

Digital Governance and Rights in South Asia and the Path Forward

2026
Update



Table of Contents

Acknowledgment	3
Executive Summary	4
Introduction	4
Bangladesh	6
India	9
Nepal	11
Pakistan	13
Sri Lanka	16
Thematic Overlaps	18
Policy Considerations	20
Conclusion	22
References	22

Acknowledgment

This paper is the 2026 update of [Digital Governance and Rights in South Asia, and the Path Forward](#), first published in February 2025. This update is intended as an annual record of how technology governance and accountability are changing across the region, from digital public infrastructure to platforms, in one of the fastest growing parts of the world.

This edition was written collaboratively. The paper has

been edited and compiled by Shumaila H. Shahani, with country sections contributed by Priya Ahsan Chowdhury (Bangladesh Legal Aid and Services Trust) for Bangladesh, Nilay Shah and Sameer Bajaj for India, Monisha Choudhary (Body & Data) for Nepal, Farieha Aziz (Bolo Bhi) for Pakistan, and Prihesh Ratnayake, Sivashanthi Sivalingam and Devmini Bandara (Factum) for Sri Lanka.

Executive Summary

Across Bangladesh, India, Nepal, Pakistan, and Sri Lanka, control over the digital sphere is concentrating in the executive. This edition finds it happening through three channels at once: obligations imposed by ministries rather than legislatures, as in India's successive IT Rules amendments; courts brought under political influence, as in through Pakistan's 26th and 27th constitutional amendments; and digital identity and service platforms that the state alone designs, runs, and makes compulsory. Shutdowns remain the bluntest instrument with South Asia accounting for 91 of the 313 recorded worldwide in 2025.

Two things complicate that picture. Nepal showed that the public can still reverse repressive measures, forcing the withdrawal of the Social Network Bill after a youth-led uprising, though at the cost of at least 19 lives on the first day alone. And Bangladesh's post-2024 reforms removed most inherited speech offences, only for draft amendments in September 2026 to propose reviving them. Neither reversal is secure.

Meanwhile, the actors best placed to hold the line are weaker. Technology companies continue to underinvest in content moderation in the region's languages. Civil society remains the main source of accountability but is working with sharply reduced resources after the 2025 collapse in donor funding, and, in Pakistan, with public interest litigation effectively closed off

The paper sets out what should change. Governments should legislate through parliament rather than executive rule, repeal vague speech offences, require independent authorization for surveillance and shutdowns, and protect judicial independence. Governments and the development partners financing

digital public infrastructure should put data protection and redress mechanisms in force before these systems scale, guarantee offline alternatives, and consult before rollout. Technology companies should resource local-language moderation in proportion to their users, publish what governments ask of them, and build standing channels with regional civil society. Funders should provide flexible core support that reaches new, youth-led forms of organizing as well as established organizations.

The paper updates each country section through August 2026, revisits the five themes identified in 2025 and adds a sixth on techno-solutionism and state digital infrastructure, and assesses which routes to accountability held up over the year. Courts proved an important but unreliable check, public pressure the most decisive and the least durable, and civil society coordination valuable but confined within national borders.

Introduction

When the first edition of this paper was published in February 2025, it argued that South Asia's digital rights landscape was being shaped by two pressures at once. States were using technology to expand their control, and governance models borrowed from the Global North were being imposed without regard for local realities. It called for a regional coalition of civil society to respond, a call that led to the launch of the South Asians for Digital Rights (SADR) coalition in June 2025 (Tech Global Institute, 2025). This 2026

update returns to that argument a year on. The past year confirmed the diagnosis, but it also changed the picture in three ways.

First, the public pushed back. In September 2025, Nepal's ban on 26 social media platforms triggered a youth-led uprising that forced the resignation of Prime Minister KP Sharma Oli (Business Standard, 2025) and, in February 2026, led to the withdrawal of the Social Network Bill (Kathmandu Post, 2026). Elections in March 2026 then produced the world's youngest cabinet (Chakraborty, 2026). It was the clearest demonstration yet that attacks on digital freedoms can mobilize people at scale. It also showed the cost: security forces killed at least 19 protesters on the first day of the movement alone (Al Jazeera, 2025).

Second, the institutions meant to check state power narrowed further. In Pakistan, the 26th and 27th constitutional amendments brought the judiciary closer to executive and military control (Chatham House, 2025). New speech offences under the Prevention of Electronic Crimes Act have produced 17-year prison sentences for two human rights lawyers (Front Line Defenders, 2026). In India, successive amendments and draft amendments to the IT Rules have turned executive rule-making into a de facto omnibus framework governing AI, content moderation, and user rights, bypassing the parliamentary oversight the IT Act requires (SFLC.in, 2026). In Bangladesh, the post-2024 transition produced new cyber and data protection laws, yet proposed amendments to the new cyber law already revive speech restrictions associated with its predecessors (Mahmud, 2026). Shutdowns remain routine: in 2025, South Asia accounted for 91 of the 313 internet shutdowns recorded worldwide (Access Now, 2026).

