso. Si vedano R.A. Peerzada, A. Sharma, S. Kannan, G. Malhotra, *The politics of internet shutdowns in Jammu and Kashmir*, in *Human Geography*, 2025; D. Tayal, S. Jaggarwal, *A Perspective of Internet Shutdown in J & K: Outcomes And Challenges*, in 7 *International Journal of Research and Analytical Reviews* 1 (2022); Nota HLW, *From domicile to dominion: India's settler colonial agenda in Kashmir*, in 134 *Harvard Law Review* 7 (2021); S. Bashir, M.B. Awan, *India's digital repression in Jammu and Kashmir: A human rights perspective*, in 18 *Webology* 5 (2021); S. Qadir, A.A. Dar, *How Internet Shutdowns Affects the Entrepreneurs in J&K*, in 12 *International Journal of Asian Business and Information Management* 3 (2021); H. Duschinski, S.N. Ghosh, *Constituting the occupation: Preventive detention and permanent emergency in Kashmir*, in 49 *The Journal of Legal Pluralism and Unofficial Law* 3 (2017).

degli Interni) per riesaminare periodicamente (circa ogni quindici giorni) la necessità di mantenere la rete a 2G²¹.

In conclusione, questi casi hanno consolidato il concetto che l'accesso alla rete, pur non essendo nominato esplicitamente in Costituzione, sia ormai una "infrastruttura" essenziale per l'esercizio pieno di molte libertà fondamentali²² e sia, quindi, meritevole di una tutela indiretta. La giurisprudenza ha finora esercitato un ruolo da tutore: la Corte Suprema e le *High Courts* hanno, infatti, ampliato l'ombrello dei diritti fondamentali per adattarlo all'era di Internet, affermando il principio per cui la rete tutela certe libertà e stoppando derive troppo repressive, ma, al contempo, non hanno esitato a richiamare l'esecutivo ai suoi doveri di salvaguardia della sicurezza e dell'ordine, ricorrendo però a mezzi legali e proporzionati.

4. Le regole tradizionali: dai giornali alla televisione

Il sistema mediatico indiano è stato a lungo regolato da un mosaico di organismi settoriali, istituiti in epoche diverse e ben prima dell'avvento dei *social network* e delle piattaforme digitali. Nel settore cinematografico, ad esempio, un ruolo centrale è svolto dalla *Central Board of Film Certification* (CBFC), istituita nel 1952, che esercita un controllo preventivo sui film, sulle serie e sui documentari destinati alla distribuzione nelle sale cinematografiche e alla trasmissione televisiva. La CBFC è incaricata di visionare le opere prima della loro diffusione pubblica, attribuendo la certificazione per fasce di età e imponendo, ove ritenuto necessario, tagli, modifiche o divieti di proiezione, sulla base di criteri legati alla moralità pubblica, alla decenza, all'ordine pubblico e alla sicurezza dello Stato. Questo modello riflette una concezione della regolazione dei *media* fortemente improntata al controllo *ex ante* dei contenuti, nella quale l'intervento dell'autorità pubblica si colloca, pertanto, "a monte" della circolazione dell'opera. Al tempo stesso, la competenza della CBFC resta circoscritta all'ambito cinematografico e audiovisivo in senso stretto: l'organo non svolge alcuna funzione di vigilanza sulla correttezza dell'informazione, sul pluralismo dei *media* o sui contenuti giornalistici, che rimangono affidati a meccanismi e organismi distinti.

Il *Press Council of India* (PCI) esiste invece dal 1978 e rappresenta il principale organismo di autoregolazione della stampa nell'ordinamento indiano. Istituito ai sensi del *Press Council of India Act*, il PCI è «*a statutory and quasi-judicial body*», finalizzato a «*preserving the freedom of the press by maintaining and improving the standards of newspapers and the news agencies*»²³. La composizione del Consiglio è abbastanza articolata: il

²¹ Alla fine, dopo circa un anno, il 5 febbraio 2021, il governo ha ripristinato l'accesso mobile a Internet 4G, restituendo alla regione la piena connettività alla banda larga.

²² Non deve sorprendere che questa giurisprudenza abbia trovato eco in altre giurisdizioni: la *Kenya High Court*, ad esempio, ha citato espressamente il precedente indiano, quando ha riconosciuto il diritto di accesso a Internet come diritto fondamentale nel 2021.

²³ In sintesi, il PCI è chiamato a tutelare la libertà di stampa e, al contempo, a promuovere il rispetto di standard etici e professionali nel giornalismo.

Presidente è scelto solitamente tra gli ex giudici della Corte Suprema, mentre dei 28 membri aggiuntivi 20 sono espressione dei *media*, indicati da giornali e altri organi di stampa operanti nel Paese, 5 sono componenti del Parlamento e 3 vengono dalla cultura letteraria e dall'ambito legale²⁴. Il Consiglio dispone di diverse facoltà, tra cui la possibilità di avviare procedimenti su segnalazione o d'ufficio, formulare rilievi e raccomandazioni nei confronti delle testate e pronunciarsi su condotte ritenute contrarie alla deontologia giornalistica²⁵. Tuttavia, i suoi poteri restano prevalentemente di natura morale e persuasiva, in quanto privi di efficacia coercitiva diretta, circostanza che ha alimentato nel tempo un ampio dibattito sui limiti strutturali dell'autoregolamentazione nel garantire un'effettiva responsabilità dei *media*. Inoltre, la sua giurisdizione resta, comunque, limitata alla carta stampata²⁶, non potendo esercitare alcun potere diretto sui *media* elettronici (radio, televisione), né tantomeno su quelli digitali o sui *social network*.

L'avvento di TV private e piattaforme *online* ha, quindi, fatto emergere presto vaste aree della comunicazione politica che restavano fuori controllo ed era stato ipotizzato un ampliamento della competenza del *Press Council* o la creazione di un organismo analogo per TV e radio, nella consapevolezza che la sola autoregolamentazione rischia di essere insufficiente, in particolare nei contesti politicamente sensibili e durante le campagne elettorali²⁷. Per quanto riguarda televisione e radio, la regolazione è stata storicamente accentrata a livello federale presso il *Ministry of Information and Broadcasting* (MIB): fino ai primi anni '90 la radiotelevisione era ancora monopolio statale, poi con la liberalizzazione è stata consentita la nascita di emittenti private, sottoposte a licenza e a codici di condotta emanati dal Ministero. Il *Cable Television Networks (Regulation) Act, 1995* (Cable TV Act), ha imposto alle emittenti via cavo (oggi è esteso a satellite/IPTV) di rispettare un Codice di programmi e pubblicità con standard di decoro, veridicità e rispetto delle varie comunità, consentendo il sequestro delle apparecchiature dei distributori via cavo che diffondono programmi contrari al Codice. Il rispetto di questo Codice non è lasciato alla sola volontà delle TV: in caso di violazioni flagranti (ad

²⁴ Questi tre componenti sono indicati rispettivamente da *Sahitya Academy*, *University Grant Commission* e *Bar Council of India*.

²⁵ Le decisioni del *Press Council* non sono, inoltre, giustiziabili in Tribunale e, soprattutto, non possono imporre il pagamento di sanzioni economiche o prevedere effetti penali. Il PCI può determinare solo una sanzione di immagine, richiedendo, ad esempio, la pubblicazione delle proprie deliberazioni sulle testate coinvolte e confidando così nel "tribunale dell'opinione pubblica" come deterrente.

²⁶ In questo contesto si inserisce il *Press and Registration of Periodicals Act, 2023*, che ha sostituito la disciplina ottocentesca del *Press and Registration of Books Act, 1867*, modernizzando il sistema di registrazione delle pubblicazioni periodiche e semplificando le procedure amministrative, senza incidere in modo significativo sulla struttura, sulle funzioni e sui poteri del *Press Council of India*.

²⁷ Sul *Press Council of India*, sulla sua composizione, sui poteri prevalentemente non coercitivi e sui limiti strutturali in termini di indipendenza ed efficacia, si vedano, tra gli altri, S. Seshadri, *Press Council of India Act, (Nov. 2023), working paper*, disponibile su <http://dx.doi.org/10.2139/ssrn.4629750>; S. Kumari, *Press Council of India: A Critical Analysis*, in *Bharati Law Review* (April–June 2015). Inoltre, sono utili i *Press Council of India Annual Reports* per dati attuali sull'attività dell'organismo.

esempio, incitamento all'odio, volgarità estrema, allarmismo infondato), le autorità possono intervenire d'ufficio. Inoltre, le condizioni di ogni licenza radiotelevisiva includono il rispetto ulteriore di linee guida sui contenuti e il MIB può sospendere o revocare la licenza di un canale in caso di infrazioni gravi o reiterate.

La *Telecom Regulatory Authority of India* (TRAI) è stata istituita nel 1997 originariamente per il settore telecomunicazioni, ma dal 2004 ha ottenuto competenze anche sulla trasmissione radiotelevisiva (*broadcasting*) per quanto riguarda gli aspetti tecnici e commerciali (tariffe, interconnessioni, qualità del servizio), ma non sul contenuto editoriale. La TRAI garantisce pluralità e concorrenza nelle infrastrutture (ad esempio, regola i prezzi degli abbonamenti TV, gli accordi tra *broadcaster* e operatori via cavo/DTH), ma le questioni di etica dell'informazione o di propaganda politica esulano dal suo mandato: la TRAI non sanziona, infatti, né le *fake news*, né la propaganda sui canali, limitandosi a interventi pro-concorrenziali (come imporre il *must-carry* di canali pubblici o limitare la concentrazione proprietaria nelle piattaforme). In questo ambito, quindi, si realizza una distinzione funzionale delle competenze: il MIB conserva un ruolo decisivo sui contenuti e sulle politiche editoriali, mentre la TRAI è prevalentemente responsabile della regolazione tecnica ed economica, oltre ad avere poteri consultivi su molti aspetti.

Proprio in sede consultiva, la TRAI aveva proposto la creazione di un'autorità unica, che ricalcasse un po' il modello dell'*Office of Communications* (*Ofcom*) britannico, l'autorità di regolamentazione e concorrenza del Regno Unito per i settori della radiodiffusione, di Internet, delle telecomunicazioni e dei servizi postali, ma queste proposte non si sono mai concretizzate e l'industria mediatica ha allora tentato forme di autoregolamentazione. Ad esempio, le *TV news* private hanno creato la *News Broadcasters Association* (NBA), oggi *News Broadcasters & Digital Association* (NBDA), con un proprio Codice etico e un organo di vigilanza interno chiamato *News Broadcasting Standards Authority* (NBSA), oggi *News Broadcasting & Digital Standards Authority* (NBDSA). La NBDSA riceve reclami del pubblico sui notiziari e può ammonire o irrogare sanzioni pecuniarie (fino a circa 100.000 rupie) alle emittenti associate per violazioni etiche.

Sempre nell'ambito dell'autoregolamentazione, esistono il *Broadcast Editors' Association* e l'*Advertising Standards Council of India* con linee guida sugli spot pubblicitari. Tuttavia, questi organismi non esercitano poteri vincolanti, funzionano su base volontaria e i loro membri aderiscono, infatti, per impegno deontologico, non per obbligo di legge. Di conseguenza, il loro impatto su fenomeni come la disinformazione politica o i discorsi d'odio è rimasto limitato ai soli aderenti e spesso inefficace nei casi più gravi. Il rafforzamento di questi meccanismi e la creazione di un regolatore indipendente sono stati spesso oggetto di dibattito, alla luce della consapevolezza che l'assenza di sanzioni reali rende l'autodisciplina un'arma spuntata.

In sintesi, nel sistema tradizionale il governo federale, attraverso il MIB, ha formalmente mantenuto poteri diretti di controllo sui contenuti *broadcast*, esercitati soprattutto tramite la censura cinematografica e una regolamentazione di carattere generale, volta a prevenire contenuti ritenuti

lesivi dell'ordine pubblico, della moralità o del decoro nei notiziari e nei programmi di intrattenimento. In assenza di un regolatore indipendente, tuttavia, questi poteri sono stati nella prassi esercitati prevalentemente attraverso strumenti informali e cooperativi, favorendo prassi di autoregolamentazione *de facto* nel funzionamento ordinario, mediante l'adozione di *advisories* e *warnings*, e confidando nell'adeguamento spontaneo dei *media*²⁸, mentre interventi punitivi diretti nei confronti dei canali televisivi sono rimasti circoscritti a casi eclatanti.

Nel complesso, queste “vecchie regole” hanno mostrato forti limiti di efficacia di fronte alle trasformazioni digitali. Il *Press Council*, come si è visto, resta il “guardiano” della stampa, ma non ha potere su portali *online*, *social network* o canali TV. Il MIB, pur potendo sorvegliare e intervenire sulla TV tradizionale, non ha avuto strumenti equivalenti per YouTube o Netflix fino a tempi recenti. La supervisione pubblica sui contenuti politici in rete è rimasta, dunque, a lungo vacante: i *social media* e le piattaforme digitali prima del 2021 erano regolati solo da norme penali generali (diffamazione, oltraggio, odio religioso) e dall'IT Act del 2000, che però, come vedremo, non aveva meccanismi precisi per il monitoraggio continuo dei contenuti. Persino il *Ministry of Electronics and Information Technology* (MeitY), competente per Internet, si limitava a interventi mirati (come disporre blocchi di siti web o la rimozione di contenuti illegali), senza un sistema organico di vigilanza. Si comprende, quindi, come i vuoti normativi abbiano indotto il governo indiano a emanare nuove regole e proporre riforme strutturali per colmare la “zona franca” in cui prosperavano disinformazione e propaganda politica *online*.

5. L'IT Act: procedure, giurisprudenza e applicazioni concrete

L'*Information Technology Act* (IT Act), approvato nel 2000, costituisce il quadro di riferimento generale per il mondo digitale in India. Nato per regolare il commercio elettronico e i reati informatici, questo testo è divenuto nel tempo l'infrastruttura normativa sulla quale costruire regole per *social media*, *streaming* e comunicazioni *online*. Già nel 2008 il Parlamento indiano ha profondamente emendato l'IT Act, introducendo, tra le altre misure, la sezione 66A, in materia di *punishment for sending offensive messages through communication service*, etc, e la sezione 69A, che attribuisce al governo centrale il *power to issue directions for blocking for public access of any information through any computer resource*. In base a tale norma, le autorità possono oscurare informazioni accessibili al pubblico tramite qualsiasi computer o rete, qualora ciò sia «*necessary or expedient [...] in the interest of sovereignty and integrity of India, defence of India, security of the*

²⁸ Sul modello indiano di autoregolazione dei *media* e sui limiti strutturali della *self-regulation* nel contesto della libertà di stampa e della responsabilità giornalistica, si veda M. Mathew, *Media Self-Regulation in India: A Critical Analysis*, in *ILI Law Review* (Winter 2016), che, muovendo dall'analisi del *Press Council of India*, esamina più in generale le criticità dei meccanismi di autoregolamentazione nel sistema dei *media* indiani, evidenziando la debolezza dei poteri vincolanti e l'inefficacia delle procedure di reclamo nel garantire standard etici e *accountability*.

State, friendly relations with foreign States or public order, or for preventing incitement to the commission of any cognizable offence relating to above».

Come si può subito notare, le motivazioni che consentono il blocco ricalcano quasi esattamente le eccezioni costituzionali previste dall'art.19(2) Cost., con la significativa differenza che nella sezione 69A non compaiono concetti come la moralità o la diffamazione: la scelta del legislatore è stata, dunque, quella di escludere dalle prerogative governative la possibilità di oscuramenti connessi a contenuti indecenti o lesivi della reputazione (che restano tutelati da altre leggi, a partire dal Codice penale), limitando invece questa facoltà alle ipotesi di minaccia alla sicurezza e all'ordine pubblico in senso lato.

La procedura per il blocco di un sito o di un contenuto *online* è contenuta nelle *Blocking Rules* del 2009, che danno attuazione alla sezione 69A dell'IT Act. Il reclamo non può essere presentato direttamente da un cittadino, ma deve essere prima "filtrato" da un *Nodal Officer* di un'amministrazione competente, il quale, se ritiene fondata la richiesta, la inoltra al *Designated Officer* (DO) del governo centrale. Ricevuta la segnalazione, il DO, da una parte, la protocolla e la sottopone a un *Committee for Examination of Request*²⁹; dall'altra, deve compiere «*all reasonable efforts*» per identificare la persona o l'intermediario che ha ospitato le informazioni, nonché la risorsa informatica su cui tali informazioni sono ospitate, al fine di notificare la richiesta e offrire la possibilità di «*appear and submit their reply and clarifications*» con un preavviso di almeno 48 ore³⁰.

Il Comitato esamina la richiesta e valuta se rientra nello spettro di applicazione della sezione 69A: se ritiene giustificato bloccare le informazioni, formula una raccomandazione scritta da trasmettere al *Secretary* del *Department of Information Technology*, che è l'autorità competente a emettere l'ordine di blocco. Se il Segretario approva la richiesta, il DO dispone nei confronti di «*any agency of the Government or the intermediary to block the offending information generated, transmitted, received, stored or hosted in their computer resource for public access within the time limit specified in the direction*» (*Rule 8*), mentre, se non la ritiene fondata, si procede all'archiviazione. L'intero procedimento deve, comunque, concludersi entro sette giorni lavorativi dal momento della ricezione della richiesta³¹.

²⁹ Il Comitato è presieduto dal *Designated Officer* ed è composto da rappresentanti, non inferiori al grado di *Joint Secretary*, dei Ministeri *Law & Justice*, *Home Affairs* e *Information & Broadcasting*, oltre che dell'*Indian Computer Emergency Response Team* (CERT), un ufficio che opera sotto il *Ministry of Electronics and Information Technology*, fornendo servizi in materia di sicurezza informatica. La sua principale funzione è il coordinamento delle attività di risposta agli incidenti, ma svolge anche un importante ruolo preventivo tramite l'analisi e la diffusione di informazioni su attacchi informatici, l'emissione di avvisi e previsioni, l'implementazione di misure di emergenza.

³⁰ Se non vengono presentate memorie, la decisione è presa, comunque, sulla base dei documenti raccolti.

³¹ La *Rule 9* prevede una procedura d'urgenza: nei casi in cui non è ritenuto possibile attendere, il DO può sottoporre immediatamente la questione al Segretario del *Department of Information Technology*, il quale ha il potere di decidere un blocco

L'impianto di regole comprende altri aspetti significativi, tra cui si evidenziano gli obblighi stringenti in capo agli intermediari (sulla base della *Rule* 13 devono nominare un referente capace di ricevere gli ordini e dare conferma entro due ore dalla notifica, pena la possibilità di subire azioni ai sensi della sezione 69A, paragrafo 3) e la previsione di un *Review Committee*, che si riunisce almeno ogni due mesi per esaminare gli ordini di blocco già emessi e verificare che siano conformi alla legge (*Rule* 14)³². Tutto il procedimento, dalla segnalazione alla decisione finale, è coperto poi da un regime rigoroso di riservatezza: le richieste, i documenti e le azioni intraprese non sono resi pubblici (*Rule* 16): la segretezza imposta agli ordini di blocco è ideata, pertanto, in termini di garanzia, ma ha comportato la spiacevole conseguenza di rendere più difficile la verifica della loro proporzionalità e legittimità sostanziale.

Tutti questi profili procedurali sono stati determinanti per la legittimità costituzionale della sezione 69A dell'IT Act: nel già menzionato caso *Shreya Singhal*, considerato una pietra miliare nella protezione della libertà di parola *online*, la Corte Suprema ha deciso di confermarne la validità proprio alla luce delle importanti cautele previste. La Corte ha sottolineato che la norma delimita chiaramente i casi eccezionali in cui la libertà di espressione *online* può essere compressa e che le *Blocking Rules* stabiliscono un *iter* rigoroso (ordine scritto motivato, diritto al contraddittorio e revisione interna), tale da rendere più difficili arbitri eccessivi dell'esecutivo. Nel rispetto della ragionevolezza nell'applicazione delle restrizioni e nel rispetto delle tutele previste, la norma ha, dunque, superato il vaglio di costituzionalità per la sua precisione e proporzionalità: può essere considerato uno strumento mirato, utilizzabile solo per gravi esigenze di sicurezza e incardinato in un processo decisionale, che bilancia le diverse esigenze e i diritti che entrano in gioco.

È fondamentale sottolineare che nel medesimo giudizio la Corte Suprema ha invece bocciato la sezione 66A dell'IT Act³³, articolando il proprio ragionamento lungo tre assi principali. La prima questione risiede nella vaghezza dei termini utilizzati («*open-ended and undefined*»), in quanto «*expressions such "grossly offensive" or "menacing" are so vague that there is no manageable standard by which a person can be said to have committed an offence*» (par. 83): l'indeterminatezza della norma genera inevitabilmente arbitrarietà e discrezionalità, in contrasto con il principio di legalità. Il secondo tema riguarda la non riconducibilità delle restrizioni alle categorie

senza *hearing*, ma tale ordine deve essere riesaminato entro 48 ore dal Comitato. Se il Comitato non conferma, l'ordine viene revocato e il sito deve essere sbloccato. Un'ulteriore ipotesi (*rule* 10) è quella in cui il blocco sia disposto da un Tribunale competente: in quel caso il DO, dopo aver ricevuto copia certificata dell'ordine, lo trasmette direttamente, che si occupa dell'esecuzione immediata.