Third, beyond its regulatory function, the state has taken on a developmental one. Every country examined has adopted or is drafting a national AI policy. Each is also expanding state-run platforms for digital identity, payments, and public services: Pakistan's Digital Nation Act, Sri Lanka's Unique Digital Identity (SLUDI) and GovCloud, Nepal's Nagarik App, and India's continued export of its digital public infrastructure (DPI). These systems promise inclusion in a region where 46% of the population now uses mobile internet and over 90% have access to a 4G or 5G smartphone (GSMA, 2026). But they are arriving ahead of the data protection, oversight, and redress mechanisms needed to govern them.

The external environment has shifted too. The United States, whose regulatory choices had shaped

platform governance worldwide and whose funding had sustained much of the region's digital rights work, cut at least \$1.7 billion in freedom of expression programming in 2025 (ARTICLE 19, 2026). Other donors have also pulled back: official development assistance from OECD DAC member countries and associates fell by 23.1% in 2025, the largest annual drop on record, with 26 of the 34 DAC members reducing their aid — including all top providers: Germany, the United Kingdom, Japan, and France, alongside the United States (OECD, 2026). External influence on the region's digital governance is therefore now exercised less through funding and more through regulation, and here the European Union's reach continues to grow. The Brussels Effect made the General Data Protection Regulation a template for data protection across jurisdictions (Bradford, 2020), and the EU's Artificial Intelligence Act, which entered into force in 2024, may extend that influence to AI (European Union, 2024). Closer to home, the Delhi Effect described in the first edition has deepened, and DPI has become a regional norm (Asian Development Bank, 2025). India's IT Rules, 2021 and Digital Personal Data Protection Act, 2023 served as legislative templates for its neighbors (Mahmood, 2022). Its Digital Personal Data Protection Rules, 2025 and its rules on synthetically generated content are likely to do the same.

What has not changed matters just as much. Technology companies, which have long been headquartered in the Global North (Tworek, 2021), still underinvest in content moderation in the region's languages. Fewer than 0.1% of the notes in X's Community Notes program are written in South Asian languages, although the region is home to roughly a quarter of the world's population (Center for the Study of Organized Hate, 2025), and Meta's 2026 job cuts extended to its integrity teams (Shahid, 2026). Civil society organizations remain the region's main source of accountability, working through legislation, litigation, investigation, and user empowerment (Tech Global Institute, 2024), but they now do so with fewer resources (Tech Global Institute, 2025) and, in countries such as Pakistan, fewer legal avenues. South Asian governments have long cooperated on trade, energy, and security through SAARC and smaller sub-regional arrangements, but official regionalism has largely stalled (Jacob, 2024), and there is still no intergovernmental mechanism for digital rights, despite the region's significant engagement with content takedown and user data requests to digital intermediaries. Civil society has begun to fill that gap through coalitions such as South Asians for Digital

Rights (SADR) and Digital Accountability Collective South Asia (DACSA), which now brings together organizations and digital rights defenders from South Asia.

This update follows the structure of the first edition. The country sections have been revised to reflect developments through August 2026. The thematic overlaps have been revisited, with a sixth theme added on techno-solutionism and state digital infrastructure. The policy considerations build on the principles set out in the first edition and reassess the routes to accountability it proposed.

Bangladesh

Bangladesh's approach to technology regulation has evolved substantially over the past two decades, reflecting a shift from facilitating digital development towards increasingly extensive state regulation of online spaces. The regulatory foundation was established through the Bangladesh Telecommunication Act, 2001, as amended from time to time, most recently in 2026, which created the Bangladesh Telecommunication Regulatory Commission (BTRC), followed by the National ICT Policy, 2002, which positioned information and communication technology as a driver of economic growth and public service delivery. Parliament subsequently enacted the Information and Communication Technology (ICT) Act, 2006, under the Bangladesh Nationalist Party government, introducing the country's first statutory framework addressing electronic records, electronic signatures, and digital offences including vague speech offences.

Following the Awami League's return to power in 2009, the Digital Bangladesh agenda accelerated the expansion of digital infrastructure, e-governance, financial inclusion, and internet connectivity. This period also saw the nationwide rollout of biometric SIM registration, expansion of the biometric National Identity (NID) system, rapid growth of mobile financial services, and expansion of the digital economy through increased smartphone adoption and broadband infrastructure. By August 2026, Bangladesh had more than 137 million internet subscriptions (The Financial Express, 2026).

At the same time, the expansion of digital governance was accompanied by an increasingly restrictive framework for online expression. The

2013 amendments to the ICT Act, particularly section 57, were widely criticised for enabling arrest without warrant for broadly framed online speech offences concerning, among others, false, offensive, defamatory, religiously hurtful, or prejudicial content (Human Rights Watch 2018). In 2018, these provisions were replaced by the Digital Security Act (DSA), which retained and expanded several speech-related offences, including through further vaguely worded provisions, while permitting arrest without warrant. The DSA also established the Digital Security Agency and Digital Security Council, both government-appointed bodies, and gave the former significant powers relating to initiating content removal and blocking.