³² Se il *Review Committee* accerta che un ordine non soddisfa i requisiti della sezione 69A, può «*set aside the directions and issues order for unblocking of said information generated, transmitted, received, stored or hosted in any computer resource for public access*».

³³ G. Bhatia, *The Striking Down of Section 66A*, in *Indian Constitutional Law and Philosophy* (26 Mar. 2015); R. Samueli, *Shreya Singhal v. Union of India: Part I – Overbreadth, chilling effect and permissible restrictions on speech*, in *Spicyip - De-Coding Indian Intellectual Property Law* (2 Apr. 2015).

stabilite in Costituzione per ritenere «*reasonable*» la contrazione della libertà di espressione: infatti per la Corte «*information that may be grossly offensive or menacing is not necessarily information which falls under any of the subject-matters contained in Article 19(2)*» (par. 90). Il terzo profilo attiene alla distinzione già trattata nel § 2 tra discussione/*advocacy* e incitamento: la Corte Suprema prima richiama la giurisprudenza statunitense e la metafora del “*market place of ideas*” (par. 13), poi stabilisce la differenza tra i due concetti (parr. 15-16) e, infine, conclude con la necessità di una «*proximate and imminent causal connection with the expression that is sought to be curtailed*» (par. 20)³⁴ per rientrare tra le restrizioni legittime³⁵.

La sentenza *Shreya Singhal* ha affrontato la questione di legittimità costituzionale anche della sezione 79 dell’IT Act, che prevede il *safe harbour* per gli intermediari *online* (*social network*, *forum*, *provider*), esonerandoli da responsabilità per le pubblicazioni degli utenti, a patto che rispettino alcune condizioni e rimuovano sollecitamente eventuali contenuti illegali. Questo “scudo” ha reso le piattaforme non penalmente responsabili di ogni post e la Corte Suprema ha chiarito che gli intermediari non hanno un obbligo di rimozione, dopo una richiesta proveniente da singoli cittadini, ma solo da ordini giudiziari o direttive governative: da una parte, si rafforza così l’equilibrio tra libertà di espressione e responsabilità nel contesto digitale, mentre, dall’altra, si cercano di limitare possibili abusi ad opera della polizia o delle burocrazie inferiori.

Tornando alla sezione 69A, è opportuno evidenziare che la Corte Suprema, pur avendo salvato la norma, ha ribadito che il suo utilizzo deve essere ragionevole e rispettare in pieno le garanzie previste: il governo non può, quindi, scavalcare le procedure in modo discrezionale: ogni *takedown* di siti o oscuramento di post e account dev’essere giustificato dai motivi elencati nella legge e deve seguire la procedura corretta, pena l’illegittimità del provvedimento. Nonostante la cornice garantista, negli ultimi anni

³⁴ Il criterio della “*proximate and imminent causal connection*”, elaborato dalla Corte Suprema indiana, trae chiaramente ispirazione dal modello statunitense del “*clear and present danger*”, teorizzato da Oliver Wendell Holmes in *Schenck v. United States*, 249 U.S. 47 (1919): «*the question in every case is whether the words are used in such circumstances and are of such a nature as to create a clear and present danger that they will bring about the substantive evils that Congress has a right to prevent*». Negli Stati Uniti la dottrina è stata poi affinata con la sentenza *Brandenburg v. Ohio*, 395 U.S. 444 (1969), con il test dell’“*imminent lawless action*”, per il quale sono ammesse restrizioni unicamente per discorsi «*directed to inciting or producing imminent lawless action and likely to incite or produce such action*». Tale costruzione concettuale ha certamente contribuito a orientare anche la giurisprudenza indiana, che oggi, infatti, utilizza un parametro analogo per distinguere la semplice *advocacy* dall’incitamento punibile.

³⁵ È significativo osservare che, nonostante la dichiarazione di incostituzionalità della sezione 66A dell’IT Act, pronunciata nel 2015, la disposizione abbia continuato a essere applicata nella prassi per diversi anni. Con l’ordinanza del 14 luglio 2021 (*People’s Union for Civil Liberties v. Union of India*), la Corte Suprema ha preso atto che oltre 1.300 procedimenti penali risultavano ancora pendenti o erano stati avviati successivamente alla sentenza *Shreya Singhal*, sulla base di una norma ormai priva di efficacia giuridica. La Corte ha, pertanto, ordinato l’archiviazione di tutti i procedimenti fondati sulla sezione 66A e ha richiamato formalmente l’Unione e gli Stati al dovere di conformarsi al giudicato costituzionale, evidenziando le gravi criticità nell’attuazione effettiva delle garanzie sulla libertà di espressione *online*.

questa disposizione è diventata però lo strumento con cui l'esecutivo ha gestito svariate crisi legate al web.

Le prime applicazioni rilevanti arrivano nel 2020: il 29 giugno il governo Modi mette al bando 59 applicazioni mobili di origine cinese o, comunque, con forti legami societari cinesi (tra cui *TikTok*, *WeChat*, *CamScanner* e *UC Browser*), giustificando la decisione per ragioni di sicurezza nazionale e tutela della protezione dei dati dei cittadini indiani; il successivo 2 settembre segue un pacchetto di altre 118 *app* (tra cui *PUBG Mobile*, gestita dalla *Tencent Holdings*, *Camcard* e *Baidu*) e il 24 novembre un terzo blocco, stavolta riguardante 43 *app* (tra cui *AliExpress* e *Ding Talk*), con motivazioni analoghe, basate su considerazioni relative a sovranità, integrità, difesa, sicurezza dello Stato e ordine pubblico. In tutte queste "ondate", la matrice cinese è chiaramente rivendicata nei comunicati ufficiali ed emerge nella stampa internazionale³⁶. Il 14 febbraio 2022 vengono bloccate ulteriori 54 *app* (la gran parte è ancora cinese, ma la lista non è omogenea e vi figura, ad esempio, anche il popolare videogioco *Garena Free Fire*, sviluppato da *Sea Ltd* di Singapore): la motivazione è ancora legata a minacce alla sicurezza, confermando una persistente politica di contenimento³⁷.

Nel 2021 si realizza invece una svolta qualitativa nel ricorso alla sezione 69A, perché si passa dalle applicazioni riguardanti l'estero e potenziali minacce geopolitiche al contrasto di contenuti interni al dibattito politico e sociale. Durante le proteste contadine contro le leggi agricole, milioni di agricoltori si portano ai confini di Delhi, catturando l'attenzione internazionale. Le piattaforme digitali si stavano rivelando strumenti cruciali per l'organizzazione del dissenso e la diffusione di narrazioni alternative a quella dell'esecutivo ed è in questo contesto che il governo indiano emette l'ordine di oscurare 1.178 account Twitter e di deindicizzare specifici *hashtag*, come *#FarmersGenocide*, ritenuti incitamenti alla violenza o collegati a campagne di disinformazione "filo-pakistane". La vicenda porta a un conflitto aperto con Twitter e la piattaforma inizialmente riattiva diversi account oscurati, sostenendo che si trattava di giornalisti, attivisti o politici e che i contenuti non violavano le proprie *policy* interne. Dopo la minaccia del governo di sanzionare penalmente alcuni dirigenti della società fino a sette anni di reclusione, Twitter conforma parzialmente la propria condotta, bloccando oltre 500 account e limitando la visibilità di

³⁶ Sull'analisi del ban di *TikTok* e di altre applicazioni cinesi in India come espressione di *digital sovereignty* e nel più ampio quadro delle tensioni sino-indiane, si vedano A. Kumar, D. Thussu, *Media, digital sovereignty and geopolitics: the case of the TikTok ban in India*, in 45 *Media, Culture & Society* 8 (2023), che inquadrano la narrazione governativa e le implicazioni geopolitiche del divieto; e N.R. Sabitha, P.C. Mavroidis, *India and China: Brinkmanship in the Realm of Apps*, in 13 *Indian J. Int'l Econ. L.* 179 (2021), sul profilo delle implicazioni commerciali e delle eventuali dispute di diritto internazionale relative a misure di restrizione delle *app* nel contesto WTO/GATS.

³⁷ Per i comunicati ufficiali del *Ministry of Electronics and Information Technology*, relativi ai blocchi delle applicazioni di origine cinese, si vedano *Press Release MeitY*, 29 June 2020; 2 September 2020; 24 November 2020; 14 February 2022, tutti fondati sulla sezione 69A dell'IT Act e motivati con riferimento alla sovranità, all'integrità e alla sicurezza nazionale.

alcuni *hashtag*, ma senza eseguire integralmente gli ordini governativi. Questo episodio ha messo in luce la tensione tra la disciplina legale interna e le logiche delle piattaforme globali, sollevando interrogativi sulla libertà di espressione e sulla capacità dello Stato di disciplinare il dissenso politico attraverso strumenti pensati per la sicurezza nazionale³⁸.

Nel gennaio 2023 la BBC diffonde un documentario in due parti intitolato *India: The Modi Question*, dedicato al ruolo del premier indiano durante le violente rivolte del Gujarat del 2002 (di cui era all'epoca *Chief Minister*), quando morirono centinaia di musulmani. Il documentario contiene valutazioni critiche espresse dal governo britannico e per questo la sua diffusione in India è stata accolta dal governo con estrema ostilità³⁹: il 21 gennaio YouTube e Twitter ricevono l'ordine formale del MeitY, fondato sulla necessità di proteggere la sovranità e l'integrità dell'India, e rimuovono *link* e *clip*, impedendo così la diffusione di materiale considerato ostile alla "narrazione nazionale" e di propaganda coloniale⁴⁰. Nel generale disegno di contrasto agli oppositori della revoca dello *status* speciale del Jammu e Kashmir, avvenuta nel 2019 con l'abrogazione dell'art. 370 Cost., il successivo 19 agosto il governo federale indiano, sempre attraverso il MeitY, blocca senza alcun preavviso, né comunicazione ufficiale il sito web del portale di informazione indipendente *The Kashmir Walla*⁴¹, la cui redazione viene informata dell'ordine direttamente dal *provider*, subendo l'oscuramento di tutti i suoi account sui *social media*, e ricevendo contestualmente un avviso di sfratto, che determinò l'abbandono della propria sede. A dicembre 2023 il MeitY fornisce delle cifre che consentono una riflessione complessiva sul fenomeno: nel corso dell'anno erano stati, infatti, bloccati 7.502 tra account, siti web e URL, mentre, tra il 2018 e il 2023, forme di divieto avevano riguardato ben 36.800 URL, di cui oltre 13.600 erano account su X (ex Twitter).

Il culmine di questa traiettoria si è avuto nel 2025, quando la sezione 69A è stata al centro di una delle più controverse vicende di censura digitale della storia indiana. A inizio maggio, nell'ambito di un'operazione denominata "*Operation Sindoor*", il governo ordina a X di

³⁸ Diverse analisi accademiche hanno studiato come le piattaforme digitali siano state utilizzate: sul ruolo di Twitter nella mobilitazione della protesta, si veda S. Monteiro, *Farmer protests in India and the mobilization of the online diaspora on Twitter*, (19 May 2021), disponibile su <http://dx.doi.org/10.2139/ssrn.3849515>, in cui si analizza il flusso e la struttura dei *tweet*, comprese le dinamiche di viralità e diffusione internazionale. Un altro contributo, N. Kumari, P. Pradhan, *Public Deliberation on Twitter during Farmers' Protest*, in *Dialog*, 40 (Autumn 2022), esamina le deliberazioni politiche e pubbliche su Twitter, mostrando come la piattaforma abbia offerto uno spazio di discussione politica diretto tra cittadini e attivisti.

³⁹ Sulla vicenda, si veda R. Sarma, *On the Road to Censorship: BBC and Freedom of Expression in India*, in *VerfBlog* (2 Mar. 2023).

⁴⁰ In risposta, gruppi studenteschi organizzano proiezioni clandestine del documentario in vari atenei (Delhi, Hyderabad, Calcutta), che in alcuni casi comportano l'intervento della polizia per impedire le proiezioni, arrestare temporaneamente studenti e bloccare la distribuzione fisica del materiale.

⁴¹ Il fondatore e direttore del portale, Fahad Shah, era, peraltro, già detenuto dal febbraio 2022 per accuse in base al *Public Safety Act* (legge statale che consente la detenzione preventiva amministrativa) e all'*Unlawful Activities Prevention Act* (legge federale antiterrorismo).

bloccare oltre 8.000 account, accusati di diffondere disinformazione filo-pakistana in seguito a gravi fatti di violenza in Kashmir. La lista include non solo profili individuali (ad esempio quello del giornalista Anuradha Bhasin), ma anche testate giornalistiche indiane indipendenti (tra cui *Maktoob Media*, *The Kashmiriyat* e *The Wire*), e media stranieri (tra cui *Global Times*, *Xinhua* e *TRT World*): nei giorni successivi questi account risultano “withheld in India”. La nota di X sottolinea anche la mancanza, in molti casi, di indicazioni puntuali su quali contenuti avessero violato la legge, denunciando il carattere censorio del blocco a livello dell’intero account. Dalla tarda serata del 5 luglio la tensione si acuisce, perché i due account ufficiali di *Reuters* – quasi uno stress test per verificare il limite d’intervento – risultano inaccessibili e vengono ripristinati soltanto dopo proteste pubbliche. L’8 luglio X pubblica una nota ufficiale in cui afferma che il Ministero avrebbe impartito il 3 luglio un ordine di blocco immediato contro 2.355 account da eseguire entro un’ora, mentre la versione governativa è che si trattasse di una semplice applicazione ritardata di ordini già emessi a maggio. Gli ordini e i relativi atti sono rimasti secretati, in virtù della *Rule 16*, e non è stato possibile verificare la sussistenza delle diverse ragioni addotte.

La portata di questi episodi e l’intensificarsi del ricorso alla sezione 69A dimostrano come uno strumento nato per contrastare minacce esterne e per regolare la circolazione di *app* di provenienza straniera si sia progressivamente trasformato in un meccanismo di *governance* dello spazio informativo interno. Sotto il profilo teorico, vanno, infatti, evidenziate tre tensioni strutturali: la coesistenza tra un impianto procedurale “garantito” sulla carta e un elevato tasso di segretezza nella prassi (che rende arduo verificare il rispetto dell’*iter*); la tendenza delle autorità governative a fondare la richiesta di blocchi molto estesi su esigenze di sicurezza in tempo reale, ricorrendo a vaste misure “orizzontali” su interi account; la difficile condizione degli intermediari, stretti tra obblighi giuridici, rischi penali per i dipendenti e impegni (nazionali e globali) sulla libertà d’espressione. Le tensioni con le piattaforme digitali, la pressione sui loro rappresentanti e la segretezza procedurale alimentano, dunque, un dibattito va oltre la mera dimensione giuridica, toccando il cuore del rapporto tra sicurezza, libertà e sovranità digitale.

6. Le IT Rules 2021: una nuova disciplina per intermediari e piattaforme digitali

Nel febbraio 2021 il governo indiano ha emanato un ampio regolamento denominato *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* (IT Rules 2021), che ha determinato una svolta nella disciplina delle piattaforme digitali. Le nuove regole sono *secondary or subordinate legislation*, emanate ai sensi della sezione 87 dell’IT Act, e hanno sostituito le precedenti *Intermediary Guidelines Rules* del 2011. Formalmente il testo normativo è diviso in *Part I* (disposizioni generali e definizioni), *Part II* (*Intermediary Guidelines*) e *Part III* (*Digital Media Ethics Code*). Nel complesso, si pongono un duplice obiettivo: da una parte, ridefinire gli obblighi e le condizioni di *due diligence* che gli intermediari

online (*social network*, servizi di messaggistica, forum, etc.) devono rispettare per mantenere l'esenzione di responsabilità (*safe harbour*); dall'altra, creare, per la prima volta, un regime di regolamentazione per i cd. *Digital News*⁴², che in precedenza sfuggivano a un'autorità regolatoria specifica e, non essendoci licenze o registri come per i *media* tradizionali, operavano in un "vuoto" normativo. Oltre agli intermediari *online* e agli editori digitali, le piattaforme di *streaming* digitale cd. *Over-The-Top* (OTT) e contenuti audiovisivi curati (*Online Curated Content*) rappresentano il terzo settore interessato dalle regole del 2021: anche nel caso di servizi come Netflix, Amazon Prime Video, Disney+ etc., si tratta del primo intervento normativo, poiché in precedenza serie TV e film *online* non erano soggetti né alla censura cinematografica, né alle regole radiotelevisive.

Per quanto concerne la disciplina degli intermediari, essi sono tutti soggetti a un meccanismo di reclamo (*grievance redressal*), che individua tempistiche stringenti per intervenire su contenuti illeciti o lesivi, segnalati da utenti privati: se si tratta di nudi non consensuali o *revenge porn*, al fine di tutelare rapidamente la dignità e la *privacy* delle vittime, la piattaforma deve rimuoverli già entro 24 ore dalla ricezione del reclamo, mentre per altre categorie (odio religioso, terrorismo, diffamazione) il termine è più ampio, ma è comunque vincolato (generalmente 15 giorni) per fornire una decisione motivata. Le regole rafforzano l'obbligo di rimozione tempestiva di un contenuto anche nel caso di richiesta proveniente da un soggetto pubblico: se un Tribunale indiano o un'autorità governativa competente emette un ordine formale di rimozione di un post o di blocco di un account (ex sezione 69A), l'intermediario è tenuto a conformarsi e comunicare di aver ottemperato. Come abbiamo visto nel § 5, la sentenza *Shreya Singhal* della Corte Suprema aveva già chiarito che gli intermediari non sono tenuti a filtrare attivamente tutti i contenuti, cioè non hanno un dovere di monitoraggio proattivo generale, ma sono tenuti ad agire quando ricevono un ordine valido (quel momento rappresenta la *actual knowledge* della illegalità). In sostanza, il nuovo regime ha codificato questo principio: nessuna piattaforma può più rimanere inerte di fronte a un ordine legittimo, altrimenti sulla base della *Rule 7* la mancata aderenza alla *due diligence* fa decadere il *safe harbour* e l'intermediario diventa perseguibile come co-responsabile.

Le IT Rules 2021 hanno introdotto una serie di oneri operativi più stringenti per i grandi *social* con oltre 5 milioni di utenti (detti *Significant Social Media Intermediaries*, SSMI). In particolare, ogni SSMI deve indicare tre diverse figure: il *Chief Compliance Officer* (responsabile del rispetto delle regole), il *Nodal Contact Person* (referente per i rapporti con le forze dell'ordine e le autorità governative) e il *Grievance Officer* (responsabile per i reclami), che devono essere tutti residenti in India. All'approssimarsi della scadenza per conformarsi alle nuove regole, cioè tre mesi dalla pubblicazione (quindi entro il 25 maggio 2021), Twitter chiese maggiore tempo per la nomina dei responsabili locali richiesti ed esitava anche sull'applicazione di altre norme ritenute invasive: l'esecutivo ha, quindi,

⁴² Ricade sotto questa definizione praticamente qualsiasi soggetto che pubblica contenuti di *news* o attualità *online* (giornali *online*, portali di *news*, agenzie di stampa sul web, aggregatori di notizie digitali..).

minacciato esplicitamente la piattaforma di perdita del *safe harbour* e ha posto in essere atti quasi intimidatori⁴³. Successivamente Twitter ha formalmente ottemperato a tutti gli obblighi, nominando i referenti (prima in via provvisoria e poi in modo permanente) e adeguando alcune *policy* interne, ma ha contestualmente iniziato a resistere in via giudiziaria.

Nella primavera 2022, Twitter ha presentato un *writ petition* presso la *Karnataka High Court* contro 39 ordini di blocco emessi dal MeitY tra il 2021 e il 2022, che riteneva arbitrari. Tra questi ordini vi erano richieste di oscurare completamente account di giornalisti, attivisti e politici dell'opposizione, spesso senza fornire motivazioni sufficienti in termini di minaccia alla pubblica sicurezza. Con la sentenza *X Corp v. Union of India*, WP n. 13710/2022 Kar, pronunciata il 30 giugno 2022, la *High Court* stabilisce che gli ordini di blocco contestati erano conformi alla legge (la sezione 69A dell'IT Act consente, dunque, anche il blocco di interi account) e condanna Twitter a pagare una sanzione simbolica di 50 *lakh* di rupie per la mancata tempestività nell'ottemperare alcuni ordini. La decisione viene impugnata tramite *special leave petition* (SLP) e portata davanti alla Corte Suprema che con la sentenza *X Corp v. Union of India*, (2023) 10 SCC 545, pronunciata il 10 aprile 2023⁴⁴, respinge l'SLP e conferma il giudizio.