Civil society, journalists, the general public, politicians, activists, and international human rights bodies, including the UN Special Rapporteur on freedom of expression and the Office of the High Commissioner for Human Rights (Khan, 2021, 2023, 2025; UN High Commissioner for Human Rights, 2022), repeatedly criticised the DSA for facilitating arbitrary arrests, pre-trial detention, and prosecutions of journalists, human rights defenders, political opponents, and other social media users under vaguely framed speech offences.

The DSA was replaced by the Cyber Security Act (CSA) in 2023, shortly before the January 2024 national elections. Although the CSA reduced certain penalties and made other amendments, all of the DSA's speech-related provisions were retained, prompting continued criticism that the legislative changes did not address the underlying concerns about vague criminalisation of online expression.

The events surrounding the July–August 2024 uprising, which culminated in the removal of the Awami League government amid extensive state facilitated violence and bloodshed, further exposed the extent of executive control over digital infrastructure. During the protests, authorities imposed nationwide internet shutdowns, mobile broadband suspensions, and social media restrictions. The shutdowns affected access to banking, health and other essential online services (OHCHR, 2025). There has also been an extensive surveillance architecture involving telecommunications and video-camera surveillance, and surveillance information was used to monitor, target, and abduct perceived critics and dissenters including lead student coordinators for the uprising (OHCHR, 2025).

Following the political transition in August 2024, the Interim Government acknowledged the need to reform the digital regulatory framework. Reform efforts subsequently moved beyond simply renaming existing

legislation. In 2025, the Interim Government adopted the Cyber Protection Ordinance (The Daily Star, 2025), repealing the CSA and removing most of the previous speech offences, while introducing a new speech offence concerning the publication or dissemination of material intended to spread religious or ethnic hatred (Cyber Protection Act, 2026, § 26; The Business Standard, 2025). Concerns were raised about the breadth and vagueness of some of the terms used in the new hate-related offence with scope for abuse (Transparency International Bangladesh, 2026). The Ordinance also introduced offences addressing forms of technology-facilitated harm, including sextortion, non-consensual dissemination of intimate images, online sexual harassment, and child sexual abuse material, including material created or edited using artificial intelligence. The framework was subsequently enacted by Parliament as the Cyber Protection Act, 2026.

The regulatory framework also expanded in 2026 beyond cybercrime regulation. The Bangladesh Telecommunication Act, 2001, was amended to make changes to the telecommunications regulatory framework, including provisions concerning interception and related regulatory powers. In the same period, Parliament enacted the Personal Data Protection Act, 2026, following the Interim Government's adoption of the Personal Data Protection Ordinance, 2025. The Act established a dedicated statutory framework for personal data protection, but concerns have been raised regarding broad exemptions for state authorities, the independence of data-governance institutions, and the adequacy of safeguards against excessive state access to personal data and surveillance (Afrin, 2025).

In September 2026, the government currently led by the Bangladesh Nationalist Party published the Draft Cyber Protection (Amendment) Act for an 8 working days' public consultation (BLAST, 2026), proposing to

reintroduce speech offences including defamation and maligning, and to add offences concerning rumours and misinformation. Criminal defamation already exists under the colonial era Penal Code, 1860, and was widely abused when adopted under the DSA and CSA.

Concerns have been raised that these proposed speech offences are broadly and vaguely drafted and carry disproportionate penalties. These concerns have been linked by rights groups (The Daily Star, 2026) to the history of section 57 of the ICT Act, the DSA and the CSA, which were criticised for vague speech offences and their use against journalists, activists and critics.

The draft also proposes institutional changes that would further increase executive representation within the cyber regulatory framework, including the addition of three ministers, the Cabinet Secretary, and the Secretary of the Ministry of Information and Broadcasting to the National Cyber Protection Council, and the removal of the Chairman of the National Human Rights Commission, currently the only member with an explicit human rights mandate. It further proposes expanded executive powers over content blocking and raises concerns regarding surveillance-related powers and the lack of independent oversight and meaningful judicial safeguards.

Taken together, these developments demonstrate an increasingly complex and fragmented technology governance framework, with regulatory authority distributed across multiple institutions. Although the Constitution guarantees freedom of expression under Article 39, and Bangladesh is a party to the ICCPR and other major international human rights treaties, concerns remain that broadly drafted criminal offences, extensive executive discretion over digital infrastructure and content, and limited independent oversight will continue to constrain the effective protection of digital rights.