Nel 2025 X (ex Twitter) ha aperto un nuovo fronte della sua battaglia legale, depositando a marzo un altro ricorso presso la *Karnataka High Court* per far dichiarare illegittimo l'uso della sezione 79(3)(b), come fondamento per legittimare gli ordini di blocco⁴⁵. L'argomento giuridico consiste nel fatto che la sezione 79, essendo una disposizione di *safe harbour*, non conferisce un potere censorio al governo e non può essere trasformata dall'esecutivo in una sorta di "procedura parallela"⁴⁶, al fine di aggirare con questo stratagemma tutte le garanzie procedurali previste invece dalla sezione 69A. In sintesi, X accusa il governo di abusare della sezione 79 e violare la sentenza *Shreya Singhal* della Corte Suprema, nel tentativo di nascondere sotto la presunta necessità di tutelare interessi pubblici la reale volontà di sopprimere senza controlli il legittimo dissenso.

Le censure formulate da X non hanno, tuttavia, trovato accoglimento: con la sentenza *X Corp v. Union of India*, WP n. 7405/2025 (GM-RES), pronunciata il 24 settembre 2025, la *Karnataka High Court* ha

⁴³ Il 24 maggio 2021 un *team* speciale della *Delhi Police* si è, ad esempio, presentato negli uffici di Twitter a Delhi e Gurgaon formalmente per consegnare un avviso in merito all'indagine su un *tweet* di un portavoce del partito di governo (BJP) che Twitter aveva etichettato come "*manipulated media*". Questo episodio è stato considerato da molti osservatori come un atto intimidatorio nei confronti, dato il contesto di tensione tra l'esecutivo e la compagnia.

⁴⁴ X (ex Twitter) non ha annunciato formalmente di voler appellare questa decisione alla Corte Suprema: considerato che nel frattempo ha spostato l'attenzione sul nuovo contenzioso riguardante la sezione 79, è possibile che stia concentrando gli sforzi su quest'ultimo sperando in un precedente più favorevole.

⁴⁵ La Corte ha esaminato le argomentazioni di X e quelle del governo, oltre agli interventi di terzi come l'associazione di editori digitali DIGIPUB. Il 29 luglio 2025 la *Karnataka High Court* si è riservata la decisione, concludendo le udienze prima di emettere la sentenza definitiva.

⁴⁶ La procedura si svolge spesso attraverso la piattaforma *Sahyog*, lanciata nel 2024 proprio per permettere alla polizia locale e a strutture governative di emettere massivamente richieste di blocco.

respinto il ricorso, ritenendo che la sezione 79(3)(b) operi su un piano distinto rispetto alla procedura di blocco prevista dalla sezione 69A e che il suo utilizzo risulti compatibile con i principi affermati dalla Corte Suprema nel caso *Shreya Singhal*. Al tempo stesso la Corte ha statuito che X, in quanto società di diritto statunitense priva di sede legale in India, non sarebbe legittimata a invocare la tutela dell'art. 19 della Costituzione indiana e questa valutazione sembra porsi in contrasto con quanto già affermato dalla stessa *Karnataka High Court* nella citata sentenza WP n. 13710/2022 Kar, in cui il giudice Dixit aveva riconosciuto la legittimazione di X a stare in giudizio ai sensi dell'art. 14 della Costituzione. Il 14 novembre 2025 X ha depositato un *writ appeal* davanti alla *Division Bench* della stessa *Karnataka High Court*, contestando entrambe le statuizioni e chiedendo alla Corte collegiale di dirimere il contrasto interno⁴⁷. Il giudizio è ancora pendente.

Le IT Rules 2021 chiedono ai SSMI anche di utilizzare sistemi automatici, su base *best effort*, per identificare e rimuovere determinati contenuti illeciti: *in primis* materiali di abuso sessuale su minori, pornografia esplicita, oltre a elementi che istighino a reati gravi come stupro, terrorismo, etc. Tali strumenti di *content filtering* preventivo vanno bilanciati con il rischio di *over-censorship* (censura eccessiva di contenuti legittimi), ma indicano la tendenza normativa a coinvolgere attivamente le piattaforme nel “ripulire” lo spazio digitale. Inoltre, sussiste l'obbligo di pubblicare un rapporto mensile di trasparenza sui reclami ricevuti e le azioni intraprese mira a rendere più *accountable* le piattaforme.

Come si vedrà in dettaglio nel § 8, un'altra grande questione giuridica si è aperta con la *Rule 4.2*, che impone ai servizi di messaggistica *end-to-end encrypted* classificati come SSMI (WhatsApp è il caso emblematico) l'obbligo di essere in grado di risalire all'autore “iniziale” di un messaggio illecito, su richiesta di un ordine dell'autorità. Questa clausola di *traceability* ha sollevato immediatamente forti critiche in materia di *privacy* e della sicurezza informatica, in quanto implica di fatto l'indebolimento della crittografia *end-to-end* o la conservazione di dati addizionali sugli utenti. WhatsApp ha avviato un'azione legale presso la *Delhi High Court*, sostenendo che quest'obbligo di tracciabilità violi appunto il diritto fondamentale alla *privacy*⁴⁸ e non sia un mezzo proporzionato per

⁴⁷ Si vedano S.N. Thyagarajan, *X Corp. files appeal against Karnataka High Court verdict upholding Sahyog portal*, in *Bar and Bench* (15 Nov. 2025); Jurist staff, *India dispatch: social media platform X to challenge Karnataka High Court ruling over free speech concerns*, in *Jurist news* (6 Oct. 2025).

⁴⁸ Nella sentenza *Justice K.S. Puttaswamy*, approvata all'unanimità dalla Corte Suprema, viene stabilito che il diritto alla *privacy* è «*protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution*». Questa decisione ha ribaltato la precedente giurisprudenza degli anni '50 e '60, che negava la *privacy* come diritto fondamentale, e ha allineato l'India agli standard internazionali in tema di diritti della persona. Si vedano, *ex aliis*, T. Kaur, *Right To Privacy in Digital Age: A Study with Indian Context*, in *14 European Economic Letters* 4 (2024); M. Senor, *Il riconoscimento della tutela costituzionale del diritto alla privacy in India*, in *MediaLaws*, 1 (2018), che analizza anche i due precedenti capisaldi della Corte Suprema in materia di *privacy*, cioè *M.P. Sharma v. Satish Chandra, District Magistrate, Delhi*, AIR 1954 SC 300, pronunciata il 15 marzo

perseguire i responsabili di reati *online*, argomentando alla luce dei principi enunciati nella storica sentenza *Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors.*⁴⁹, (2017) 10 SCC 1, pronunciata il 24 agosto 2017. Dopo il deposito di questo ricorso nel 2021, Meta, proprietaria di WhatsApp, ne ha presentato uno parallelo in via precauzionale, ritenendo altrimenti di dover essere soggetta alla medesima regola per la messaggistica privata di Facebook Messenger. Essendoci state molteplici impugnazioni delle IT Rules 2021 presso diversi Tribunali, la Corte Suprema ha proceduto a un accorpamento e ha indicato la *Delhi High Court* per una trattazione coordinata: in attesa di una sentenza definitiva, restano valide le misure cautelari e *de facto* la clausola sulla tracciabilità al momento non viene applicata.

Il governo ha, dunque, imposto nuove responsabilità alle *Big Tech* e parallelamente ha esteso forme di controllo pubblico su quelle attività editoriali, che fino ad allora sfuggivano a qualsiasi autorità precisa, come le testate solo digitali e i produttori di serie in *streaming*. Il metodo del 2021 impone alle piattaforme di farsi parte diligente: non più *conduits* neutri, ma soggetti che vigilano sui propri servizi e collaborano strettamente con le autorità indiane. Il mancato adeguamento a queste *due diligence* comporta la perdita dell'esenzione di responsabilità e potenziali incriminazioni: la *Rule 7* specifica, infatti, che, in caso di inadempienza, oltre a decadere il *safe harbour*, l'intermediario può essere perseguito ai sensi di qualsiasi legge applicabile.

Il *Digital Media Ethics Code* (Part III delle IT Rules 2021) ha applicato per la prima volta uno schema di vigilanza ai *media* digitali: fino a quel momento, i siti giornalistici *online* e le piattaforme OTT non rientravano né sotto il *Press Council*, né sotto la *Central Board of Film Certification*, operando in una sorta di *far west* normativo. Le nuove regole li designano come «*publishers of news and current affairs content*» e «*publishers of online curated content*», sottoponendoli a un Codice etico mutuato dai codici esistenti per la stampa e la TV. In concreto, i notiziari digitali devono rispettare gli standard di deontologia (accuratezza, neutralità, rispetto delle

1954, e *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295, pronunciata il 18 dicembre 1962.

⁴⁹ In questa pronuncia, la Corte Suprema ha chiarito che, se il governo vuole imporre una misura che incide sul diritto alla *privacy* di un individuo, tale restrizione deve soddisfare tre condizioni fondamentali: *legality* (deve esistere una base legale chiara e valida che autorizzi la restrizione; *necessity & legitimate aim* (la restrizione deve perseguire un obiettivo legittimo dello Stato ed essere effettivamente necessaria per raggiungere tale scopo; *proportionality* (deve esserci una proporzione adeguata tra il beneficio pubblico perseguito e il danno inflitto alla *privacy*). Se la restrizione non soddisfa anche soltanto uno di questi criteri, allora viola il diritto fondamentale alla *privacy* ed è incostituzionale. Se esistono metodi meno invasivi per ottenere lo stesso risultato, lo Stato deve adottare quelli (principio del *minimal impairment*). Si vedano P. Panigrahi, E. Mehta, *The Impact of the Puttaswamy Judgement on Law Relating to Searches*, in 15 *NUJS L. Rev.* 1 (2022); V. Bhandari, A., Kak, S. Parsheera, F. Rahman, *An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict*, in *IndraStra Global*, 11 (2017); L. Pelucchini, *Diritto alla privacy, data protection e Costituzioni mute: la Corte Suprema indiana riconosce il diritto alla vita privata come inalienabile*, in *Nomos – Le attualità del diritto*, 2 (2017).

minoranze, etc.) già imposti ai giornali e alle emittenti dal *Press Council Act* e dal *Program Code televisivo*, e le piattaforme OTT devono classificare i contenuti per fasce d'età (U, 7+, 13+, 16+, A, etc.), prevedere sistemi di *parental control* e *age verification* per i contenuti per adulti e assicurare che niente di ciò che trasmettono violi leggi penali (es. oscenità, oltraggio alla religione, etc.).

Si istituisce un articolato meccanismo di reclamo su tre livelli (*three-tier grievance redressal mechanism*), rivolto specificamente ai contenuti digitali editoriali. Il primo *step* è quello dell'autoregolazione interna (*self-regulation by the publishers*): sia *news* che OTT devono predisporre un proprio *iter* interno analogo a quanto fanno i *social media* per gestire i reclami degli utenti sul contenuto (nomina di un *Grievance Officer*, decisioni entro 15 giorni sulle segnalazioni, etc.). C'è poi un'autoregolazione di secondo livello (*self-regulation by the self-regulating bodies of the publishers*): gli editori digitali devono aderire (singolarmente o in gruppi di settore) a uno o più organismi di autoregolazione, composti magari da ex giudici o esperti indipendenti, che svolgono funzione di appello in caso l'utente non sia soddisfatto della prima risposta al reclamo. Questi organismi devono essere registrati presso il *Ministry of Information and Broadcasting*; hanno il compito di esaminare i reclami non risolti al primo livello o eventuali violazioni sistemiche; sulla base della *Rule 12* possono «*warning, censuring, admonishing or reprimanding*» l'editore, chiedergli «*an apology [...] to include a warning card or a disclaimer; [...] reclassify ratings of relevant content; make appropriate modification in the content descriptor, age classification and access control measures; [...] edit synopsis of relevant content*» o segnalare un contenuto al Ministero per l'esame da parte dell'*Oversight mechanism* di cui alla *Rule 13* in relazione ai motivi dalla sezione 69A. L'*Oversight mechanism* rappresenta il terzo livello: il MIB ha istituito una Commissione interministeriale, l'*Inter-Departmental Committee (IDC)*, che sovrintende all'intero sistema. L'IDC può, in ultima istanza, esaminare reclami non risolti ai primi due livelli o affrontare questioni particolarmente sensibili; e ha il potere di convocare gli editori e le piattaforme e, se riscontra violazioni gravi del Codice etico o delle leggi, può raccomandare al Ministero provvedimenti vincolanti, come l'ordinanza di rimuovere o modificare un contenuto, di pubblicare una smentita o un'esplicita scusa, fino al blocco totale di un servizio nei casi estremi. In situazioni di emergenza (*Rule 16*), il Segretario del Ministero I&B può emanare ordini immediati di blocco di contenuti digitali (analogamente alla procedura di emergenza della sezione 69A), che poi devono essere confermati o revocati collegialmente dall'IDC entro breve tempo. Questo apparato di controllo sul digitale colma un vuoto, ma concentra notevoli poteri nel governo: di fatto, la stessa autorità esecutiva (Ministero) che per decenni ha gestito la TV (con una forma di controllo pubblico simile, prevista per le emittenti televisive dal *Cable TV Act*), ora si arroga la supervisione ultima anche su *news* e spettacoli in rete, ponendosi come arbitro della conformità etica dei contenuti *online*.

Prima dell'approvazione delle IT Rules 2021, avevano fatto molto discutere alcuni casi⁵⁰ legati a serie trasmesse su piattaforme OTT. Il primo

⁵⁰ R. Roy, *The 2021 Intermediary Guidelines and their impact on OTT Platforms*, CCG Blog, Centre for Constitutional Governance, NLU Delhi, 17 Feb. 2022,

risale al novembre 2020, quando Gaurav Tiwari, *leader* della sezione giovanile del *Bharatiya Janata Party* (BJP), aveva depositato una denuncia formale (*First Information Report*) alla polizia di Rewa (Madhya Pradesh) contro due dirigenti di *Netflix India*, contestando la scena del bacio fra una ragazza indù e un ragazzo musulmano di fronte a un tempio nella serie *A Suitable Boy*⁵¹. Con l'introduzione delle nuove regole, reclami di questo tipo sono assegnati a un ente di secondo livello (*self-regulatory body*), mentre in questa circostanza non risultano essere state comminate sanzioni, né rimosso alcun contenuto.

Nel gennaio 2021 si sono registrati due episodi analoghi. La messa in onda su *Amazon Prime Video* della serie *Tandav*⁵² (a sfondo politico-religioso) aveva, infatti, scatenato proteste di diversi gruppi e di politici nazionalisti indù, portando alla presentazione di FIR contro gli autori e *Amazon*, accusati di offesa religiosa. Di conseguenza, il MIB aveva convocato i rappresentanti di *Amazon Prime*, chiedendo loro spiegazioni, e il regista Ali Zafar aveva dovuto pubblicare un video di scuse e accettare di rimuovere o edulcorare le scene contestate. Questi interventi (scuse e tagli) hanno rappresentato una "correzione" extragiudiziale⁵³, avvenuta anche se i nuovi meccanismi non erano ancora entrati pienamente a regime. Nel medesimo periodo era stata avviata l'apertura di procedimenti giudiziari contro i produttori di *Mirzapur*, accusati di aver rappresentato in modo offensivo la città omonima e i suoi abitanti. La controversia⁵⁴, originata da una FIR e da una petizione presentate da residenti della città, ha portato la Corte Suprema a un'altra notifica ad *Amazon*.

Nell'ottobre 2022 le IT Rules hanno subito ulteriori modifiche per rafforzarne l'efficacia: è stato, infatti, emendato il quadro relativo agli intermediari per istituire i *Grievance Appellate Committees* (GAC), ossia i Comitati di appello di emanazione governativa per i reclami degli utenti dei *social*. Prima, se un utente denunciava un contenuto pubblicato su Facebook o Twitter e si vedeva, ad esempio, rifiutata la rimozione del post, l'unico rimedio era adire il Tribunale. Ora, invece, i cittadini hanno

disponibile su <https://ccgnludelh.wordpress.com/2022/02/17/guest-post-the-2021-intermediary-guidelines-and-their-impact-on-ott-platforms/>.

⁵¹ Sulla vicenda si vedano *A Suitable Boy row: Madhya Pradesh police books two Netflix officials*, 23 Nov. 2020, disponibile su <https://www.thehindu.com/entertainment/a-suitable-boy-row-madhya-pradesh-police-books-two-netflix-officials/article61726129.ece>; *FIR filed in MP for hurting religious sentiments over kissing scenes in Netflix's A Suitable Boy*, 23 Nov. 2020, disponibile su <https://scroll.in/latest/979238/>.

⁵² Sulla vicenda si veda *Explained: Amazon Prime's Web Series Tandav Faces Legal Trouble*, 19 Jan. 2021, disponibile su <https://www.boomlive.in/fact-file/tandav-amazon-prime-saif-ali-khan-police-complaint-fir-ib-ministry-11607>.

⁵³ Si veda <https://www.aljazeera.com/economy/2021/3/2/amazon-apologises-to-indian-viewers-over-tandav-controversy>.

⁵⁴ Sulla vicenda si vedano *SC sends notices to Amazon, Mirzapur makers for allegedly maligning Uttar Pradesh's image*, 21 Jan. 2021, disponibile su <https://scroll.in/latest/984693/sc-sends-notices-to-amazon-mirzapur-makers-for-allegedly-maligning-uttar-pradeshs-image>; *SC issues notice to makers of Mirzapur and Amazon Prime Video*, 21 Jan. 2021, disponibile su <https://www.tribuneindia.com/news/nation/sc-issues-notice-to-makers-of-mirzapur-and-amazon-prime-video-201662>.

un'alternativa alla via giudiziaria e possono presentare ricorso a uno dei tre GAC, ciascuno composto da un Presidente e due membri, nominati tra funzionari e dirigenti del settore (anche in pensione), sotto la supervisione di diversi Ministeri⁵⁵.

Il GAC esamina l'appello e può emettere una decisione vincolante per la piattaforma entro tempi rapidi, ordinando la rimozione di un contenuto precedentemente mantenuto *online* o viceversa il ripristino di un account ingiustamente sospeso. Dal primo trimestre 2023, i GAC hanno iniziato ad operare, emettendo da subito centinaia di ordini: segno che molti utenti, specie per *ban* di account, hanno colto questa nuova opportunità di riesame indipendente⁵⁶. Tuttavia, la creazione dei GAC è stata accolta con preoccupazione da attivisti e imprese *tech*: diversi *stakeholder* hanno, infatti, criticato il fatto che organismi esecutivi possano ribaltare decisioni private delle piattaforme, denunciando un ulteriore strumento per il governo di influenzare la moderazione dei contenuti *online*.

Il timore è che il governo, tramite la sua presenza nei GAC, possa “forzare la mano” alle piattaforme su questioni politicamente sensibili, ottenendo la rimozione di post scomodi con la giustificazione di un reclamo partito da un utente privato⁵⁷. Il MeitY ha naturalmente difeso i GAC, rivendicandone innanzitutto una utilità pratica, dato che nascono dall'esigenza di gestire migliaia di reclami inevasi o risolti male dalle *Big Tech*, e rilanciando la questione dell'urgenza di responsabilizzare queste aziende verso i consumatori indiani. Resta però inevaso il nodo dell'effettiva indipendenza dei GAC, composti quasi interamente da persone legate allo Stato, senza rappresentanza di giudici in attività o società civile, e senza la previsione di un meccanismo di appello ulteriore, sebbene le decisioni dei GAC possono essere impugnate in Tribunale mediante ricorsi ordinari.

Un secondo aggiornamento, nell'aprile 2023, ha riguardato la lotta alle *fake news*⁵⁸. È stata inserita una norma che impone agli intermediari di non ospitare o di rimuovere tempestivamente qualunque informazione ritenuta *fake* o *false* da un'apposita unità di *fact-checking* governativa (FCU)⁵⁹: se, dunque, il *Press Information Bureau* (PIB) o un altro organo

⁵⁵ Il GAC 1 è presieduto dal CEO dell'*Indian cyber-crime coordinate centre* (espressione del Ministero dell'Interno), il GAC 2 da un *Joint Secretary* (Ministero dell'Informazione e del *Broadcasting*) e il GAC 3 da uno *Scientist G*, rango *Joint Secretary* (MeitY).

⁵⁶ Si registrano molti ricorsi su WhatsApp per recuperare account bloccati e su Instagram per contenuti moderati automaticamente.