TABLE 1 - RELEVANT TECH-RELATED POLICIES IN BANGLADESH

Law	Description
Bangladesh Telecommunication Regulation Act, 2001	● Established a commission (BTRC) to regulate telecommunication and internet service providers. ● Criminalises proposing or knowingly sending obscene, threatening, frightening or seriously insulting telecommunications messages, including certain communications used to collect money. ● Criminalises repeated telecommunication connections causing annoyance or harm and AI-enabled misuse of another person's voice, image, personal identifying, sensitive or biometric data. ● Prohibits intentional interception of conversations and surveillance using SIM or device-registration data. ● Grants the Ministry of Home Affairs and intelligence authorities authority to collect user data for national security, public order, and other vague grounds.
Cyber Protection Act, 2026	● Criminalises digital/electronic blackmail, sexual harassment, revenge pornography, sextortion and digital CSAM, including captured, edited, AI-generated and AI-edited material, with enhanced penalties where the victim is a woman or child. ● Empowers the Director General of the Cyber Shurokkha Agency to take measures or request BTRC in relevant matters to remove, relocate, or block content that threatens cybersecurity, and empowers law enforcement to seek the same measures through the DG where they have reason to believe content threatens national integrity, security, defence, public order, incites violent religious or ethnic hatred, or instructs criminal activity. It requires BTRC or the relevant authority of the Information and Communication Technology Division of the Government to implement such requests, subject to Cyber Tribunal's approval within three days, failing which the content must be restored.
Pornography Control Act, 2012	● Criminalizes possession, distribution, production, and use of pornography, including child pornography and content likely to arouse sexual desire. ● Does not regulate deepfake pornography or provide measures to remove or stop distribution of content deemed illegal under the law.
[Draft] Regulations for Digital and Social Media Platforms 2021	● Introduces intermediary liability on digital, social media, and over-the-top (OTT) platforms, requiring local registration, content moderation, and a complaints system. ● Expand BTRC's authority for content removal. ● Risk restricting access to information and communication and limiting freedom of expression.
[Draft] Over the Top Content Based Service Provision and Management Policy, 2022	● Proposes banning OTT platforms from offering news, talk shows, and current affairs, and restricting broad categories of prohibited content. ● Requires platforms to categorize content by age and establish mechanisms for handling complaints. ● Mandates OTT platform registration with the Information Ministry and grants BTRC authority to block or remove prohibited content.
Personal Data Protection Act, 2026	● Introduces lawful processing, consent requirements, data fiduciary obligations, data subject rights, security safeguards, retention limits and regulatory oversight. ● Covers unlawful disclosure of personal and location data.

India

India's tech regulatory framework is centred on achieving digital sovereignty, with an emphasis on control over data, autonomy, and security (Lalani, 2024). Packaged as public-first through its Digital Public Infrastructure (DPI) and now its democratising AI mission, there are growing concerns around surveillance and private capture of public functions. With 920 internet shutdowns in the last ten years, significant concerns are arising due to the concentration of state power, the erosion of individual privacy and the loss of digital rights (Bhalla, 2026).

Governance issues are exacerbated due to the fragmented nature of departments and state policy. The Union Budget 2026-27's weak commitments to equitable telecom access and cyber safety, coupled with overemphasis on AI infrastructure, reflects the absence of a clear strategy for digital safeguards and equitable growth (Internet Freedom Foundation, 2026). The Digital Personal Data Protection Act, 2023, which sets a baseline for data privacy, grants the government extensive authority to control data flows and enforce data localisation, raising concerns about state surveillance. The newly notified Digital Personal Data Protection Rules, 2025 (DPDPR) further compromise press freedom and weaken the Right to Information (News

Laundry, 2025). Regulatory development at the state level with the Karnataka Hate Speech and Hate Crimes (Prevention) Bill and the Telangana Hate Speech and Hate Crimes Prevention Bill enables officials to take "preventive action", indicating a shift from regulating harm to policing anticipated events and risking further bypassing the nation's limited constitutional safeguards (Sinha, 2026). The Ministry of Electronics and Information Technology (MeitY)'s recent emergency action against the cloud-based messaging platform Telegram, along with its subsequent validation by the judiciary, reiterates the consolidation of power in state authority (Sinha, 2026). Amendments to the IT Rules in February 2026 and Draft Amendments in March 2026 also significantly expand the powers of the Ministry, usurping Legislative function while being unchecked by review and Parliamentary discussion. This solidifies a trend of overreach, where the IT Rules essentially function as an omnibus legislation, governing AI, content moderation, intermediary liability, gaming, media reporting, and user rights (SFLC.in, 2026).

Each new regulation revises and reframes concepts from earlier laws while consistently maintaining vague language. Although often defended as necessary for adapting to emerging technologies, this ambiguity serves as a tool to shield the government from accountability. Instead of introducing concrete safeguards, these laws frequently postpone meaningful oversight to future legislative revisions.

TABLE 2 - RELEVANT TECH-RELATED POLICIES IN INDIA

Amendment / Policy Update	Core Changes Introduced
IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023 (Fact-Check Unit)	Empowered the Central Government to notify a Fact-Check Unit (FCU) to identify “fake, false, or misleading” content about “any business of the Central Government,” with loss of safe harbour for non-compliant intermediaries
Digital Personal Data Protection Act, 2023 — enactment	Enacted 11 August 2023; substantive provisions held in abeyance pending Rules
Telecommunications Act, 2023 — phased commencement	Ss. 1–2, 10–30, 42–44, 46–47, 50–58, 61–62 effective 26 Jun 2024; Ss. 6–8, 48, 59(b) effective 5 Jul 2024
Telecommunications (Telecom Cyber Security) Rules, 2024	First rules under the new Telecom Act; mandate SOC, telecom cyber-security policies, and government power to demand traffic/ other data from telecom entities
IT (Intermediary Guidelines) Amendment Rules, 2025 — Synthetic/Deepfake Content	Defines “synthetically generated information”; mandates permanent visible labelling (≥10% of frame/duration) and metadata/traceability for AI-generated content; requires SSMIs (5M+ users) to obtain user declarations and verify them via “reasonable and proportionate technical measures”
Digital Personal Data Protection Rules, 2025	Operationalises the Act: staggered/phased compliance timeline (up to 18 months for most obligations); Significant Data Fiduciary (SDF) category with mandatory annual DPIA + independent audit; two-stage breach notification (Board immediately, Data Principals within 72 hours); verifiable parental consent via DigiLocker for processing children’s data with a ban on behavioural tracking/profiling of minors; digital, portal-based Data Protection Board with TDSAT appellate jurisdiction
Telecommunications (Telecom Cyber Security) Amendment Rules, 2025	Introduces “Telecommunication Identifier User Entities” (TIUEs) — extends telecom-style cyber obligations to any non-licensee using phone numbers as identifiers (banks, fintechs, e-commerce, ride-hail, OTT/messaging); creates centralised Mobile Number Validation (MNV) platform and IMEI blacklist/device-control powers
India AI Governance Guidelines, 2025	Adopts seven “sutras” (Trust, People First, Innovation over Restraint, Fairness & Equity, Accountability, Understandable by Design, Safety/Resilience/Sustainability) across six pillars; explicitly rejects a standalone AI statute in favour of amending existing sectoral laws (IT Act, DPDP Act, Consumer Protection Act) to cover AI harms
RBI “Framework for Responsible and Ethical Enablement of AI” (FREE-AI) Committee Report	Seven guiding sutras and 26 recommendations across six pillars for AI adoption in regulated financial entities; calls for board-approved AI policies, AI inventories, and incident reporting
Digital India Act (DIA) — draft/consultation	Proposed comprehensive overhaul: intermediary re-classification (beyond the binary “intermediary” concept), user harm categories, real-time content-blocking review, competition/open-internet provisions, and adjudicatory mechanism reform
Draft IT (Digital Code) Rules, 2026 (reported)	Reported proposal for age-based content classification for online platforms (akin to film/OTT certification), parental-control mandates, and content-descriptor labelling

Nepal

Since holding its first election as a federal democratic republic in 2017, Nepal's tech policy has lagged on account of low internet penetration, weak telecom infrastructure, and a stark digital divide (Lamichhane, 2022). This sits within a broader context of political instability, the lingering threat of monarchist reinstatement, and entrenched economic disparity, all of which have kept digital rights low on the national agenda.

The Constitution of Nepal, 2015, guarantees fundamental freedoms of expression and press, but enumerates 28 grounds for restricting them. These grounds are broader, vaguer, and more subjective than the national security, public order, public health, or morals standards set by the ICCPR (Human Rights Treaty Monitoring Coordination Centre, 2020). Former PM KP Oli's government wielded the Constitution and the *Electronic Transactions Act, 2008* to silence protestors, journalists, activists, and online critics, while the Telecommunications Authority and Ministry of Information and Communication Technology (MoICT) retain power to impose arbitrary platform bans. In November 2023, the *Telecommunications Act, 1997* was invoked to ban TikTok for alleged harm to "social harmony" (CNN, 2023). In 2025, MoICT used the *Directives for Managing the Use of Social Networks, 2023* to ban 26 platforms amid the anti-corruption "Nepo Baby" trend. This ban catalyzed the Gen-Z Movement of 2025 against systemic corruption and state repression, wherein security forces killed at least 19 protestors on the first day of the movement (Al Jazeera, 2025).

This ban on major social media platforms followed the tabling of the *Social Network Bill, 2025*, which sought to codify the 2023 directives, mandate platform registration, and sanction online harms, while also expanding executive overreach, criminalizing anonymous/pseudonymous accounts, and over-criminalizing online activity without clear intent standards. This Bill was withdrawn in February 2026 in the movement's aftermath.

Simultaneously tabled was the *Information Technology and Cybersecurity Bill, 2025*, which aimed to replace the Electronic Transactions Act by regulating cyberspace, protecting critical infrastructure, and criminalizing online harms. However, it proposed a government-controlled internet gateway that would

centralize traffic under state supervision, enabling censorship and surveillance, while leaving gaps in sensitive-data regulation and the environmental/communal impact of data infrastructure. It also criminalized vague, undefined dissemination of "obscene material", risking arbitrary interference and increasing surveillance of online spaces (Kathmandu Post, 2025). It lapsed after the House of Representatives was dissolved in September 2025 and awaits re-registration.

Despite criticism that Nepal's biometric national ID system disproportionately harms vulnerable populations and raises serious privacy risks (Opiah, 2024), it was integrated with voter ID cards in November 2025. This led to the addition of 200,000 new voter registrations but failed to include citizenship-affected individuals (Nationality for All, 2025), address data interoperability, and consider deepening concerns over increasing data consolidation and state control of sensitive data.