⁵⁷ Sul rischio che la composizione dei GAC possa compromettere l'effettiva indipendenza dell'organismo, si vedano T. Panjiar, P. Waghre, *A public brief on the IT Amendment Rules, 2022*, 10 Nov. 2022, disponibile su <https://internetfreedom.in/public-brief-on-the-it-amendment-rules-2022/>; *IT rules: Centre withdraws draft proposal to set up a new grievance panel*, 3 June 2022, disponibile su <https://scroll.in/latest/1025389/it-rules-centre-withdraws-draft-proposal-to-set-up-a-new-grievance-panel-say-reports>.

⁵⁸ Già il 20 gennaio 2023 il MeitY aveva pubblicato la proposta di emendamento alle IT Rules 2021 per creare un'unità di *fact-checking* governativa con il potere sia di dichiarare *fake*, *false* o *misleading* qualsiasi informazione pubblicata *online* relativa al governo centrale, sia poi di imporne la rimozione.

⁵⁹ Questa unità è generalmente nota come *PIB Fact Check Unit* o, più formalmente, *FCU (Fact-Checking Unit)* del governo centrale. PIB sta per *Press*

governativo accreditato etichetta un contenuto *online* come *fake news* riguardante attività del governo centrale, i *social network* dovranno eliminarlo, pena la possibile perdita dell'esenzione dalla responsabilità. Come intuibile, questa modifica ha suscitato fortissime proteste da parte di associazioni di giornalisti, *media* e società civile, oltre che dell'opposizione, che l'hanno definita "censura istituzionalizzata". La regola, di fatto, fa del governo l'arbitro unico della verità su qualunque notizia che lo coinvolga ed è plausibile che possano essere bollate come "false" anche notizie "vere ma scomode", riducendo i *media* al silenzio per evitare grane legali. Numerosi editori digitali (tra cui *The Wire* e *The News Minute*) hanno denunciato il soffocamento del giornalismo indipendente e la limitazione della libertà di stampa⁶⁰, oltre al rischio di creare potenzialmente un paradossale clima di autocensura generalizzata: un *chilling effect*⁶¹ per cui le piattaforme, pur di non rischiare la perdita del *safe harbour*, potrebbero rimuovere anche contenuti critici genuini, qualora la FCU li etichetta come falsi, soffocando così il dissenso *online*.

Sul piano giudiziario, la norma che istituisce la *Fact Check Unit* è stata subito impugnata da varie parti (giornalisti, la *Editors Guild*, etc.) e la *Bombay High Court* ha emesso una misura cautelare temporanea. Il 3 marzo 2024 il governo federale ha allora notificato la costituzione della FCU, forte del fatto che l'efficacia della norma non risultava sospesa: questa situazione ha spinto definitivamente la questione davanti alla Corte Suprema, che il successivo 21 marzo ha esaminato un ricorso urgente, sospendendo l'attuazione della notifica di istituzione della FCU e ritenendo la questione fondata e meritevole di approfondimento. Quindi, di fatto, la FCU è stata bloccata dalla Corte Suprema poco dopo essere stata resa operativa.

A settembre 2024, la *Bombay High Court* si è poi espressa sul merito, dichiarando la norma sulla FCU lesiva della libertà di espressione. Il governo ha, dunque, presentato appello (*special leave petition*), depositato il 24 dicembre, ma per mancata sanatoria di vizi procedurali l'SLP è stata considerata archiviata nel luglio 2025. Il successivo 4 dicembre l'esecutivo ha chiesto il ripristino del ricorso, sostenendo che i ritardi fossero involontari e, trattandosi di archiviazione per ragioni puramente procedurali, la Corte Suprema ha accolto la richiesta il 16 febbraio 2026, con prima trattazione avvenuta il 10 marzo. In quella sede la Corte Suprema ha rifiutato di sospendere la decisione della *Bombay High Court*: allo stato attuale, pertanto, la FCU non è operativa e il governo federale non può ricorrere a questo strumento.

Più in generale, le impugnazioni delle IT Rules 2021 sono state molteplici e in certi casi anche assai tempestive, come nel caso del portale

Information Bureau, che è l'ufficio stampa ufficiale del governo indiano all'interno del quale è incardinata.

⁶⁰ Il governo ha replicato che l'obbligo è circoscritto alle sole piattaforme (non impone direttamente ai giornali di rimuovere articoli) e serve a porre un argine alla disinformazione dilagante.

⁶¹ Sul rischio di *chilling effect* generato dalle IT Rules 2021 e dalle successive modifiche, si veda M. Sharma, K. Pendyal, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 – Protection from Malicious Content or Chilling Free Speech*, 4 Feb. 2022, disponibile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3967857.

giuridico *LiveLaw*, che ha ottenuto già nel 2021 un'ingiunzione dalla *Kerala High Court*, che impediva al governo di intraprendere azioni coercitive contro di loro per il mancato rispetto delle regole, riconoscendo la serietà delle questioni costituzionali sollevate. Nella stessa direzione, la *Bombay High Court*, adita da *The Leaflet* e altri, aveva sospeso due disposizioni chiave (*Rules 9.1 e 9.3*), che obbligavano i *publisher* a conformarsi al Codice etico e a «*good taste and decency*», termini decisamente ampi e vaghi, che rischiano di conferire un controllo eccessivo allo Stato sul contenuto dei *media*⁶².

Questo vero e proprio “campo minato” di impugnazioni e misure sospensive ha spinto il governo federale indiano già a luglio del 2021 ad avanzare alla Corte Suprema una *transfer petition* per ottenere un esame congiunto delle questioni. L'ordinanza del 9 maggio 2022 ha così sospeso lo svolgimento dei procedimenti pendenti davanti alle varie *High Courts*, stabilendo però che dovessero restare in piedi gli *interim orders*, emessi in via cautelare. Al fine di evitare giudizi contrastanti, quasi due anni dopo, con la decisione del 22 marzo 2024 la Corte Suprema ha disposto di accentrare tutti i ricorsi pendenti in materia presso un unico giudice, la *Delhi High Court*, che il successivo 14 agosto ha organizzato i casi per categorie tematiche e a novembre 2024 ha avviato le udienze nel merito. Allo stato attuale, dunque, alcune disposizioni (specie sul contenuto di *news*) risultano ancora “congelate” per via giudiziaria e l'esito del giudizio sarà cruciale anche per capire il confine tra la legittima tutela dell'informazione corretta e il rischio di abuso da parte del potere esecutivo nell'etichettare come “*fake*” notizie sgradite.

In conclusione, le IT Rules 2021 hanno imposto una assunzione di responsabilità senza precedenti da parte delle piattaforme digitali: rimozione più rapida dei contenuti illeciti, meccanismi di reclamo e appello, possibilità di intervento diretto del governo in caso di inerzia. La nuova cornice giuridica ha portato però a un quadro ibrido: da un lato, maggiore tutela per utenti e società; dall'altro forti preoccupazioni per la libertà di espressione e l'indipendenza dei *media online*, dati i poteri penetranti che l'esecutivo si è riservato. Il ruolo dei Tribunali è stato finora decisivo per mettere alcuni paletti, ma spetterà alla Corte Suprema definire principi di equilibrio, in attesa di interventi legislativi, che potrebbero sostituire queste regole con una legge più organica. Nel frattempo, l'India sta cercando un delicato punto di incontro tra libertà digitale e responsabilizzazione delle piattaforme, in un contesto politico vivace, dove la comunicazione *online* ha un impatto determinante sul discorso pubblico.

7. La disciplina speciale per le campagne elettorali: dal fenomeno dei *deepfake* al ruolo degli *influencer*

⁶² Queste ordinanze hanno subito ritardato l'applicazione piena del Codice etico ai *news publisher* in attesa del giudizio finale, sebbene il MIB abbia cercato di dare seguito “normalmente” al nuovo quadro normativo, inviando, ad esempio, due richieste di informazioni (26 maggio e 9 settembre 2021) in base alla *Rule 18*, ricevendo migliaia di risposte, ma anche rifiuti e resistenze da parte di chi aveva ottenuto misure cautelari.

In India i contenuti sulle piattaforme digitali sono, dunque, soggetti all'IT Act, alle IT Rules 2021 e alle altre leggi generali applicabili, ma durante le campagne elettorali si attiva un quadro giuridico speciale, ideato per garantire al massimo la correttezza della competizione: si tratta del *Model Code of Conduct* (MCC), elaborato dalla *Election Commission of India* (ECI), che stabilisce regole di comportamento per partiti e candidati dal momento dell'annuncio delle elezioni fino alla conclusione del voto.

Il soggetto chiave è, dunque, l'ECI, organismo indipendente previsto dall'art. 324 Cost. con il compito di sovrintendere, dirigere e controllare lo svolgimento di tutte le elezioni federali e statali. In virtù di tale mandato, l'ECI svolge la funzione di garante della parità di condizioni tra i *competitors* e può emanare direttive vincolanti per assicurare lo svolgimento di elezioni libere ed eque. Sebbene il MCC non sia una legge in senso formale, i partiti vi aderiscono su base volontaria e l'ECI vigila sulla sua attuazione. Nel 2013 l'ECI ha esplicitato che le disposizioni del MCC (e le istruzioni connesse) si applicano anche ai contenuti pubblicati su Internet, inclusi chiaramente anche i *social media* utilizzati dalle forze politiche o dai singoli candidati: ciò che non è consentito nei comizi o sulla stampa durante la campagna elettorale non è, quindi, più consentito neanche *online*.

L'ECI dispone di ampi poteri sanzionatori: può, ad esempio, censurare pubblicamente un candidato, disporre divieti temporanei di fare campagna per chi viola ripetutamente il codice o raccomandare provvedimenti alle autorità competenti. L'art. 324 Cost. è stato, peraltro, interpretato in senso estensivo dalla giurisprudenza conferendo all'ECI margine di intervento anche in assenza di uno specifico fondamento normativo, purché la misura sia finalizzata a tutelare la correttezza del processo elettorale⁶³. Nel contesto digitale, l'ECI ha creato unità di monitoraggio dei *social media* (*Social media monitoring cells*) a livello distrettuale, statale e federale, incaricate di segnalare le violazioni *online* del MCC, controllare la pubblicità digitale e collaborare con le piattaforme per la rimozione dei contenuti illeciti. Tali unità, supportate da strumenti di intelligenza artificiale, rappresentano ormai un'estensione difficilmente sostituibile dell'apparato di *enforcement* elettorale.

Le grandi piattaforme *social* svolgono un ruolo cruciale e controverso nella gestione della disinformazione durante le elezioni e, su pressione delle autorità, hanno dovuto innanzitutto prevedere delle misure di automitigazione. Facebook ha avviato già dal 2018 *partnership* con *fact-checker* indipendenti per individuare e segnalare le notizie false, che vengono adesso etichettate come "informazione falsa" e la loro diffusione viene penalizzata dall'algoritmo, affinché raggiungano meno utenti. YouTube ha dichiarato di rimuovere quei contenuti che violano esplicitamente le sue *policy*, come i video che sostengono falsità sul processo

⁶³ Si tratta di un principio affermato in vari casi, a partire dalla sentenza *Mohinder Singh Gill v. Chief Election Commissioner*, (1978) 1 SCC 405, pronunciata il 2 dicembre 1977. La Corte Suprema ha fornito un'interpretazione estensiva dell'art. 324 Cost., affermando la norma opera anche «*in areas left unoccupied by legislation*», consentendo all'ECI di agire mediante direttive e istruzioni vincolanti anche senza una puntuale disposizione, purché tali interventi non siano in contrasto con norme di legge vigenti e siano funzionali alla tutela dell'integrità del processo elettorale.

elettorale oppure quelli che incitano alla violenza, arrivando a chiudere vari canali che diffondevano *fake news* politiche sotto falso nome. WhatsApp, essendo una piattaforma di messaggistica privata, ha privilegiato invece modifiche tecniche per ridurre la viralità dei messaggi e contrassegnare con un'etichetta speciale i messaggi inoltrati molte volte, oltre ad aver sviluppato filtri anti-*spam* per bloccare *bot* e account automatizzati, che tentano di inondare utenti con propaganda massiva⁶⁴.

Al di là delle iniziative private, nel 2019, in vista delle elezioni generali⁶⁵, la Commissione elettorale ha promosso un accordo, noto come *Voluntary Code of Ethics*, sottoscritto dalle principali piattaforme (Facebook, WhatsApp, ex Twitter, Google), che si sono impegnate a creare canali di comunicazione prioritari con l'ECI e a intervenire tempestivamente dietro sua segnalazione⁶⁶. Questa cooperazione negoziata tra Commissione elettorale e grandi compagnie di *social media* rappresenta una peculiarità del modello indiano, che ha prodotto risultati importanti nel contrasto della circolazione di notizie false e di contenuti manipolati, intensificatasi proprio in occasione di quella campagna elettorale: ad esempio, erano proliferate su Facebook pagine e post con affermazioni non verificate o teorie del complotto che attaccavano candidati rivali⁶⁷, mentre su WhatsApp dilagavano catene di messaggi, che spaziavano dalle voci infondate sulle alleanze politiche ai contenuti di stampo religioso finalizzati a polarizzare l'elettorato. L'etica volontaria delle piattaforme ha permesso di velocizzare la gestione dei contenuti problematici: i *Social media nodal officers*, nominati dall'ECI, e le *task force* dedicate delle piattaforme hanno rimosso in tempi rapidi moltissimi post e inserzioni segnalati come illeciti.

Alle successive elezioni del 2024 l'intelligenza artificiale è definitivamente esplosa e per la prima volta abbiamo assistito a un suo utilizzo su larga scala: dall'irruzione del fenomeno del *deepfake*⁶⁸ alla

⁶⁴ Per le misure adottate dalle singole piattaforme si vedano: Meta, *Our approach to misinformation*, Meta Transparency Center, disponibile su <https://transparency.meta.com/features/approach-to-misinformation/>; YouTube, *Elections misinformation policies*, YouTube Help, disponibile su <https://support.google.com/youtube/answer/10835034?hl=en>; WhatsApp, specificamente sull'India, *Ensuring User Safety in India on WhatsApp*, WhatsApp Help Center, disponibile su <https://faq.whatsapp.com/650453616475879/>.

⁶⁵ Per una lettura di quella consultazione, si veda C. Petteruti, *Elezioni indiane 2019: la forma di governo parlamentare alla prova del fenomeno Modi*, in *DPCE Online*, 4 (2019), mentre per la tornata precedente T. Amico di Meane, *La forma di governo dell'India alla luce delle elezioni politiche del 2014: profili costituzionali*, in *DPCE*, 2 (2015).

⁶⁶ In particolare, le piattaforme digitali hanno concordato di processare entro 3 ore eventuali segnalazioni di violazione dell'art. 126 R.P. Act del 1951.

⁶⁷ In quella circostanza Facebook ha rimosso reti coordinate di account falsi (spesso gestiti da *troll farm* di partito), chiudendo pagine legate a gruppi di propaganda, che avevano milioni di *followers*, e segnando una vittoria nella lotta alla disinformazione organizzata.

⁶⁸ Si vedano A. Birrer, N. Just, *What we know and don't know about deepfakes: An investigation into the state of the research and regulatory landscape*, in 27 *New Media & Society* 12 (2024); M. Groh, A. Sankaranarayanan, N. Singh, D. Young Kim, A. Lippman, R. Picard, *Human detection of political speech deepfakes across transcripts, audio, and video*, in 15 *Nature Communications* 1 (2024); M. Hameleers, T. van der Meer, T. Dobbler, *Distorting the truth versus blatant lies: The effects of different degrees of deception*

realizzazione di contenuti leciti, come gli *avatar* digitali per personalizzare la comunicazione politica. Già ad aprile c'era stato l'“antipasto” della campagna elettorale con la circolazione *online* di falsi “video d'epoca” in cui celebri attori di *Bollywood* criticavano il Primo Ministro Modi e invitavano a votare per l'opposizione: i contenuti erano interamente artefatti, ma hanno raggiunto milioni di persone prima di essere smentiti e rimossi. Specularmente, una clip audio divenuta virale aveva cercato di riprodurre la voce del *leader* dell'opposizione Rahul Gandhi, che annunciava le proprie dimissioni dal partito: anche qui si trattava di una notizia totalmente falsa, creata clonando artificialmente la sua voce. Questi due esempi dimostrano come la disinformazione elettorale in India abbia abbracciato tecniche sempre più sofisticate, rendendo ancor più difficile per gli elettori distinguere realtà e finzione.

Su impulso di un'ordinanza della *Delhi High Court*⁶⁹, l'ECI ha emanato una direttiva⁷⁰ per affrontare in dettaglio questi aspetti e ingiungere ai partiti (nazionali e statali) di non utilizzare video *deepfake* o altri materiali distorti digitalmente che possano diffondere disinformazione, alterare fatti o, comunque, fuorviare gli elettori. Queste nuove linee guida, associate al MCC, esplicitano diversi divieti, responsabilizzando le forze politiche a non «publishing or circulating deep audio/video or any misinformation which is manifestly false or misleading in nature» sui propri canali, che, in caso contrario, devono essere rimossi entro massimo 3 ore, identificando e sanzionando il responsabile. Nello specifico, non si possono poi pubblicare contenuti manipolati che impersonino l'identità di qualcun altro, accuse non verificate o basate su distorsioni, specialmente riguardo alla vita privata degli avversari, né contenuti denigratori verso gruppi

in domestic and foreign political deepfakes, in *Computers in Human Behavior*, 152 (2024); S. Qian, C. Shen, J. Zhang, *Fighting cheapfakes: Using a digital media literacy intervention to motivate reverse search of out-of-context visual misinformation*, in 28 *Journal of Computer-Mediated Communication* 1 (2023); M. Pawelec, *Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions*, in 1 *Digital Society* 19 (2022); T. Dobber, N. Metoui, D. Trilling, N. Helberger, C.H. de Vreese, *Do (microtargeted) deepfakes have real effects on political attitudes?*, in 26 *International Journal of Press/Politics* 1 (2020); C. Vaccari, A. Chadwick, *Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News*, in 6 *Social Media + Society* 1 (2020).

⁶⁹ Più precisamente, il 2 maggio 2024 la *Delhi High Court*, investita di una *public interest litigation* (PIL), promossa dall'associazione di avvocati *Lawyers Voice*, ha affrontato la questione dei *deepfake* in campagna elettorale. I giudici hanno dichiarato di non poter emanare loro stessi una *policy* a urne aperte, invitando l'ECI ad agire con urgenza. In questa circostanza, i legali dell'ECI hanno informato la Corte di aver già fatto rimuovere alcuni video *deepfake* (tra cui quelli citati nel testo) e di aver sporto denunce penali in merito ad essi. La *Delhi High Court* ne ha preso atto e ha disposto che l'ECI si occupasse di emanare linee guida anti-*deepfake* entro il 6 maggio, considerato che le elezioni erano già in corso.

⁷⁰ Il documento ufficiale è identificato come ECI/PN/72/2024 del 6 maggio 2024, con titolo «*ECI directs responsible and ethical use of social media platforms by political parties and their representatives*». L'ECI utilizza il termine “*directions*” per qualificare il provvedimento: giuridicamente possiamo considerarlo una direttiva vincolante, che rientra tra le prerogative riconosciute all'ECI dall'art. 324 Cost.

protetti⁷¹. La rilevazione e gestione dei *deepfake* resta complicata anche con l'obbligo di etichettatura imposto dall'ECI, perché manca un sistema automatizzato di verifica e non esistono sanzioni sempre chiare per chi diffonde contenuti non etichettati, generati o manipolati artificialmente⁷².

La direttiva sollecita un ruolo più incisivo dei partiti, i quali, invitati a segnalare prontamente alle piattaforme eventuali account falsi o contenuti illegali, che imitano i loro canali ufficiali, in caso di mancato intervento della piattaforma, possono rivolgersi al GAC per ottenerne la rimozione. L'integrazione del MCC con linee guida specifiche per il contesto digitale testimonia la consapevolezza da parte dell'ECI del rilievo assunto da questi strumenti come fortissimi rischi per il corretto svolgimento della competizione elettorale.

Per far rispettare concretamente le regole, oltre ai suoi poteri sanzionatori, l'ECI può naturalmente appellarsi alle leggi esistenti: nella direttiva del 2024 citava, tra gli altri, l'art. 171G del Codice penale⁷³, che sanziona le dichiarazioni false sui candidati fatte per influenzare il risultato elettorale, e la sezione 123(4) del *Representation of the People Act, 1951* (RPA), che configura come *corrupt practice* la diffusione di fatti falsi su un candidato da parte di un avversario⁷⁴. Un partito o un candidato sorpreso a diffondere *fake news* o *deepfake* diffamatori potrebbe teoricamente essere perseguito secondo queste norme⁷⁵, su impulso della Commissione. Nella prassi, considerati i tempi ristretti delle campagne, l'ECI predilige però soluzioni rapide extra-giudiziarie – come l'ordine di cessazione di una condotta, il ritiro di un post o le scuse pubbliche – piuttosto che estenuanti cause giudiziarie.