The post-movement elections in March 2026 were fought amid a surge of AI-generated content, mis/disinformation, and algorithmic amplification. Although the election brought in the world's youngest cabinet, it shifted the political landscape from tech-driven nationalism toward techno-solutionism—using digital fixes for structural problems rather than social restructuring. This is most notably visible in the expansion of e-government, particularly the *Nagarik (Citizen) App*, which requires registration via phone numbers registered under the legal names of users and stores critical identifying documents without accounting for the persistent digital divide. Compounding this, officials routinely use personal, monetized accounts rather than official channels for national announcements. Unregulated online incitement against activists amid rising communal tension threatens the rights to dissent, privacy, and protection for marginalized communities.

Nepal's digital revolution, AI-marred elections and consequent techno-optimist government have established digital governance as a core national agenda. However, growing data consolidation, pervasive surveillance, and executive discretion must be balanced with efforts to close the digital divide and enact binding laws protecting privacy, autonomy, and freedoms online, regulating harm, and enforcing platform accountability. Digital solutions cannot substitute social restructuring.

TABLE 3 - RELEVANT TECH-RELATED POLICIES IN NEPAL

Law	Description
Nepal Telecommunications Act, 1997	● Aims to regulate telecommunication services and licensing of operators. ● Grants Nepal Telecommunications Authority broad authority over telecommunications operators and communication services.
Electronic Transactions Act, 2008	● Sought to ensure security and authorization in electronic transactions and address cybercrimes like piracy, source code alteration, confidentiality breaches, and fraud. ● Criminalizes vaguely defined acts online offences, enabling arbitrary criminalization. ● Used to detain journalists and rights activists, and suppress online criticism of the government.
National Information and Communication Technology Policy, 2015	● Establishes Nepal's long term ICT development strategy by institutionalizing digital infrastructure, e-governance, digital literacy, and ICT-based public service delivery
National Penal (Code) Act, 2017	● Comprehensive criminal code covering both online and offline offenses, complementing Electronic Transactions Act in prosecuting cybercrimes ● Criminalizes eavesdropping, unauthorized photography, distorted-image publication, online defamation, extortion and digital forgery
Individual Privacy Act, 2018	● Protects individual personal information and private communications but does not establish a comprehensive data protection regime
National Cyber Security Policy, 2023	● Proposes a government-controlled internet and telecom gateway, inspired by China's Great Firewall and Cambodia's National Internet Gateway. ● Criticized for enabling surveillance and censorship, potentially fragmenting the internet and restricting free data flow.
Directives for Managing the Use of Social Networks, 2023	● Regulates social media use while promoting self-regulation among users and platforms on manipulated media, obscene content, unauthorized sharing, and deceptive calls. ● Criticized for targeting criticism and social media activities, while lacking clarity on issues like fake pages and accounts. ● Resulted in Nepal banning TikTok over hate speech concerns, later lifted after the platform complied with government-mandated content regulations.
National Artificial Intelligence Policy, 2025	● Sets out a state-led AI framework and creates a National AI Centre under the Ministry of Communication and Information Technology to promote, facilitate, and regulate AI.
Electronic Commerce Act, 2025	● Establishes a nationwide legal framework for online businesses and strengthens consumer protection. ● Criticized for broad administrative oversight for smaller sellers and increased regulatory burden on platforms.
Nagarik App (Operation and Management) Guidelines, 2025	● Operationalizes the Nagarik App as a multi-device service platform and, according to the Department of Information Technology, positions it as a gateway for 67 online government services. ● Raises concerns regarding concentration of identity, data, and service access in a single state gateway, and increase in cyber security vulnerabilities in the one-stop platform.
[Proposed] Personal Data Protection Policy, 2025	● Aims to complement existing data protection frameworks including the Right to Information Act 2007, the National Statistics Act 2022, and the Individual Privacy Act 2019. ● Explicitly enlists gaps in current frameworks regarding consent, ownership, data governance, data sharing, cross-border transfer, third-party processing, etc. ● Proposes the establishment of a Data Protection Board, and penalties for unauthorized modification or transfer of personal data. ● Criticized for lack of right to be forgotten provisions and clear delimitation of regulatory powers.

Pakistan

Pakistan has adopted a techno-authoritarian approach to the internet. From heightened surveillance powers being granted to its intelligence agencies (Asad, 2024) to banning platforms for hosting “objectionable content,” the country fails to provide judicial grounding or transparency in its actions of filtering, blocking, and taking down content (Jahangir, 2024). Its courts continue to approach new digital media regulations with an antiquated media mindset, failing to account for the complexities of modern digital communication.

These oppressive practices have been codified primarily through the *Prevention of Electronic Crimes Act (PECA), 2016* and the influence of the *Pakistan Telecommunications Authority (PTA)* (Ahmed et al., 2023). Initially introduced as a legal framework to address digital harms, PECA is laden with vague provisions that grant authorities broad enforcement discretion. Rather than serving this stated purpose, the law facilitates government overreach under the guise of national security (Aziz, 2022). Empowered by PECA, the PTA frequently restricts internet access as a means of suppressing political dissent, while internet shutdowns have become a routine tool for silencing religious or political opposition (Migliano, 2025). Recent amendments have further expanded PECA's reach, introducing stricter provisions that legitimize and extend the state's surveillance powers (Amnesty International, 2025).