Pur non eliminando la disinformazione, le varie restrizioni hanno ridotto il raggio di diffusione di certi contenuti "tossici", favorendo

⁷¹ L'ECI ha menzionato esplicitamente l'obbligo di «*refrain from posting derogatory content towards women*» e di «*abstain from using children in campaigns*».

⁷² Il governo indiano potrebbe valutare di investire in strumenti di autenticazione dei media (ad esempio filigrane digitali per i video ufficiali) o in collaborazioni internazionali per sviluppare *software* di rilevamento AI avanzati. Sul fronte penalistico, alcuni chiedono poi di dare un segnale deterrente con un'applicazione più rigorosa delle leggi già esistenti (ad esempio, perseguendo chi crea *deepfake* calunniosi tramite l'art. 469 IPC, che punisce la falsificazione a scopo diffamatorio).

⁷³ Testualmente l'articolo dispone: «*whoever with intent to affect the result of an election makes or publishes any statement purporting to be a statement of fact which is false and which he either knows or believes to be false or does not believe to be true, in relation to the personal character or conduct of any candidate, shall be punished with fine*». A differenza della sezione 123(4) del RPA, si applica a chiunque (non solo candidati/agenti) realizzi la condotta e la pena prevista è una multa.

⁷⁴ Più precisamente, la fattispecie riguarda «*the publication by a candidate or his agent or any other person (with the consent of the candidate or his agent) of any statement of fact which is false, and which he either believes to be false or does not believe to be true, in relation to the personal character or conduct of any candidate, made for the purpose of influencing the election result of that candidate*».

⁷⁵ Se un candidato (o appunto qualcuno che agiva per suo conto e con il suo consenso) viene riconosciuto colpevole di tale pratica in una *election petition* post-elettorale, la sua elezione può essere invalidata e può essere dichiarato ineleggibile per un periodo di tempo. Si sottolinea che la fattispecie richiede la consapevolezza della falsità (cioè l'elemento del dolo).

l'emersione di eventuali smentite. Inoltre, vi sono iniziative *bottom-up* della società civile, che generano un contributo positivo: nelle consultazioni più recenti varie organizzazioni di *fact-checking* indipendente hanno smontato centinaia di bugie elettorali, pubblicando analisi, che ne hanno mitigato l'impatto e che talvolta sono state rilanciate dai *media mainstream*⁷⁶.

Nonostante tutto, molti osservatori evidenziano che le contromisure delle piattaforme restano ancora insufficienti rispetto alla vastità del fenomeno. La moderazione dei contenuti in India incontra, infatti, ostacoli specifici: la diversità linguistica (le "bufale" circolano in decine di lingue locali, rendendo arduo il monitoraggio algoritmico), la cifratura *end-to-end* di WhatsApp (trattata nel § 8) e, in certi casi, anche conflitti di interessi, perché le piattaforme monetizzano l'*engagement* e non hanno reali incentivi a rallentare la diffusione di contenuti virali, anche se polarizzanti.

Un ulteriore aspetto assai problematico, emerso con prepotenza durante le ultime campagne elettorali, è il ricorso ai *social media influencer* come vettori di messaggi politici⁷⁷: figure popolari del web, come *youtuber*, creatori di *meme*, star di Instagram, vengono ingaggiate (ufficialmente o dietro le quinte) dai partiti con sempre maggiore frequenza per orientare gli elettori in modo non convenzionale⁷⁸. Invece di pubblicare un manifesto politico palese, questi *influencer* inseriscono nei loro contenuti abituali su libri e musica dei messaggi oppure delle allusioni favorevoli a un partito: in questo modo il messaggio politico risulta confezionato come racconto di vita vissuta per risultare più autentico agli occhi del pubblico e mascherare la sponsorizzazione dietro un'apparente spontaneità, che trae in inganno gli spettatori più ingenui. Un esempio emblematico di questo fenomeno sono state le ultime elezioni statali nel *Rajasthan*, quando diversi *influencer* regionali hanno realizzato brevi video su Instagram mostrando gli aspetti positivi di un programma governativo e lodando implicitamente la forza politica che lo aveva introdotto⁷⁹.

⁷⁶ Per una ricostruzione dell'attività di *fact-checking* durante le elezioni generali indiane del 2024, si vedano gli archivi elettorali di *Alt News*, *BoomLive* e *India Today Fact Check*, che hanno documentato e smentito numerosi contenuti falsi o manipolati diffusi durante la campagna elettorale.

⁷⁷ Sull'ipotesi di condizionamento elettorale da parte degli *influencer*, si veda, *ex aliis*, H. Klüver, *Social Influencers and Election Outcomes*, in 58 *Comparative Political Studies* 13 (2024), che ha verificato empiricamente l'effetto di un video pubblicato dall'*influencer* di YouTube Rezo sull'esito delle elezioni per il Parlamento europeo del 2019, confrontando la differenza percentuale dei voti ottenuti dalla CDU/CSU per corrispondenza, solitamente espressi diversi giorni prima delle elezioni e quelli espressi di persona (gruppo di trattamento), perché solo questi ultimi sono stati esposti al video (la CDU/CSU, principale bersaglio del video di Rezo, ha subito perdite elettorali quasi del 5%).

⁷⁸ Sul caso indiano, si vedano S. Dash, D. Mishra, G. Shekhawat, J. Pal, *Divided We Rule: Influencer Polarization on Twitter during Political Crises in India*, in 16 *Proceedings of the International AAAI Conference on Web and Social Media* 1 (2022); P. Sharma, V. Jain, *Influencers and the Building of Political Brands – The Case of India*, in M. Moufahim (ed.), *Political Branding in Turbulent times*, London, 2022.

⁷⁹ Il governo statale del *Rajasthan*, all'epoca guidato dall'*Indian National Congress* con il *Chief Minister* Ashok Gehlot, aveva lanciato un'ambiziosa strategia di comunicazione, coinvolgendo attivamente i *social media influencer* per promuovere i propri programmi di *welfare* in vista del voto del novembre 2023. Già a giugno, il

I partiti hanno fatto ampio ricorso a queste strategie⁸⁰, con campagne di *influencer marketing* politico mirate ai giovani e alle aree rurali: ci sono ormai agenzie di comunicazione specializzate, che offrono ai politici pacchetti di post a pagamento su profili di *creator* digitali con elevato seguito. Il vantaggio per le forze politiche è duplice: da un lato raggiungono milioni di utenti *online* (l'India conta oltre 620 milioni di persone connesse); dall'altro sfuggono ai tradizionali controlli della stampa e dell'ECI. Infatti, le interviste "amichevoli" condotte dagli *youtuber* evitano ai candidati domande scomode e, da un punto di vista giuridico, le leggi elettorali non prevedono obblighi di dichiarazione per un post o un video di un *influencer*⁸¹, a differenza degli spot ufficiali. Attualmente, la normativa indiana non ha ancora strumenti efficaci per tracciare e disciplinare questo fenomeno, che rappresenta una "zona grigia"⁸² della propaganda *online*, ma un primo passo decisivo potrebbe essere già l'imposizione dell'obbligo di

governo aveva annunciato l'acquisto di spazi pubblicitari presso *influencer* su piattaforme come Facebook, Twitter, Instagram e YouTube, fissando i loro compensi mensili in base ai *followers* con lo scopo dichiarato di rendere rapidamente accessibili al pubblico le iniziative di *welfare* del governo statale. A luglio il governo del Rajasthan aveva poi avviato un vero e proprio *video contest*, invitando i cittadini a pubblicare video creativi in cui raccontavano come avevano beneficiato dei programmi pubblici statali, caricandoli con l'*hashtag* ufficiale per concorrere ai premi giornalieri in denaro. Il risultato è stato virale: in poche settimane più di 26.000 video sono stati caricati su Facebook/Instagram, in cui "comuni cittadini" (di fatto spesso *micro-influencer* locali, insegnanti, studenti, persino qualche sostenitore avversario attratto dai premi!) elogiavano gli schemi di *welfare* statale.

⁸⁰ A titolo di esempio, si può menzionare la giovanissima *influencer* Chandni Bhagat (con oltre 200.000 *followers*), che, dopo aver incontrato funzionari del *Bharatiya Janata Party* (BJP), ha iniziato a pubblicare post a favore di quel partito, tra cui uno virale su dei programmi regionali per la salute delle donne. Analogamente, sia l'INC, sia l'*Aam Aadmi Party* hanno cercato di collaborare con *influencer* locali in Stati come Punjab e Telangana. Nel caso citato sopra del Rajasthan, il BJP aveva, comunque, tentato di rispondere con *micro-influencer* per promuoverlo in modo "organico" l'operato del governo centrale.

⁸¹ La questione è evidente: contenuti apparentemente genuini possono, in realtà, rappresentare pubblicità occulta, finanziata con fondi elettorali e sottratta a ogni rendicontazione, con la possibilità concreta di eludere i limiti di spesa. A monte, resta aperto il problema della prova del compenso, essendo talvolta difficile dimostrare il nesso economico tra *creator* e candidato o partito.

⁸² Sul versante dell'autoregolamentazione pubblicitaria, è rilevante il ruolo dell'*Advertising Standards Council of India* (ASCI), organismo di *self-regulation* del settore pubblicitario, che nel 2021 ha adottato le *Guidelines for Influencer Advertising in Digital Media* (aggiornate nel 2022). Queste linee guida impongono agli *influencer* l'obbligo di rendere chiaramente riconoscibile qualsiasi contenuto promozionale, mediante etichette visibili (come #ad, #sponsored), al fine di evitare forme di pubblicità occulta e pratiche ingannevoli. In linea di principio, le regole ASCI si applicherebbero anche ai contenuti di natura politica o istituzionale, laddove vi sia un rapporto economico o una forma di "*material connection*" tra il *creator* e il soggetto promosso. Tuttavia, trattandosi di uno strumento di autoregolamentazione privo di poteri sanzionatori pubblici e non coordinato con la disciplina elettorale, le linee guida ASCI non risolvono il problema specifico della propaganda politica mascherata durante le campagne elettorali, lasciando aperta una significativa zona grigia tra comunicazione commerciale, *endorsement* personale e messaggio politico.

dichiarare e taggare come “messaggio politico pagato” qualsiasi contenuto *online* per il quale sia stato versato un compenso da parte di un partito o di un candidato, includendo, quindi, anche i post degli *influencer*.

L'India sta continuando ad aggiornare, in modo progressivo, i propri strumenti di regolazione delle campagne digitali in risposta alle nuove tecnologie. Un primo passaggio chiave è stato la Comunicazione dell'ECI 491/Social media-SOP/2025 del 16 gennaio, che richiama i partiti all'uso responsabile dei *social media* e, soprattutto, introduce esplicitamente la richiesta di *disclosure*: quando un contenuto elettorale è generato o alterato tramite AI, deve essere chiaramente etichettato come tale, per evitare che audio, video o immagini manipolati inducano in errore l'elettorato. Questa indicazione è stata successivamente attuata sul piano operativo, nel contesto delle elezioni statali in Bihar di ottobre, attraverso istruzioni applicative e richiami amministrativi, che hanno ribadito l'obbligo di segnalazione di questo genere di contenuti e il dovere di rimozione tempestiva, inquadrati come presidio di integrità elettorale.

Più in generale, il dibattito su una possibile normativa più incisiva prosegue e ci sono proposte per aggiornare la normativa elettorale, al fine di affrontare in modo più strutturale temi emersi, come la pubblicità politica sui *social* e la disinformazione *online*. Finora, tuttavia, l'approccio indiano è stato quello di evitare leggi draconiane, in favore di una combinazione di Codici di condotta, provvedimenti dell'ECI e cooperazione con le *big tech*, mantenendo un equilibrio tra innovazione digitale e integrità elettorale. La Commissione rappresenta il fulcro istituzionale di questo assetto, opera come “guardiano” del corretto uso dei *media* digitali in periodo elettorale e adatta le sue azioni all'evoluzione del panorama mediatico per continuare a esercitare il proprio *soft power*, avvalendosi delle prerogative costituzionali e della cooperazione (volontaria ma sostanziale) delle piattaforme. L'autorevolezza dell'ECI è, infatti, un efficace mezzo di pressione: un richiamo pubblico della Commissione per violazione del MCC danneggia pesantemente la reputazione di un candidato e lo induce normalmente a conformarsi. È questo prestigio a consentire alla Commissione elettorale di condizionare le aziende tecnologiche verso le quali non avrebbe poteri sanzionatori diretti: ciò avviene, perché queste non si possono permettere contrapposizioni frontali⁸³ con il soggetto regolatore del processo democratico da cui deriverebbero ripercussioni negative presso l'opinione pubblica.

8. La dimensione “privata” della campagna elettorale: WhatsApp e la messaggistica

La comunicazione politica via messaggistica privata si caratterizza per una propagazione virale dei contenuti attraverso reti fiduciarie ed è divenuta tanto efficace, quanto difficile da controllare. Questi strumenti sono, infatti,

⁸³ Ad esempio, X (ex Twitter) ha accettato di bloccare temporaneamente quattro post durante le elezioni del 2024, perché l'ECI li aveva segnalati come violazioni dell'MCC. In quell'occasione, l'ECI ha ricordato formalmente a X di aver la responsabilità di rimuovere quei contenuti in quanto firmataria del *Voluntary Code of Ethics*.

impareggiabili nel convocare sostenitori e nel coordinare attività: basti pensare alle campagne di *get-out-the-vote*, in cui alla vigilia del voto i partiti possono inviare a milioni di contatti promemoria su come e dove votare oppure organizzano via *chat* il trasporto collettivo di elettori ai seggi. Al tempo stesso, la viralità offerta dalle *chat* di gruppo comporta il rischio di una diffusione incontrollata di informazioni false o polarizzanti.

In India, WhatsApp⁸⁴ ha assunto nell'arena politica un ruolo di primo piano ed è diventato uno strumento essenziale per la mobilitazione e la propaganda durante le campagne elettorali, essendo un canale, che bypassa i *media* tradizionali e raggiunge direttamente l'elettorato. Un singolo utente di Whatsapp può girare un messaggio ricevuto a vari gruppi, ognuno dei quali ha fino a 256 membri (estesi a 1024 membri nei gruppi "comunità") e così via "a cascata". Molti elettori, specialmente nelle aree rurali, ricevono gran parte delle notizie politiche proprio via WhatsApp⁸⁵, spesso inoltrate da persone di fiducia come parenti o amici, il che conferisce a questi contenuti un'aura di maggiore credibilità. Ricerche su gruppi WhatsApp pubblici collegati a partiti hanno riscontrato elevati livelli di *junk news*⁸⁶ e messaggi polarizzanti condivisi durante la campagne, ma anche in periodi pre-elettorali non è raro imbattersi in fotomontaggi o brevi *clip* audio, che attribuiscono a personaggi politici frasi mai dette o atti scandalosi, calibrati per suscitare indignazione e diffondersi viralmente⁸⁷.

L'importanza strategica di Whatsapp era emersa alle elezioni generali del 2014 per affermarsi definitivamente cinque anni più tardi, quando il BJP aveva costruito una capillare infrastruttura comunicativa sull'*app*⁸⁸: secondo fonti del partito, in quell'occasione furono nominati circa

⁸⁴ Alcune stime di mercato indicano che il numero di utenti di Whatsapp ha superato abbondantemente i 3 miliardi di attivi mensili, confermando la posizione dominante dell'app nelle comunicazioni digitali. In termini di mercati nazionali, l'India è di gran lunga il Paese con la più ampia base di utenti: 532,2 milioni, secondo il *Report Backlinko, WhatsApp User Statistics: How Many People Use WhatsApp?*, (24 Nov. 2025), seguita a grande distanza da Brasile (124) e Indonesia (94,3), mentre sarebbero già 535,8 milioni, con Brasile (148) e Indonesia (112), secondo il *Report Resoucera, Insights On 3.3 Billion Global WhatsApp Users*, (17 Nov. 2025).

⁸⁵ La *Columbia Journalism Review* ha rilevato che per molti indiani le *chat* WhatsApp sono diventate una fonte primaria di informazione, spesso sostituendo media tradizionali nelle comunità locali.

⁸⁶ Nell'ambito del *Project on Computational Propaganda* di Oxford, uno studio ha dimostrato che il 25% dei link condivisi su gruppi WhatsApp politici indiani appartenevano a fonti di *junk news* o propaganda. Si veda V. Narayanan, B. Kollanyi, R. Hajela, A. Barthwal, N. Marchal, P.N. Howard. *News and Information over Facebook and WhatsApp during the Indian Election Campaign*, in *Data Memo*, 2 (2019).

⁸⁷ Un contenuto multimediale emozionale, come un *meme* o un video di disinformazione ben confezionato, ha, infatti, maggiori probabilità di venire inoltrato da molti utenti, alimentando la sua diffusione.

⁸⁸ Già nel 2018 l'*Hindustan Times* scriveva di un "*booth-level WhatsApp plan*" secondo il quale il BJP puntava ad avere almeno tre gruppi WhatsApp per ogni seggio elettorale per la *Lok Sabha*: considerato che i seggi in India sono circa 927.000, si parlava potenzialmente di quasi tre milioni di gruppi. In parallelo, il *Deccan Herald* riferiva cifre ancora più alte, riportando che dirigenti del BJP vantavano l'esistenza di almeno cinque milioni di gruppi WhatsApp gestiti dal partito a livello nazionale.

900.000 *WhatsApp pramukh* (leader *WhatsApp*)⁸⁹, ciascuno incaricato di gestire uno o più gruppi e aggregare centinaia di elettori in *chat* apposite⁹⁰. Questi volontari fungevano da snodo locale della campagna digitale, assicurando un flusso costante di messaggi a favore del partito. Nel 2019 la rete di gruppi WhatsApp del BJP copriva virtualmente ogni collegio elettorale, con l'obiettivo di coinvolgere gli elettori su base territoriale sempre più granulare, talvolta persino a livello di seggio: se, in ipotesi, ciascun *WhatsApp pramukh* avesse gestito anche solo un gruppo di 200 membri, teoricamente il BJP sarebbe arrivato a circa 180 milioni di contatti tramite questi canali⁹¹.

Anche altri partiti, pur con ritardo, hanno replicato strategie simili: l'*Indian National Congress* (INC) ha lanciato l'*app Shakti* per organizzare gruppi WhatsApp dei suoi attivisti, mentre varie formazioni regionali hanno istituito canali ufficiali e diffuso inviti per far entrare i sostenitori nelle loro *chat*. Il fenomeno è cresciuto durante la pandemia, quando WhatsApp è stato usato per diffondere video messaggi di candidati in sostituzione dei complicati comizi fisici, garantendo, comunque, un contatto politico-emotivo con le comunità locali. In sostanza, WhatsApp offre ai movimenti politici la possibilità di mobilitare rapidamente le basi, diffondendo slogan, appelli e istruzioni organizzative in modo istantaneo, e parallelamente garantisce la circolazione virale di contenuti all'interno di uno spazio comunicativo "chiuso", percepito come più personale e credibile.

La natura privata e cifrata delle comunicazioni su WhatsApp e su servizi analoghi pone enormi sfide di regolamentazione. A differenza di un comizio o di un volantino, i messaggi in *chat* non sono visibili pubblicamente e, quindi, sfuggono per definizione alla supervisione diretta dell'ECI o di altre autorità. Attualmente in India non esiste una normativa specifica che disciplini la propaganda su WhatsApp o che ne limiti l'uso in campagna elettorale, ma si applicano soltanto i principi generali⁹². Allo stesso modo, l'uso di minacce oppure l'istigazione all'odio razziale o religioso in un gruppo WhatsApp può configurare reati perseguibili ai sensi del Codice penale e della legge elettorale. Il problema concreto diventa però scoprire e provare tali violazioni, dato che la Commissione elettorale e la polizia dipendono da segnalazioni degli stessi utenti⁹³.

⁸⁹ Ogni *WhatsApp pramukh* sarebbe responsabile di uno specifico mini *cluster*, coordinando 2-3 gruppi tendenzialmente a livello di seggio. I gruppi sono organizzati sulla base di un elemento comune (villaggio, casta, interesse): ad esempio, ci sono gruppi di agricoltori, di studenti, di donne del luogo, etc., tutti però almeno simpatizzanti del partito e bendisposti verso la condivisione di *meme*, video brevi, audio con messaggi del BJP, *link* a articoli pro-Modi, contenuti denigratori dell'opposizione...

⁹⁰ Spesso i *pramukh* si dovevano occupare, infatti, di aggiungere nuovi membri ai gruppi, pescando tra i contatti di vicinato, amici, parenti, simpatizzanti identificati durante le campagne porta a porta, etc.

⁹¹ Ovviamente c'è sovrapposizione e non tutti i gruppi saranno stati pieni, ma è per rendere l'idea dei numeri.

⁹² Se, ad esempio, un candidato invia in una *chat* ristretta offerte di denaro in cambio di voti, viola la legge (corruzione elettorale) come se lo facesse di persona.