These developments coincide with increased internet restrictions since 2024. VPN disruptions, initially attributed to a “technical glitch,” were later justified under a new VPN registration mandate issued by the PTA under the *Monitoring and Reconciliation of Telephony Traffic Regulation, 2010* (Ali, 2024). Officials defended the measure as necessary to curb “immoral” content and terrorist activity. Simultaneously, users experienced slow internet speeds, allegedly due to web-management system upgrades, raising concerns about a national firewall following previous deployments of Sandvine technology (Aziz, 2024). Government officials have provided conflicting statements on the existence of such a system, but patterns of throttling, slow speeds, and VPN restrictions indicate enhanced digital surveillance without official disclosure. Furthermore, under PTA directives, telecommunication companies operate a mass surveillance system, as confirmed by an Islamabad High Court ruling that exposed warrantless

data interception (Abbas, 2024). This was later reinforced by a government notification authorizing the country's intelligence agency to conduct surveillance for “national security.”

The notification was seemingly in response to litigation before the Islamabad High Court in two cases. Pakistan's Lawful Intercept Management System (LIMS) is a telecom surveillance architecture that came into public focus through litigation in 2024 (Qazi, 2025), although Amnesty International reports that versions of the system have existed since 2007. Telecom operators are required to provide interception capability, and PTA told the Islamabad High Court that operators must be able to place up to 2% of their subscriber base under surveillance, which adds to potentially more than four million users at any given time. Amnesty's 2025 investigation found that LIMS can enable access to call and SMS data, location information, browsing metadata and certain internet activity, with surveillance initiated through a target's phone number. The core concern is the scale, opacity and weak safeguards surrounding the system. Surveillance without individualised suspicion, meaningful judicial authorisation, transparency or effective data-protection law violates privacy and produces a chilling effect on journalists, political actors, civil society, and ordinary users.

Pakistan has also significantly expanded its internet filtering architecture, generally referred to as the “firewall” or Web Monitoring System (WMS) (Hussain, 2024). The original system was deployed years earlier, but investigative reporting and Amnesty International's 2025 *Shadows of Control* report indicate that it was substantially upgraded from 2023 onward into what Amnesty calls WMS 2.0, with capabilities that can include filtering websites, restricting VPNs, and managing internet traffic at network level. The main concerns are lack of transparency over procurement, technical capabilities, legal thresholds and oversight; the potential use of network infrastructure for political censorship; and collateral damage to freedom of expression, privacy, internet reliability and Pakistan's digital economy.

Litigation was the primary avenue for civil society to hold the government accountable. Alongside this, CSOs actively engage in policy advocacy, public awareness efforts, and capacity-building programs while also providing legal assistance in digital rights-centered court cases.

However, the 26th and 27th amendments to the Constitution changed the approach towards public

interest litigation. The amendments enabled executive capture of the judiciary and PILs, which had long been the go-to tool of resistance against the executive's overreach, are no longer an option taken into

consideration by digital rights advocates, with former successes being suspended or overturned through intra-court appeals.

TABLE 4 - RELEVANT TECH-RELATED POLICIES IN PAKISTAN

Law	Description
Prevention of Electronic Crimes Act, 2016	● Enacted in 2016, it creates various categories of criminal offences for online activity ● Has been used to charge journalists, political activists, and academics for “anti-state” and “anti-institution” speech. ● Criminal defamation has been abused against women in retaliation to #MeToo disclosures. Constitutionality challenged before courts and currently pending decision by the Supreme Court. ● Various High Courts have called out the investigation agency for abuse of power. ● A presidential ordinance expanded its scope to include the institutions of military and judiciary as potential targets of cyber offenses, thereby increasing digital policing, which was struck down by the High Court ● Censorship powers given to the Pakistan Telecommunication Authority for online content ● Various challenges brought to courts for ad hoc blocking of websites and apps over the years ● PTA routinely sends takedown requests to platforms referencing various criminal offences under the law
Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules, 2021	● Grant PTA unconstitutional censorship powers. ● Challenged before the Islamabad High Court, which directed revisions, no changes implemented as of yet. ● The government has been blocking social networking sites citing non-compliance with the rules and takedown requests.
[Proposed] Personal Data Protection Bill, 2023	● Despite discussions since 2005, no formal data protection law has been enacted. ● The existing draft mandates data localization, requiring critical personal data to be stored in Pakistan. ● Proposed data protection regulator under federal government control. ● Uses ambiguous terms such as “national security,” “legitimate interest,” and “public interest.”
Punjab Defamation Act, 2024	● Hastily passed with jurisdiction extending beyond the province. ● Allows public officeholders to be claimants and shifts burden of proof to defendants; claimants do not need to prove loss or damage. ● Cases are heard by government-appointed tribunals with powers to impose fines and disable social media accounts. ● Defendants do not have the right to a defense by default; they must request permission to present one. ● Remains under challenge before the Lahore High Court.
Prevention of Electronic Crimes (Amendment) Act, 2025	● Further tightens the government’s control over the digital landscape. ● Introduces offenses such as false and fake information with vague and ambiguous framing throughout. ● One of the first convictions under this new offence is of human rights lawyers Imaan Zainab Mazari-Hazir and Hadi Ali Chatta, who remain imprisoned, and routine notices being sent to journalists for reporting deemed critical of state policies ● Social Media Regulatory Authority established replacing the Pakistan Telecommunication Authority as regulator ● National Cyber Crime Investigation Agency established replacing the Federal Investigation Agency
Digital Nation Pakistan Act	● Enacted in January 2025 ● Provides the legal framework for digital transformation ● Establishes the Pakistan Digital Authority (PDA) which is supposed to develop and enforce a National Digital Masterplan, develop standards and coordinate federal and provincial digital systems ● Focuses on digital public infrastructure such as interoperable systems for digital identity, data exchange, payments, cloud-based government services, and open-data platforms
Artificial Intelligence Policy	● Approved in July 2025, focuses on skills, innovation, public-sector AI, infrastructure, and a National AI Fund ● Focus has shifted to implementation and AI sovereignty, including domestic capacity, infrastructure like data centers, and stronger state-led governance
techglobalinstitute.com	Digital Governance and Rights in South Asia, and the Path Forward: 2026 Update