⁹³ Durante le elezioni dell'Uttar Pradesh del febbraio 2022, ci sono state denunce da parte del Partito *Samajwadi* secondo cui alcuni elettori avevano ricevuto telefonate minatorie, che intimavano di non votare per la loro forza politica. Akhilesh

La propagazione a macchia d'olio via messaggistica rende estremamente difficile tracciare l'origine di messaggi di propaganda e disinformazione: quando la correzione arriva, il messaggio iniziale potrebbe aver già raggiunto anche centinaia di migliaia di persone, radicandosi nell'opinione di una parte di esse e rendendo la smentita tardiva, oltre che spesso parziale. Dopo l'introduzione nel 2021 dell'obbligo di tracciabilità, i legali di Whatsapp hanno presentato ricorso⁹⁴ presso la *Delhi High Court*, sostenendo che la *Rule 4.2* manchi innanzitutto di proporzionalità e poi che la *traceability by design* violi il diritto alla *privacy*, trasformando la piattaforma in un sistema di sorveglianza di massa⁹⁵. Inoltre, per i ricorrenti la norma eccede anche formalmente le previsioni della legge, perché obbligare un intermediario a ricostruire la sua architettura tecnica (indebolendo la crittografia) non rientra nelle previsioni delle sezioni 69A e 79 dell'IT Act.

Nelle memorie depositate in Tribunale e nelle dichiarazioni ufficiali, il governo indiano ha replicato che la norma risponde a un legittimo interesse dello Stato, cioè arginare la propagazione di contenuti che possono causare danni enormi (*fake news* che scatenano violenze, reti di pedopornografia, minacce terroristiche) e l'Avvocatura dello Stato ha citato episodi di linciaggi e sommosse popolari fomentati da *rumors* virali su WhatsApp per sostenere che in questi casi poter rintracciare chi ha messo in circolazione per primo la notizia falsa è cruciale per l'ordine pubblico⁹⁶. L'esecutivo minimizza poi la generalizzazione della *traceability*, che si attiverebbe solo in casi eccezionali e su autorizzazione espressa: non ci sarebbe, dunque, alcuna sorveglianza di massa continua, ma solo la possibilità di identificare l'origine del contenuto illecito, dopo che un magistrato emette un ordine relativo a un reato. Sul piano formale, infine, il governo sostiene di essere legittimato a imporre tale obbligo, perché la sezione 87 dell'IT Act 2000 gli delega il potere di emanare regole e la

Yadav incoraggiò pubblicamente i cittadini a registrare tali minacce per poter sporgere denuncia. Anche se in questo caso si trattava di telefonate, il problema è analogo: eventuali minacce via WhatsApp verrebbero alla luce solo se chi le riceve decidesse di segnalarle, perché altrimenti restano invisibili.

⁹⁴ Per una ricostruzione dei contenuti del ricorso, si vedano A. Saxena, *Delhi High Court Issues Notice To Centre On WhatsApp's Plea Challenging Traceability Clause Under IT Rules 2021*, 27 Aug. 2021, disponibile su <https://www.livelaw.in/top-stories/delhi-high-court-notice-centre-whatsapps-plea-challenging-traceability-clause-under-it-rules-2021-180387>; N. Thapliyal, *Traceability Rule Will Break End-To-End Encryption; Can Put Privacy Of Journalists, Activists, Politicians At Risk: WhatsApp Tells Delhi High Court*, 10 June 2021, disponibile su <https://www.livelaw.in/news-updates/whatsapp-delhi-high-court-traceability-end-to-end-encryption-privacy-risk-174743>.

⁹⁵ Sapendo di poter essere tracciati, gli utenti vedrebbero, infatti, soffocata la propria libertà di espressione *online*, arrivando perfino ad autocensurarsi e ad evitare di condividere contenuti legittimi per timore di ripercussioni.

⁹⁶ Per una ricostruzione della posizione del governo, si veda *Traceability Clause Of IT Rules Reasonable, Govt Expects Platforms To Use Mechanism That Guards Encryption, Protects User Privacy: Centre Tells Delhi HC*, 22 Oct. 2021, disponibile su <https://www.livelaw.in/news-updates/traceability-clause-it-rules-reasonable-platforms-use-mechanism-guards-encryption-protects-user-privacy-delhi-hc-told-184135>.

crescente minaccia dell'uso criminale dei *social* porrebbe la *traceability* nei limiti di tale delega.

Dopo l'accentramento dei vari ricorsi, siamo, dunque, ancora in attesa di una pronuncia complessiva sulla controversia da parte della *Delhi High Court*, ma sappiamo che l'esito dipenderà probabilmente dall'applicazione concreta dei principi della sentenza *Puttaswamy*: i giudici dovranno stabilire, infatti, se l'interesse pubblico a identificare i diffusori originari di messaggi con contenuti illeciti giustifichi l'impatto sulla *privacy* di centinaia di milioni di utenti. Allo stato attuale la norma però non è attuata e la regolazione di WhatsApp rimane soprattutto nelle mani della piattaforma stessa e dei suoi utilizzatori: l'ECI può, infatti, solo richiamare i partiti a un uso etico del mezzo, inserendo i canali WhatsApp ufficiali nelle comunicazioni elettorali soggette al MCC e intervenendo *ex post*, se emergono infrazioni documentabili.

Vista l'impossibilità di un monitoraggio diretto, la strategia per contenere gli abusi su WhatsApp si è focalizzata su misure indirette e preventive. Sul versante tecnologico, WhatsApp ha implementato dal 2018-19 cambiamenti rilevanti: come accennato nel § 7, ha limitato il numero di inoltri possibili per ogni messaggio (prima illimitati, poi passati a 5 già nel 2019 e adesso ad 1 *chat* oltre una certa soglia di *forwarding*) e ha introdotto indicatori visivi che segnalano se un messaggio è stato inoltrato molte volte (la doppia freccia) per mettere in guardia i lettori. Ha reso anche più facile per gli utenti segnalare *spam* o abusi, inoltrando l'ultimo messaggio ricevuto direttamente a WhatsApp che può liberamente esaminarne il contenuto crittografato, trattandosi di una condivisione volontaria del destinatario.

Sulla base delle segnalazioni degli utenti e di sistemi di rilevamento anomalo, l'azienda dichiara di bannare proattivamente ogni mese addirittura milioni di account⁹⁷, che violano i termini di servizio: spesso si tratta di numeri sospetti, perché creano troppi gruppi o inviano messaggi massivi a non contatti, comportamenti tipici di *bot* o di strumenti illeciti usati da alcune agenzie di propaganda. Questi interventi hanno reso più costosa e difficile la diffusione virale artificiale di messaggi politici: i gruppi non possono più essere usati come altoparlanti illimitati e i tentativi di aggiungere automaticamente migliaia di persone a *chat* propagandistiche vengono bloccati dai filtri "anti-automazione"⁹⁸.

Le ultime campagne elettorali hanno visto un uso più sofisticato di WhatsApp: gruppi per comparto (donne, giovani, caste specifiche), dove circolano poster digitali e brevi video personalizzati; *chatbot* sperimentali, in grado di rispondere agli elettori su programmi e candidature; chiamate vocali automatizzate⁹⁹ su vasta scala, in cui una voce preregistrata del politico esorta gli ascoltatori al voto. Dal punto di vista dei contenuti, le

⁹⁷ Questa informazione è confermata dai *Transparency Reports* di WhatsApp che mostrano il *ban* di 2-3 milioni di account al mese in India per comportamenti anomali.

⁹⁸ Queste misure non hanno fatto sparire la propaganda via WhatsApp, ma i partiti si sono dovuti adeguare alle nuove regole: adesso invece che su "grandinate" di messaggi anonimi, puntano su messaggi mirati e contestualizzati, spesso scritti da volontari locali nella lingua e nel dialetto dell'area, così da risultare più autentici.

⁹⁹ Si tratta di *robocalls* telefoniche, non semplici messaggi vocali inoltrati via WhatsApp.

dinamiche dell'ultimo periodo mostrano una polarizzazione pronunciata: ogni schieramento ha il proprio "ecosistema" di *chat* in cui domina una narrazione favorevole alla propria parte, creando una sorta di "camere dell'eco" private.

Le bufale a tema elettorale non mancano mai¹⁰⁰, ma spesso è difficile stimarne l'impatto reale, dato che restano confinate nelle reti sociali di chi le riceve. Gli osservatori concordano che la comunicazione via WhatsApp abbia avuto un peso non trascurabile sugli esiti elettorali recenti in India, sebbene sia arduo isolare la sua influenza esatta¹⁰¹. Il BJP attribuisce parte del suo successo nel 2019 alla mobilitazione digitale, rivendicando di aver saputo raggiungere e convincere elettori in aree remote grazie all'organizzazione della propria "macchina WhatsApp". Studi accademici e *reportage* giornalistici¹⁰² hanno anche documentato come in molti villaggi le discussioni politiche su WhatsApp abbiano sostituito i comizi come fonte primaria di informazioni sul voto. La grande diffusione di *smartphone* a basso costo ha fatto sì che persino fasce di popolazione prima isolate oggi ricevano audio e video di propaganda direttamente sul telefonino. Questo ha indubbiamente ampliato la cassa di risonanza dei partiti: un messaggio può essere reiterato quotidianamente in centinaia di *chat*, condizionando gli elettori molto più di un titolo di giornale.

Tuttavia, è dibattuto se l'uso della messaggistica e dei contenuti sintetici sia davvero in grado di cambiare il voto delle persone o se si limiti ad amplificare narrazioni già esistenti, rafforzando convinzioni preesistenti più che realizzare delle conversioni. In altre parole, WhatsApp può servire a motivare e organizzare i propri sostenitori (mobilitazione orizzontale) e a demonizzare gli avversari agli occhi di chi è già vicino, ma è meno certo che riesca a far cambiare schieramento a un elettore convinto. Detto questo, in competizioni serrate anche uno spostamento di pochi punti percentuali può risultare decisivo e nelle elezioni generali indiane ci sono collegi uninominali, che si decidono per poche migliaia di voti, un margine che una campagna WhatsApp ben orchestrata potrebbe colmare, raggiungendo con argomenti mirati gli indecisi e i simpatizzanti un po' più recalcitranti.

¹⁰⁰ Nel 2022, ad esempio, circolò ampiamente su WhatsApp la falsa notizia che in un certo Stato la macchina elettronica di voto (EVM) fosse stata modificata per assegnare i voti solo a un partito, costringendo l'ECI a una smentita ufficiale.

¹⁰¹ Il *Financial Times* e altri *media* avevano definito le elezioni 2019 "*WhatsApp election*", segno che quasi tutti i commentatori attribuivano a WhatsApp un ruolo significativo.

¹⁰² Sul ruolo di WhatsApp come strumento primario di informazione e discussione politica nei contesti rurali indiani si vedano V. Srivastava, M. Singh, *PoliWAM: An Exploration of a Large Scale Corpus of Political Discussions on WhatsApp Messenger*, in *Proceedings of the Seventh Workshop on Noisy User-generated Text (W-NUT 2021)*, Association for Computational Linguistics, Nov. 2021, pp. 120-130; P. Bengani, *Tow Center for Digital Journalism*, «India had its first 'WhatsApp election'. We have a million messages from it», in *Columbia Journalism Review* (16 Oct. 2019); V. Narayanan, B. Kollanyi, R. Hajela, A. Barthwal, N. Marchal, P.N. Howard. *News and Information over Facebook and WhatsApp during the Indian Election Campaign*, cit.

Dal punto di vista qualitativo, l'impatto di queste piattaforme sulla democrazia indiana è quantomeno ambivalente¹⁰³. Da un lato, hanno democratizzato l'accesso all'informazione politica¹⁰⁴: non occorre più un televisore o saper leggere il giornale, se chiunque può ricevere video esplicativi sui programmi o addirittura interagire direttamente con i candidati in forum *online*. Dall'altro, l'opacità e l'assenza di controllo di queste comunicazioni hanno facilitato pratiche deleterie – dalla diffusione di odio settario alla propagazione di teorie del complotto –, che possono minare la qualità del dibattito pubblico e la correttezza del voto. In conclusione, la messaggistica privata è diventata per le elezioni indiane un'arma a doppio taglio: potentissima per organizzare e motivare al voto, ma altrettanto efficace nel disinformare e segmentare l'elettorato in bolle impermeabili. Fino a quando non interverrà una regolazione più incisiva o non maturerà una maggiore consapevolezza mediatica collettiva, il peso elettorale di WhatsApp continuerà a farsi sentire, probabilmente crescendo ancora, come fattore sia di partecipazione, sia di potenziale distorsione dei processi democratici.

9. La stampa al servizio della politica: inserzioni a pagamento e *paid news*

Il comune denominatore di inserzioni politiche e *paid news* risiede nell'uso di risorse finanziarie per influenzare il discorso pubblico durante le elezioni. La normativa indiana tratta le due fattispecie in modo distinto, ma entrambe rientrano in una più ampia riflessione sulla trasparenza del rapporto tra utilità economica e informazione: da una parte, le inserzioni regolamentate rappresentano la forma ufficiale e riconosciuta di pubblicità politica a pagamento; dall'altra, il fenomeno delle *paid news* ne costituisce l'ombra, l'impiego "occulto" di denaro per ottenere copertura giornalistica favorevole sotto forma di notizie apparentemente neutrali. Analizzare in parallelo le due pratiche consente di cogliere tanto le dinamiche lecite e trasparenti di finanziamento della comunicazione politica, quanto le distorsioni che derivano dal ricorso a pratiche nascoste e spesso difficilmente sanzionabili.

In India, le inserzioni pubblicitarie a pagamento, soprattutto quelle di natura politica, sono soggette a una regolamentazione severa¹⁰⁵, in particolare nel periodo elettorale. L'organo centrale di riferimento resta sempre l'*Election Commission of India* ed è previsto che tutte le pubblicità

¹⁰³ In senso fortemente critico, si veda C. Arun, *On WhatsApp, Rumours and Lynchings* in S. Narrain (ed.), *Acts of Media: Law and Media in Contemporary India*, New Delhi, 2022, spec.128-137.

¹⁰⁴ Il condizionamento di Whatsapp va chiaramente ben oltre la dimensione politica: si veda, ad esempio, P. Krishna, *WhatsApp Is Changing the Way India Talks About Food*, in *New York Times* (23 Nov. 2018).

¹⁰⁵ La regolamentazione si fonda sulle direttive dell'ECI in materia di certificazione preventiva delle inserzioni politiche, attuate attraverso i *Media Certification and Monitoring Committees* (MCMC), istituiti nell'esercizio dei poteri di cui all'art. 324 Cost., sulla sezione 126 del RPA per il silenzio elettorale, e sulle IT Rules 2021 per le piattaforme digitali.

politiche diffuse sui diversi canali ¹⁰⁶ (televisione, radio, stampa e piattaforme digitali) debbano essere preventivamente certificate: sussiste, quindi, un meccanismo di pre-approvazione, introdotto proprio per evitare l'immissione nello spazio pubblico di messaggi ingannevoli o non tracciabili. Per essere trasmesso o pubblicato il contenuto delle inserzioni deve rispettare regole precise: sono vietate affermazioni false, denigratorie o fuorvianti, così come appelli a divisioni religiose, di casta o di tipo *communal*. Ogni messaggio deve poi riportare con chiarezza il nome e l'indirizzo del committente, il partito o candidato a beneficio del quale viene diffuso e i relativi costi sostenuti. Questi requisiti di trasparenza hanno lo scopo di rendere evidente all'elettorato l'origine dei messaggi e di garantire che le relative spese siano contabilizzate nel bilancio elettorale ufficiale¹⁰⁷.

La normativa impone un periodo di silenzio elettorale di 48 ore prima del voto, durante il quale non è consentita la pubblicazione o la trasmissione di nuove inserzioni¹⁰⁸. Inoltre, soltanto i soggetti politici autorizzati – cioè i partiti registrati e i candidati ufficiali – hanno la facoltà di commissionare pubblicità di natura politica, in modo tale da rendere più complicate forme di condizionamento da parte di gruppi esterni o soggetti non dichiarati. Il concetto di “pubblicità politica” è estremamente ampio e comprende qualsiasi annuncio volto a promuovere o criticare un partito, un candidato o una specifica questione politica, indipendentemente dal mezzo impiegato. Di conseguenza, le piattaforme *online* sono del tutto equiparate ai *media* tradizionali e anche gli annunci digitali devono essere pre-approvati, riportare i dati del committente e rispettare i divieti di contenuto. Le principali società tecnologiche si sono adeguate, introducendo procedure di verifica dell'identità degli inserzionisti e archivi pubblici delle inserzioni politiche¹⁰⁹, affiancando la loro azione a quella delle autorità di controllo elettorale, nel tentativo di estendere il principio di trasparenza anche alle campagne digitali, terreno sempre più decisivo nelle competizioni elettorali.

Il *Ministry of Information and Broadcasting* continua a disciplinare le trasmissioni radiotelevisive attraverso regolamenti e codici, ma è sempre l'ECI a detenere il ruolo primario in materia di propaganda politica: un ruolo cruciale è svolto, infatti, dai *Media Certification and Monitoring Committees* (MCMC), istituiti dalla Commissione a livello statale e distrettuale, con la funzione di esaminare preventivamente i contenuti pubblicitari e monitorare i *media* durante le campagne per individuare

¹⁰⁶ Le reti televisive via cavo, ad esempio, non possono trasmettere spot politici non autorizzati, pena conseguenze legali derivanti sia da queste direttive elettorali sia dal Cable TV Act. Analoghi vincoli esistono per la stampa: ogni annuncio politico sui giornali deve essere certificato preventivamente e imputato alle spese elettorali del committente.

¹⁰⁷ Tutto questo, come abbiamo visto nel § 7, non avviene nel caso degli *influencer*.

¹⁰⁸ Il periodo di silenzio elettorale di 48 ore, che vieta ogni forma di propaganda elettorale nel lasso temporale immediatamente precedente al voto era originariamente riferito a comizi e mezzi tradizionali, ma è stata progressivamente interpretata dall'ECI in senso estensivo, ricomprendendo anche *media* digitali e piattaforme *online*.

¹⁰⁹ In particolare, piattaforme come Meta, Google e YouTube hanno istituito *public ad libraries* o *ad transparency repositories*, accessibili agli utenti, che consentono di consultare le inserzioni politiche pubblicate, il soggetto pagante, la spesa sostenuta e il periodo di diffusione. Questi strumenti sono stati introdotti anche in risposta alle richieste di trasparenza avanzate dall'ECI, a partire dalle elezioni generali del 2019.

violazioni, comprese le forme occulte di *paid news*. La composizione mista dei Comitati¹¹⁰ serve a garantire imparzialità e controllo incrociato. In concreto, un candidato che intenda diffondere uno spot deve presentare il materiale con alcuni giorni di anticipo: il Comitato ne verifica la conformità alle regole e rilascia una certificazione. I MCMC sorvegliano, dunque, attivamente giornali, TV, radio e *social media*, segnalando eventuali violazioni e questo sistema rappresenta oggi un pilastro della protezione dell'integrità elettorale¹¹¹.

In India, le inserzioni politiche a pagamento risultano, quindi, strettamente regolate: i contenuti devono essere certificati, i committenti dichiarati e le spese rendicontate, al fine di prevenire manipolazioni, garantire trasparenza e assicurare parità di condizioni tra i candidati. Tuttavia, accanto a questa forma lecita e regolata di comunicazione politica, si è sviluppato un fenomeno parallelo che ne rappresenta il “lato oscuro”: il *paid news*. Se, infatti, le inserzioni regolamentate costituiscono la dimensione ufficiale della pubblicità politica a pagamento, le *paid news* ne sono la declinazione meno trasparente: si tratta della pratica con cui un politico o un partito paga un organo di stampa o un singolo giornalista per ottenere articoli favorevoli, presentati come notizie neutrali¹¹².

Le *paid news* alterano gravemente la trasparenza dell'informazione e la parità elettorale: candidati dotati di risorse ingenti possono acquistare grande copertura positiva sui *media*, ingannando il pubblico, che crede di trovarsi di fronte ad articoli imparziali. Nonostante i divieti deontologici e le linee guida elettorali, il contrasto alla pratica è reso complesso soprattutto dalla difficoltà di provare l'accordo illecito: gli articoli a pagamento sono spesso ben “camuffati” e manca un chiaro quadro normativo, che configuri la condotta come reato autonomo. Dal punto di vista giuridico, la disciplina si fonda principalmente sulle regole di trasparenza dei finanziamenti e delle spese di campagna: il RPA obbliga i candidati a includere nei rendiconti tutte le spese sostenute per la promozione della propria candidatura¹¹³, comprese quelle per articoli

¹¹⁰ I MCMC includono rappresentanti dell'ECI, funzionari governativi, membri dei *media* e della società civile.

¹¹¹ Nella documentazione ufficiale della *Election Commission of India* e nelle linee guida applicative sul controllo dei *media* in periodo elettorale, il fondamento del sistema di pre-certificazione delle inserzioni politiche viene ricondotto all'ordine della Corte Suprema del 13 aprile 2004 (*Ministry of Information and Broadcasting v. Gemini TV Pvt. Ltd.*), con cui i giudici riconobbero la legittimità costituzionale della certificazione preventiva degli spot politici su televisioni e reti via cavo, al fine di garantire elezioni libere ed eque. Questo orientamento è stato successivamente esteso dall'ECI anche alla stampa e ai *media* digitali, divenendo il presupposto giurisprudenziale dell'attuale sistema di controllo delle comunicazioni elettorali.

¹¹² Il *Press Council of India* definisce la fattispecie come qualsiasi notizia o analisi apparsa su *media* stampati o elettronici in cambio di un compenso. Si tratta di una pratica formalmente vietata dall'ordinamento, ma è diffusa in forme difficilmente individuabili, nonostante già dagli anni Duemila fosse considerata pervasiva, strutturata e organizzata.

¹¹³ Sezione 77(1) del *Representation of the People Act*, 1951 (RPA).

favorevoli, e l'omissione equivale a una falsa dichiarazione con gravi conseguenze¹¹⁴.

L'ECI ha, inoltre, sollecitato l'intervento del legislatore: in particolare, l'inclusione delle *paid news* tra le *corrupt practices* previste dal diritto elettorale, equiparandole alla corruzione di elettori tramite l'introduzione di un reato specifico, che sanzioni sia i politici, sia i giornalisti e i *media* coinvolti, con pene detentive fino a due anni. Al momento, tuttavia, le sanzioni si limitano a conseguenze elettorali: l'ECI può dichiarare un candidato colpevole di false dichiarazioni e annullarne l'elezione o disporre la squalifica fino a tre anni¹¹⁵. Nonostante divieti e sanzioni, le *paid news* rimangono diffuse, soprattutto nelle grandi competizioni elettorali¹¹⁶, e inchieste giornalistiche hanno rivelato che in passato quotidiani e canali televisivi di rilievo hanno venduto proprio dei pacchetti di copertura positiva a politici di diversi partiti¹¹⁷.

Le dimensioni del problema sono accresciute da forme di collusione strutturale tra *media* e politica. Alcuni grandi conglomerati editoriali hanno stipulato dei cd. *private treaties*, accordi con cui ricevono partecipazioni azionarie o pagamenti da aziende e politici in cambio di copertura favorevole¹¹⁸. Questi intrecci rendono ancora più difficile distinguere l'informazione genuina dalla pubblicità occulta, perché formalmente la *partnership* non è nascosta, ma non c'è neanche una spesa espressamente elettorale. Negli ultimi anni l'attenzione pubblica è cresciuta e le pressioni per una riforma normativa si sono intensificate: commissioni parlamentari hanno giudicato gli attuali meccanismi di autoregolamentazione dei *media* un palliativo inefficace, auspicando

¹¹⁴ La pubblicazione di *paid news* è considerata dall'ECI una forma di elusione dei limiti di spesa elettorale e una distorsione della volontà popolare e, quindi, i MCMC sono incaricati di monitorare sistematicamente i *media* e attribuire ai candidati le spese corrispondenti anche in relazione a questo fenomeno.

¹¹⁵ Un caso emblematico di applicazione delle regole elettorali in materia di *paid news* è quello di Umlesh Yadav (2011), deputata eletta all'Assemblea legislativa dell'Uttar Pradesh. L'ECI accerta che la candidata aveva beneficiato di articoli favorevoli a pagamento, presentati come notizie neutrali, senza includerne il costo nel rendiconto delle spese elettorali. Qualificando tali contenuti come spesa occulta e come falsa dichiarazione, l'ECI dispone la sua squalifica per tre anni: si tratta del primo caso in cui le *paid news* hanno condotto a una sanzione elettorale diretta, divenendo un precedente simbolico nella prassi della Commissione.

¹¹⁶ Sul persistere del fenomeno si vedano i dati comunicati al Parlamento indiano dal Ministro di Stato per l'Informazione e la Radiotelevisione, secondo cui il *Press Council of India* ha ricevuto 468 casi di *paid news* nel 2021-2024, con un'impennata a 290 casi nel solo dal 2024, riportati in *Press Council got most paid news complaints in 2024-25 from Rajasthan: Govt*, in *Newslandry* (12 March 2025).

¹¹⁷ Nelle elezioni del 2009 emerse che vari quotidiani pubblicarono simultaneamente articoli quasi identici in favore di alcuni candidati, segno di accordi occulti (tra i coinvolti vi fu l'ex *Chief Minister* del Maharashtra, Ashok Chavan). Più in generale, tra il 2009 e il 2013 l'ECI aveva già registrato oltre 1.400 casi accertati, probabilmente solo una frazione del fenomeno reale.

¹¹⁸ Del fenomeno si era già occupato tempestivamente anche il *Reuters Institute for the Study of Journalism* dell'Università di Oxford: si veda A. Sharma, *In need of a Leveson? Journalism in India in times of paid news and 'private treaties'*, Fellow's Paper, 2013, disponibile su <https://reutersinstitute.politics.ox.ac.uk/our-research/need-leveson-journalism-india-times-paid-news-and-private-treaties>.

l'istituzione di un organo unico di vigilanza con poteri sanzionatori più incisivi. La combinazione di divieti formali, obblighi di trasparenza e sanzioni elettorali indirette ha prodotto alcuni effetti positivi, ma l'elusione sostanziale resta diffusa, alimentata da complicità mediatiche e da questi vuoti normativi.

In conclusione, la disciplina indiana delle comunicazioni elettorali mostra un contrasto evidente: da un lato, c'è un sistema rigoroso di regolazione delle inserzioni pubblicitarie, con controlli preventivi e registrazione obbligatoria delle spese; dall'altro, la persistenza delle *paid news* mina la credibilità dei *media* e l'equità della competizione politica. Si è scelto di analizzare congiuntamente queste due dimensioni per ribadire come le risorse economiche, veicolate attraverso canali ufficiali o occulti, condizionino in profondità la formazione del consenso. La sfida principale resta quella di colmare le lacune normative e rafforzare i meccanismi di *enforcement*¹¹⁹, al fine di assicurare che il rapporto tra denaro e informazione non comprometta oltre misura la trasparenza del processo democratico.

10. L'utilizzo dei *social* da parte di titolari di cariche pubbliche

I titolari di cariche pubbliche utilizzano sempre di più piattaforme come X, Facebook, Instagram e WhatsApp per raggiungere direttamente i cittadini, promuovere le proprie politiche e costruire consenso tramite il fenomeno globale della disintermediazione della comunicazione politica. A livello federale, l'India presenta alcuni dei casi più eclatanti al mondo di *leader* politici, che hanno costruito una vasta platea di seguaci *online* e trasformato i *social media* in un'estensione del proprio ruolo istituzionale.

Il *premier* Narendra Modi è attualmente il politico in attività più seguito sui *social media*: conta 99,3 milioni di *followers* su Instagram (zero seguiti) e 109 milioni su X, risultando la personalità indiana più seguita *online* in assoluto e posizionandosi ai vertici globali (dietro Barack Obama, ma superando Donald Trump), senza contare i milioni di seguaci sulla sua pagina Facebook e sul canale YouTube. Questa enorme presenza mediatica *online*¹²⁰ non è solo quantitativa, ma anche qualitativa: Modi ha aperto il suo account Twitter già nel 2009 e da allora ha "dominato" la piattaforma come strumento di *leadership*, enfatizzando messaggi chiave del suo governo e utilizzando uno stile narrativo, che esalta i valori tradizionali e nazionalisti. Già nel 2015 il Primo Ministro aveva lanciato la *Narendra Modi App* (NaMo App), un'applicazione mobile attraverso cui diffonde

¹¹⁹ Nel 2017 Narottam Mishra, Ministro del Madhya Pradesh ed esponente di primo piano del *Bharatiya Janata Party*, viene accusato di aver finanziato oltre quaranta articoli favorevoli, durante le elezioni del 2008, senza riportarne i costi nei rendiconti elettorali. Anche in questo caso, l'ECI ne dispone la squalifica triennale, ma la sanzione viene successivamente annullata dai Tribunali per vizi procedurali, senza tuttavia mettere in discussione la qualificazione delle *paid news* come pratica distortiva del processo elettorale. Il caso evidenzia come la determinazione dell'ECI nel contrastare il fenomeno possa infrangersi contro i limiti strutturali dell'attuale meccanismo sanzionatorio.

¹²⁰ Sull'esposizione mediatica di Modi, si veda P. Sharma, V. Jain, *Influencers and the Building of Political Brands – The Case of India*, cit., 75-82.

direttamente aggiornamenti, discorsi e campagne, chiedendo al pubblico di partecipare attivamente a sondaggi e iniziative governative.

Oltre al Primo Ministro, quasi tutti i Ministri federali e gli organi centrali utilizzano attivamente i *social media*. Il Ministero degli Esteri indiano è stato pioniere nella cosiddetta *Twitter diplomacy*: già durante il primo governo Modi (2014-2019), la Ministra degli Esteri Sushma Swaraj divenne celebre per il suo uso di Twitter come strumento di assistenza consolare, trasformandolo in un vero e proprio sportello di aiuto per la diaspora indiana e rispondendo a richieste di soccorso di cittadini indiani bloccati all'estero, con problemi di visti o in situazioni di emergenza¹²¹. Analogamente altri Ministri hanno usato Twitter per migliorare i servizi: l'ex Ministro delle Ferrovie Suresh Prabhu divenne noto per rispondere personalmente ai *tweet* dei passeggeri in difficoltà¹²².

Accanto ai casi virtuosi, non mancano effetti problematici derivanti dall'uso intensivo dei *social* da parte dei titolari di cariche pubbliche: la comunicazione politica *online* può, infatti, facilmente sconfinare nella disinformazione e nell'incitamento all'odio. Un'analisi condotta da NDTV¹²³ ha mostrato un dato allarmante: nei primi quattro anni del governo Modi (2014-2018) le dichiarazioni pubbliche classificabili come *hate speech* da parte di politici di alto profilo (Ministri, parlamentari nazionali, *leader* locali) erano aumentate di quasi il 500% rispetto al lustro precedente e di questi episodi il 90% era attribuibile proprio a esponenti del BJP, il partito ancora al potere. Inoltre, il fenomeno dei "*VIP hate speech*" raramente comporta sanzioni: la quasi totalità dei politici che ha pronunciato frasi d'odio non ha subito conseguenze significative e questo dato solleva interrogativi sul bilanciamento tra libertà di espressione e responsabilità istituzionale *online*.

Questo utilizzo massiccio dei *social* si estende capillarmente ai governi statali e alle amministrazioni locali: nel 2021 una ricerca di *Microsoft Research* ha censito ben 37.633 politici indiani attivi su Twitter¹²⁴, appartenenti a diverse formazioni e distribuiti in tutti gli Stati del Paese. Naturalmente emergono differenze di approccio: in alcuni Stati con

¹²¹ Ci sono episodi ampiamente riportati dai *media* che mostrano come bastasse un *tweet* per ottenere il suo intervento: ad esempio, ha aiutato studenti indiani in difficoltà, famiglie bloccate in aeroporti stranieri e persino garantito supporto con prontezza a una ragazza quattordicenne con problemi di visto. Il suo approccio diretto e compassionevole – riassunto dalla famosa battuta «*even if you are on Mars, the Indian Embassy will help you*» – le è valso enorme popolarità e ha mostrato il lato positivo dell'*engagement* istituzionale sui *social*.

¹²² È celebre il caso di un bambino di 5 mesi, che necessitava di latte su un treno: una passeggera lanciò un SOS su Twitter e in 40 minuti il latte venne fatto trovare alla stazione successiva, con grande plauso pubblico. In un altro caso, sempre grazie a un *tweet*, le ferrovie intervennero per fermare delle molestie a bordo treno, facendo scendere e arrestare i responsabili alla stazione seguente. Questi esempi evidenziano come i *social media* possano fungere da canale di *feedback* immediato tra cittadini e istituzioni, consentendo azioni rapide che migliorano la percezione dell'efficacia governativa.

¹²³ N. Jaiswal, S. Jain, M.P. Singh, *Under Modi Government, VIP Hate Speech Skyrockets - By 500%*, in *NDTV.com* (17 Apr. 2018).

¹²⁴ G. Shekhawat, P. Singh, R. Grover, S. Dash, H. Negi, A. Sharma, S. Sagarika, J. Pal, *Twitter Use by Politicians Across States in India*, per *Microsoft Research* (Oct. 2021).

popolazione anglofona o hindi predominante (come Uttar Pradesh, Bihar, Delhi) i politici ricorrono molto a X e Facebook, mentre in Stati con lingua regionale forte (Tamil Nadu, Bengala Occidentale, Maharashtra) i *leader* locali tendono a comunicare anche in tamil, bengali, marathi, etc. per raggiungere il proprio elettorato¹²⁵.

Un primo esempio di gestione dei *social media* a livello statale è offerto nel maggio 2025 dal *Department of Science and Technology* del Gujarat, che ha emesso un *advisory*, in cui si chiedeva ai dipendenti pubblici di evitare di condividere opinioni politiche, notizie non verificate o qualsiasi contenuto, che potesse compromettere la neutralità o l'immagine pubblica del governo, mettendo anche in guardia contro la pubblicazione di dettagli relativi alle forze di sicurezza o alle operazioni interne. Il tono era di natura precauzionale, incentrato sulla professionalità e sull'autocontrollo, ma non menzionava alcuna conseguenza disciplinare: in breve, si trattava di una serie di suggerimenti piuttosto che di norme vincolanti.

Il caso emblematico è però rappresentato dallo Stato del Maharashtra (il secondo più popoloso dell'India, che comprende Mumbai), che il successivo luglio ha emanato linee guida ufficiali per l'uso dei *social media* da parte di tutti i dipendenti pubblici e funzionari dello Stato. Questo provvedimento¹²⁶ nasceva dall'esigenza di prevenire fughe di informazioni riservate e comunicazioni improprie via *social* da parte di personale governativo¹²⁷. Le nuove regole delineano una serie di obblighi e divieti: ad esempio, i dipendenti statali non possono criticare sui *social* le politiche o le azioni del governo oppure commentare eventi politici in modo negativo¹²⁸. Inoltre, viene richiesto a ogni funzionario di mantenere separati gli account personali da quelli professionali, evitando commistioni tra opinioni private e ruolo istituzionale, mentre è consentito utilizzare applicazioni di

¹²⁵ È stato osservato, ad esempio, che i *tweet* in hindi funzionano bene non solo per i politici del Nord, ma anche per i partiti nazionali operanti in Stati hindi-foni; viceversa i *tweet* in lingue regionali, pur importanti per identità locale, ottengono in media minore viralità rispetto a hindi o inglese. Ciò nonostante, molti *Chief Minister* statali hanno costruito una presenza *social* significativi.

¹²⁶ Government of Maharashtra, *Government Resolution on Use of Social Media by Government Servants*, 28 July 2025.

¹²⁷ A. Bansal, *Maharashtra Issues Social Media Guidelines for Govt Employees*, in *Medianama* (29 July 2025).

¹²⁸ Queste linee guida adottate dallo Stato del Maharashtra sull'uso dei *social media* da parte dei dipendenti pubblici sollevano interrogativi delicati in relazione all'art. 19 Cost. In particolare, il divieto generalizzato per i funzionari di criticare politiche governative o commentare negativamente questioni politiche, anche al di fuori delle funzioni ufficiali, rischia decisamente di eccedere i limiti delle restrizioni ragionevoli ammesse dall'art. 19(2). Sebbene la giurisprudenza costituzionale riconosca agli Stati un margine più ampio nel circoscrivere l'espressione dei propri dipendenti in funzione delle esigenze di neutralità politica, lealtà istituzionale, disciplina e decoro (si vedano *Kameshwar Prasad v. State of Bihar*, 1962, *O.K. Ghosh v. E.X. Joseph*, 1963, e *Union of India v. Tulsiram Patel*, 1985), questi limiti devono, comunque, rispettare quantomeno il criterio di proporzionalità (si veda ancora *Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017) e non possono tradursi in una compressione indiscriminata del dissenso politico individuale. Le regole del Maharashtra si collocano, pertanto, in una zona di frizione tra esigenze di buon andamento dell'amministrazione e tutela delle libertà fondamentali, che potrebbe essere oggetto di futuro scrutinio giudiziario.

messaggistica, come WhatsApp o Telegram, esclusivamente per comunicazioni di servizio interne. Allo stesso tempo, le linee guida incoraggiano i funzionari a promuovere sui *social* i risultati positivi dei programmi governativi, senza però indulgere in autocelebrazioni. Vengono proibiti riferimenti non autorizzati a simboli ufficiali (loghi, stemmi, immagini di edifici governativi) nei post privati, si stabilisce che solo persone espressamente autorizzate possano gestire gli account *social* ufficiali delle istituzioni e la violazione di queste norme comporta sanzioni disciplinari.

Con questa scelta il Maharashtra vuole porsi all'avanguardia nel tentare di regolamentare in modo organico la condotta *social* dei propri funzionari pubblici, riconoscendo implicitamente l'enorme impatto che anche un singolo post imprudente di un dipendente può avere sull'immagine e sulla tenuta dell'azione di governo. Oltre a queste regole interne, in vista delle locali elezioni amministrative, il governo aveva elaborato a giugno delle *Digital Media Advertising Guidelines*, che prevedono collaborazioni con *mega-influencer* (oltre 1 milione di *followers*), *macro*, *micro* e *nano-influencer* (fino a 10 mila *followers*), con l'obiettivo di coinvolgerli nella diffusione dei programmi di governo e dei messaggi di pubblica utilità. Si tratta di un'evoluzione significativa: il tradizionale ufficio relazioni pubbliche di uno Stato indiano ora include la gestione di campagne con *digital influencer*, segno di un adattamento delle istituzioni alle logiche della comunicazione "dal basso" proprie dei *social*.

L'uso dei *social media* da parte di titolari di cariche pubbliche in India ha rivoluzionato il rapporto tra istituzioni e cittadini, portando benefici in termini di comunicazione diretta, trasparenza e reattività, ma sollevando al contempo nuove sfide per la democrazia e il buon governo. A livello federale, figure come il Primo Ministro Modi hanno, come si è detto, sfruttato in maniera magistrale queste piattaforme, costruendo una presenza senza precedenti, ma al tempo stesso resta un'arena digitale poco regolamentata, dove il linguaggio d'odio e la disinformazione trovano ampia diffusione. A livello statale e locale, la pervasività dei *social media* sta invece spingendo le amministrazioni a definire codici di condotta, come in Maharashtra, e a sperimentare nuove forme di coinvolgimento.

11. Le proposte di riforma in discussione

Nell'ultimo periodo il governo indiano ha manifestato l'intenzione di rinnovare profondamente l'architettura normativa in materia di comunicazioni e *media*, per adeguarla all'era digitale e, secondo i critici, per accentrare maggiormente il controllo su un settore divenuto critico anche politicamente. Tra le nuove iniziative figurano due progetti di legge di grande portata: il *Broadcasting Services (Regulation) Bill*, 2023, e il *Digital India Bill*, destinati rispettivamente a riformare il panorama radiotelevisivo (inclusi *streaming* e *news* digitali) e a sostituire l'IT Act con una disciplina onnicomprensiva. Il *Broadcasting Bill* è circolato in bozza per consultazioni pubbliche, mentre il *Digital India Bill* è in fase di elaborazione, con il governo che prevede di presentarlo al Parlamento dopo aver raccolto pareri di esperti e *stakeholder*. Pertanto, il quadro giuridico vigente resta quello

delineato nei paragrafi precedenti, ma vale la pena esaminare cosa prevedono questi progetti e quali sono le dichiarazioni di intenti del governo.

Il *Broadcasting Bill*, mira a superare il vecchio Cable TV Act e creare un quadro unificato per tutti i servizi di diffusione. Il progetto prevede di assoggettare a una regolazione organica la TV tradizionale, le piattaforme OTT, le *digital news* e i contenuti dei *social media*, eliminando l'attuale distinzione normativa tra trasmissione via etere/cavo e *streaming* via Internet. Tra i punti salienti: a) si prevede l'obbligo per le reti televisive di registrarsi presso il governo centrale, mentre le piattaforme OTT sono tenute a notificare la loro attività, se superano un certo numero di abbonati; b) l'applicazione dei Codici dei programmi e della pubblicità sono estesi dalla TV alle piattaforme *online* per conformare tutti i contenuti di *news* e attualità (tranne la stampa) alle medesime linee guida su decoro, *hate speech*, *par condicio*, etc.; c) si definisce una struttura di co-regolamentazione tramite un meccanismo su tre livelli simile a quello delle IT Rules 2021 per i *digital media* (i tre livelli sono l'autoregolazione delle emittenti, la creazione di organismi di categoria di autoregolamentazione e al vertice un *Broadcasting Advisory Council* (BAC) nazionale con funzioni di indirizzo e vigilanza e una composizione che includa rappresentanti del governo e dell'industria); d) ogni emittente deve istituire al suo interno una *Content Evaluation Committee* (CEC), che valuti preventivamente la conformità di ogni contenuto diffuso ai Codici¹²⁹.

La proposta rischia di essere assieme ridondante e incompleta: da una parte, il disegno di legge include, infatti, la regolamentazione dei contenuti OTT, ambito già (seppur parzialmente) coperto dalle IT Rules 2021 e dall'IT Act; dall'altra, la bozza non chiarisce la formulazione del nuovo *Program Code* e paradossalmente questa mancanza potrebbe spingere i *broadcaster* a una maggiore autocensura per timore di sanzioni. Il *Bill* attribuisce poi all'esecutivo federale ampio margine d'intervento sui contenuti, prevedendo che l'autorità governativa possa disporre l'interruzione o la modifica di trasmissioni (anche quando il contenuto in questione sia, ad esempio, una critica al governo stesso). Non è invece prevista, stando alla bozza, alcuna autorità indipendente di appello contro le decisioni dell'esecutivo, con evidenti rischi di conflitto di interessi: il governo diventerebbe arbitro delle lamentele su programmi d'inchiesta o *talk show* politici, che magari lo mettono in cattiva luce.

Questo testo del 2023 è sembrato riprendere lo "spirito" di un vecchio *Broadcasting Bill* del 2006, che già puntava a un Codice stringente sui contenuti, ma non venne approvato a causa di forti resistenze dell'industria e della società civile, timorose di un ritorno a una censura statale simile a quella imposta durante lo stato di emergenza nazionale, dichiarato da Indira Gandhi nel 1975-1977, quando serviva una licenza per trasmettere qualsiasi programma. Il *Broadcasting Bill* del 2023, aggiornato all'epoca *streaming*, si inserisce chiaramente in un contesto

¹²⁹ Bisognerà verificare la puntuale declinazione della norma per evitare di cadere in una forma di autocensura obbligatoria, finalizzata a prevenire sul nascere potenziali violazioni, ma che potrebbe violare la libertà di espressione e burocratizzare la produzione di notizie.

dell'informazione molto diverso, ma la domanda di fondo resta la stessa: quanta autonomia è opportuno mantenere per i *media* e quanta supervisione pubblica è necessario introdurre? Allo stato attuale, il testo resta ancora in via di definizione: a inizio 2024 è uscita l'ipotesi di una modifica per escludere i *social media* dalla definizione di *broadcast* e di una possibile revisione delle parti più controverse.

Il *Digital India Bill* (DIB) è un progetto ancora più ambizioso¹³⁰, presentato da Rajeev Chandrasekhar, ex Ministro per *Electronics and Information Technology*, come «*a new law for a new generation*». L'idea di base è quella di rimpiazzare completamente l'IT Act, che è datato e nato per altro scopo, con una disciplina moderna, che copra tutti gli aspetti del mondo *online*: dai *social media* alla cybersicurezza, dai nuovi servizi digitali (IA, *blockchain*, etc.) alla moderazione dei contenuti, integrandosi con la normativa in vigore sui dati personali e sulle telecomunicazioni digitali. Il governo ha indicato alcuni obiettivi chiave per il DIB: a) assicurare una rete Internet «*open, safe, trusted & accountable*»; b) tutelare i diritti degli utenti e ridurre i rischi *online*; c) promuovere l'innovazione tecnologica e la crescita economica digitale. Più concretamente, è in discussione una riforma del concetto di *safe harbour* per gli intermediari: l'esecutivo sta valutando se mantenere l'immunità generale di cui godono oggi le piattaforme (cioè la sezione 79) o limitarla a certe categorie o, comunque, condizionarla con requisiti più stringenti. Se, infatti, il legislatore parte dalla convinzione che non tutti gli attori *online* siano uguali, allora la conseguenza possibile è che forse non tutti meritano lo scudo dalle responsabilità. Si prospetta, dunque, una classificazione diversificata degli intermediari: ad esempio, separare *social network*, motori di ricerca, *e-commerce*, *provider* di *cloud*, etc., modulando per ciascuno obblighi e responsabilità¹³¹.

Questo intento riformatore nasce dalla convinzione governativa che le *Big Tech* abbiano troppo potere sulla comunicazione politica e possano orientare il discorso pubblico, decidendo chi bannare o cosa promuovere via algoritmo senza sufficiente trasparenza e *accountability*. Quindi, il *Digital India Bill* è ideato come risposta a questo fenomeno e prevede obblighi specifici per gli algoritmi (anche la possibilità per gli utenti di scegliere *feed* non algoritmici) e nuovi vincoli per le piattaforme. Un altro ambito in cui interviene il DIB riguarda la definizione e la repressione dei nuovi reati *online*: si è parlato esplicitamente di *weaponisation of misinformation*¹³² e il governo ha annunciato che non sarà tollerato l'uso strumentale della disinformazione con il pretesto della libertà di parola. Questa intenzione

¹³⁰ Il DIA si inserisce in un più ampio sforzo di *governance* digitale: il governo ha già approvato il *Digital Personal Data Protection Act, 2023* (DPDP), che regola *privacy* e dati (con estese eccezioni per il governo in nome della sicurezza) e il *Telecom Bill, 2023*, che ha sostituito il desueto *Indian Telegraph Act, 1885*, e incluso anche i servizi di comunicazione via Internet, come WhatsApp, tra le licenze delle telecomunicazioni. Si veda A. Jain, A. Anand, *Tracing the Constitutional Journey of Data Privacy in India: From Puttaswamy to the Draft DPDP Rules, 2025*, (2 June 2025), disponibile su <http://dx.doi.org/10.2139/ssrn.5283949>.

¹³¹ Potenzialmente, potrebbero esserci esclusioni dal *safe harbour* per soggetti che di fatto hanno un ruolo attivo sul contenuto (ad esempio *fact-checkers* o piattaforme editoriali).

¹³² Comunicato del MeitY di maggio 2023.

lascia intendere l'introduzione di reati specifici per chi crea o diffonde volontariamente *fake news* dannose, magari con una graduazione delle sanzioni. Tra gli altri comportamenti sanzionati vi sono *cyberstalking*, *cyberbullying*, *doxxing*, furto di identità *online*¹³³. Da tempo si dibatte poi sulla possibilità di creare un meccanismo originale di risoluzione delle controversie digitali, che potrebbe assumere la forma di Tribunali o arbitri specializzati in dispute *online*, al fine di garantire rimedi celeri ai cittadini e sviluppare una giurisprudenza *cyber* in tempi rapidi¹³⁴.

In conclusione, va ricordato che al momento non esiste in India un regolatore unico delle comunicazioni sul modello britannico di *Ofcom* e la stessa *Broadcasting Authority* appare nelle bozze come un *advisory council* sotto la sfera del governo e con funzioni di indirizzo, ma senza poteri sanzionatori. Anche le recenti spinte dell'esecutivo sembrano privilegiare il controllo diretto da parte dei Ministeri, più che la delega a organismi autonomi: lo si è visto con i GAC e con la tendenza a portare sotto il MIB i poteri su *digital news* e OTT, anziché creare un'*authority* terza. In futuro, il *Digital India Bill* potrebbe prevedere una *Digital India Authority* o agenzia simile, ma non è ancora definito. Nelle risposte a delle interrogazioni parlamentari¹³⁵, il governo ha sottolineato di volere un approccio leggero ma efficace: è ragionevole ritenere che preferisca *board* governativi di appello al posto di una grande *authority*, sebbene l'industria e gli esperti sollecitino un corpo indipendente, senza un forte condizionamento politico.

12. Uno Stato forte nello spazio digitale

La crescita esponenziale della comunicazione digitale di massa ha, senza dubbio, indotto lo Stato indiano ad ampliare il proprio ruolo di supervisione e di intervento¹³⁶. Da una fase iniziale di *laissez-faire* in cui Internet era

1579

¹³³ Molti di questi atti oggi sono in realtà già puniti per vie traverse (ad esempio il *doxxing* ricade nella violazione della *privacy* e il bullismo tra le molestie), ma questo disegno di legge potrebbe tipizzarli espressamente e predisporre meccanismi semplificati per ottenere giustizia (ad esempio ordini di rimozione rapida, tribunali o *app* dedicate).

¹³⁴ L'ipotesi trova riscontro anche nel documento di consultazione pubblica sul *Digital India Bill*, presentato dal MeitY nel marzo 2023, in cui il governo indicava tra gli obiettivi del futuro meccanismo giudiziario quello di «*deliver timely remedies to citizens, resolve cyber disputes, develop a unified cyber jurisprudence*»; si veda L. Dobbertstein, *India floats dedicated tribunal to handle internet offences*, in *The Register* (13 March 2023).

¹³⁵ Il *Ministry of Information and Broadcasting* (MIB) ha confermato in sede parlamentare che il *Broadcasting Services (Regulation) Bill* non è stato abbandonato, ma rimane formalmente all'esame del governo. In risposta a un'interrogazione presso il *Rajya Sabha* del 5 dicembre 2025, è stato chiarito che il disegno di legge è attualmente oggetto di un processo di revisione sostanziale, successivo a consultazioni approfondite e riservate con *stakeholder* del settore radiotelevisivo, digitale e delle piattaforme OTT, e che le osservazioni raccolte hanno reso necessario un riesame complessivo dell'impianto originario del testo prima di una eventuale presentazione in Parlamento.

¹³⁶ Sul tema generale, si vedano R.K. Mahapatra, *Digital Sovereignty: Navigating Foreign Influence on India's Internet and Ensuring Online Safety*, New Delhi, 2024; D. Broeders, F. Cristiano, M. Kaminska, *In Search of Digital Sovereignty and Strategic*

considerato come uno spazio libero, si è passati negli ultimi anni a una crescente “statalizzazione” del cyberspazio in cui il governo, spesso con la giustificazione di proteggere la sicurezza nazionale e l’ordine pubblico, ha accumulato strumenti per monitorare, regolare e talvolta censurare i contenuti *online*. Le nuove regole e i progetti di legge in discussione confermano una tendenza all’estensione della sorveglianza e del controllo su contenuti e piattaforme digitali, prospettando il rischio di deriva autoritaria e di compressione eccessiva delle libertà civili sotto il peso di un esecutivo sempre più pervasivo nel discorso pubblico.

Una prima linea di tendenza è, infatti, proprio la centralizzazione del controllo dei contenuti nelle mani del governo. Come si è visto, invece di creare autorità indipendenti, l’esecutivo ha preferito istituire meccanismi dove il governo stesso è arbitro ultimo delle controversie: il meccanismo di reclamo per i contenuti digitali editoriali ne è un esempio lampante, dato che il terzo livello è affidato all’*Inter-Departmental Committee* (IDC), istituita dal MIB, a chiusura del sistema. Sebbene il governo non possa al momento ricorrere alla *Fact Check Unit*, ancora bloccata dalla Corte Suprema, anche questo strumento sembra rispondere alla medesima logica, attribuendo all’esecutivo la facoltà unilaterale di bollare una notizia come falsa e conseguentemente farla rimuovere. Questo istituto configura un potenziale conflitto di interessi: un governo potrebbe benissimo censurare informazioni vere ma scomode semplicemente etichettandole come *fake news*, diventando al tempo stesso giudice e boia nei confronti dei *media*, eliminando di fatto il ruolo di filtro imparziale che spetterebbe al potere giudiziario o ad organismi terzi. Questa concentrazione di funzioni, pertanto, non sembra coerente con la logica dei *checks and balances* e potrebbe portare ad abusi di potere, volti a silenziare il dissenso¹³⁷.

Un secondo trend è rappresentato dall’espansione della sorveglianza digitale. Le nuove norme hanno accentuato la possibilità di tracciare e identificare gli utenti: la regola sulla *traceability* dei messaggi – anch’essa al momento non applicata – è stata approvata con motivazioni nobili (lotta a pedofilia, terrorismo, etc.), ma comporta potenzialmente la fine dell’anonimato *online* e della crittografia *end-to-end* per milioni di cittadini. Associazioni come *Internet Freedom Foundation* avvertono che l’obbligo di tracciare l’origine dei messaggi apre le porte a violazioni della *privacy* di massa e rende vulnerabili dati sensibili, in contrasto con la

Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions, in 61 *Journal of Common Market Studies* 5 (2023); S. Mangiameli, *La sovranità digitale*, in *Dirittifondamentali.it*, 3 (2023); M. Musoni, P. Karkare, C. Teevan, E. Domingo, *Global approaches to digital sovereignty: Competing definitions and contrasting policy*, in *ECDM* (May 2023); M. Proietti, A. Venanzoni, *La sovranità digitale tra sicurezza nazionale e ordine costituzionale*, Pisa, 2023; A. Chander, H. Sun, *Sovereignty 2.0*, in *Georgetown Law Faculty Publications and Other Works*, 2404 (2021); L. Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, 33 *Philosophy and technology* 369, 371 (2020); A.K. Woods, *Litigating Data Sovereignty*, 128 *Yale Law Journal* 328, 360 (2018).

¹³⁷ La critica principale, è, infatti, quella di mancanza di indipendenza: gli organismi preposti a simili funzioni dovrebbero essere composti principalmente da membri non governativi (giudici, società civile), per non trasformarsi in strumenti di controllo dell’esecutivo sulle critiche a sé stesso.

giurisprudenza (*Justice K.S. Puttaswamy v. Union of India*, 2017). Analogamente, i poteri di *data retention* e richieste di dati utenti (rafforzati anche dal *Digital Personal Data Protection Act*, 2023) fanno temere una sorveglianza digitale sempre più pervasiva: un esempio concreto è l'istituzione della piattaforma *Sahyog* dal Ministero degli Interni nel 2024, come portale che centralizza e automatizza l'invio di ordini di rimozione alle piattaforme *online*. Questo strumento, integrato con l'*Indian Cyber Crime Coordination Centre*, consente a varie agenzie governative di emettere velocizzare e moltiplicare le richieste di blocco ai *provider*. L'esecutivo sta di fatto investendo in infrastrutture tecnologiche per controllare la rete, costruendo progressivamente uno stato di sorveglianza in cui, ad esempio, i dati personali potrebbero in futuro essere raccolti e usati dal governo sempre più liberamente anche per profilazioni in periodo elettorale.

Un terzo elemento è dato dalla spinta a uniformare e normalizzare la censura preventiva. Con il *Cinematograph (Amendment) Act*, 2023 ad esempio, il governo ha introdotto punizioni più dure per le copie non certificate e ha segnalato zero tolleranza per i film "anti-nazionali". Nel *Broadcasting Bill*, 2023 si propone che ogni contenuto passi da un *Content Evaluation Committee* interno, di fatto un filtro editoriale anticipato imposto per legge. Questo *pre-screening* generalizzato indica la volontà di evitare a monte che contenuti "sgraditi" raggiungano il pubblico e incoraggerà l'autocensura: sapendo che un proprio contenuto potrebbe non superare i controlli, editori e creatori si limiteranno da soli nelle scelte espressive. Questo è un problema fondamentale: anche senza censura diretta, la semplice esistenza di regole punitive porta i *media* a evitare argomenti controversi (cd. *chilling effect*) e già oggi alcune redazioni *online* indiane scelgono con cautela come coprire certi temi (ad esempio, movimenti separatisti o critiche alle forze armate) per non incappare in blocchi o denunce.

La società civile indiana ha reagito con forza e vi sono state prese di posizione pubbliche: l'*Editors Guild of India* ha attaccato la norma sulla *Fact Check Unit*, definendola come una misura che dà al governo poteri di censura senza precedenti e soffoca il diritto all'informazione. Organizzazioni digitali come *Internet Freedom Foundation* (IFF) e *MediaNama* stanno pubblicando analisi per evidenziare i poteri eccessivi concessi all'esecutivo e l'IFF ha parlato di stato di eccezione digitale permanente, dove il governo può etichettare chiunque come nemico digitale e silenziarlo in modo discrezionale. Il *Carnegie Endowment for International Peace* in uno studio comparativo su India e USA ha osservato che l'India sta imboccando una strada di repressione legale dei *social media*. Critiche simili giungono da organizzazioni globali: *Freedom House* nel suo Report *Freedom on the Net* ha classificato l'India come "parzialmente libera" con trend negativo, citando l'uso eccessivo di *shutdown* e l'azione punitiva contro i critici *online*.

Nel complesso, è possibile evidenziare un *pattern*: strumenti nati per scopi legittimi vengono applicati in modo sempre più estensivo e opinabile. Questo slittamento concettuale fa temere che l'esecutivo possa superare i confini di ragionevolezza garantiti dall'art.19(2) e le attese sentenze della Corte Suprema e della *Delhi High Court* allo stato attuale rappresentano il

mezzo più incisivo per porre un freno al governo. In conclusione, l'espansione del ruolo dello Stato nel digitale è innegabile: negli ultimi anni c'è stata un'accelerazione regolatoria con l'introduzione di regole via via più stringenti, che però non hanno istituito organismi indipendenti, mantengono scarsa trasparenza (molti ordini di blocco sono segreti e non possono essere sindacati facilmente), non garantiscono sempre il rispetto del principio di proporzionalità (*shutdown* prolungati, *ban* totali di *app* invece che interventi mirati), e consentono talvolta di colpire la libertà di stampa e il dissenso politico sotto pretesti generici come *fake news* o ordine pubblico. Il timore è che l'esecutivo possa usare questi poteri soprattutto per controllare la narrazione politica, specialmente in periodi elettorali. Alcuni analisti parlano di deriva verso il *digital authoritarianism*¹³⁸: l'India resterebbe, nel complesso, una democrazia, ma adotta strumenti e retorica tipici di regimi autoritari nel controllo di Internet.

Il confronto con il quadro europeo, assunto come riferimento euristico in apertura del presente lavoro, conferma le differenze strutturali inizialmente ipotizzate: laddove l'UE ha progressivamente costruito un sistema di regolazione affidato ad autorità indipendenti e fondato su strumenti normativi trasparenti come il DSA e la TTPA, l'India sta percorrendo una traiettoria opposta, accentrando i poteri di regolazione nell'esecutivo e privilegiando il controllo diretto sui contenuti. L'attuale fase di riforma, ancora in discussione, rappresenta un'occasione per invertire questa tendenza e avvicinarsi a un modello più bilanciato, in cui la tutela della libertà di espressione sia maggiormente presidiata da istituzioni terze e indipendenti.

L'interrogativo di fondo resta: come conciliare la necessità dello Stato di proteggere i cittadini dagli aspetti negativi del web con l'esigenza democratica di preservare uno spazio libero di critica e informazione? L'India sta cercando un punto di equilibrio, ma attualmente le linee di tendenza suggeriscono uno spostamento del pendolo verso un ruolo più pronunciato del governo. È allora compito delle istituzioni democratiche

¹³⁸ Si vedano U. Kashyap, P. Singh, M. Javed, L. Jee, S. Singh, *The Dynamics Of Cyber Nationalism In India's Multicultural Context: Social Media As A Catalyst For Conflict*, in 32 *Tpm – Testing, Psychometrics, Methodology in Applied Psychology* S8 (2025); M. Lucaccini, *Digital Authoritarianism: ICT-enabled Repression Across Regime Types*, in *Proceedings of the Joint National Conference on Cybersecurity (ITASEC & SERICS)*, Feb. 2025; T. Roberts, M. Oosterom, *Digital authoritarianism: a systematic literature review*, in 31 *Information Technology for Development* 4 (2025); M. Lucaccini, *Geopolitical Dynamics of Digital Authoritarianism: Emerging Global Challenges*, in *Working Paper Series SOG-WP6/2024* (May 2024); C. Codreanu, *Using and exporting digital authoritarianism: Challenging both cyberspace and democracies*, in 16 *Europolity* 1 (2022); A. Dal, E. Nisbet, *Walking through firewalls: Circumventing censorship of social media and online content in a networked authoritarian context*, in 8 *Social Media + Society* 4 (2022); M. Taylor, *China's digital authoritarianism: A governance perspective*, London, 2022; S. Feldstein, *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*, Oxford, 2021; E. Frantz, A. Kendall-Taylor, J. Wright, *Digital repression in autocracies*, in *VDEM Using Working papers* (Mar. 2020); A.R. Gohdes, *Repression Technology: Internet Accessibility and State Violence*, in 64 *American Journal of Political Science* 3 (2020); M. Michaelsen, *Transforming threats to power: The international politics of authoritarian internet control in Iran*, in *International Journal of Communication*, 12 (2018); M. Michaelsen, M. Glasius, *Authoritarian practices in the digital age – Introduction*, *ivi*.

(Parlamento, Corte Suprema, opinione pubblica) evitare che la situazione degeneri e garantire che l'India digitale rimanga plurale, aperta e rispettosa dei diritti.

Davide Ragone
Sapienza Università di Roma
davide.ragone@camera.it