Sri Lanka

Sri Lanka is rapidly advancing towards digital governance, with the Government targeting 100% digitalisation of government transactions by 2030 and a USD 15 billion digital economy (Information and Communication Technology Agency of Sri Lanka, 2025). Key initiatives include GovPay which enables secure, efficient, and transparent digital payments for government services, the Sri Lanka Unique Digital Identity (SLUDI), which will establish a secure, biometric-based digital identity for citizens aged 15 and above and GovTech, the lead agency responsible for modernizing government infrastructure and advancing citizen-centric digital services. Sri Lanka is also transitioning towards GovCloud (LGC3), a sovereign, secure and AI-ready cloud infrastructure designed to strengthen data sovereignty, resilience and service continuity.

This ambition is accompanied by two key sets of challenges facing Sri Lanka: first, challenges arising from the process through which digitalisation is being pursued; and second, gaps in the legal, institutional and regulatory foundations required to support inclusive and effective digital governance. These challenges also have significant implications for digital rights, underscoring the need to make the protection and promotion of digital rights a fundamental principle of Sri Lanka's digital transformation agenda.

Sri Lanka's digitalization agenda faces concerns regarding public participation, human rights, accessibility and accountability. It could be seen that the approach does not sufficiently reflect Sri Lanka's social and political context and has been largely top-down, with limited engagement of civil society, Parliament and the public. The lack of Sinhala and Tamil materials regarding the digitalization agenda further limits accessibility. These challenges underscore the need for a more inclusive, rights-based and participatory approach to digital governance.

Secondly, Sri Lanka faces significant legal, institutional and capacity gaps in its digital transformation. Government employees continue to face challenges relating to digital literacy, skills, and competence (Aruppala et al., 2025; Fernando & Keppitipola, 2024). The implementation of digital economy laws also remains challenging, with weak awareness and enforcement contributing to low adoption of existing legislation (Asian Development Bank 2025). Key frameworks on cybersecurity, interoperability

and cloud governance remain under development, while outdated instruments such as the Lanka Interoperability Framework continue to constrain integration (Asian Development Bank, 2025; Aruppala et al., 2025; Fernando & Keppitipola, 2024).

Inadequate infrastructure, particularly in rural areas, and limited technological capacity hinder widespread adoption. Furthermore, a lack of sufficient cybersecurity tools and protocols exposes these organizations to digital threats and creates a trust deficit. Aruppala et al., 2025; Fernando & Keppitipola, 2024). Recurring cybersecurity incidents too raise concerns about transparency and accountability. Importantly, in Sri Lanka as public services become increasingly digitalised, the right to be offline should also be recognised to ensure that citizens without digital access are not excluded from essential public services or civic participation (Herath, 2026).

Further, Sri Lanka's struggle with digital rights is tied to deeper structural issues, including economic instability, public distrust in the government, and systemic failures in addressing gender-based violence and other forms of discrimination. While the country has a strong and active civil society, perspectives on digital rights remain fragmented, with mobilization occurring primarily in response to pressing threats rather than through sustained advocacy.

TABLE 5 - RELEVANT TECH-RELATED POLICIES IN SRI LANKA

Law	Description
Personal Data Protection Act No. 9 of 2022 (PDPA)	Sri Lanka became the first South Asian country to pass a data protection law, modeled after the EU's GDPR, targeting all businesses that process data within Sri Lanka and related to its citizens. Ensures data is accurate, transparent, accessible, and provides right to erasure. It requires organisations to process data lawfully, securely, accurately, and only for specified purposes, while providing individuals with rights to access, correct, erase, and withdraw consent regarding their data. The PDPA is scheduled to become operational on 1 January 2027, including Section 2 on its application, Section 3 on its overriding effect, Part I on the processing of personal data, and Part III on data controllers and processors.
Online Safety Act No. 9 of 2024	Contains vague terms like “national security threats” and “distress” “prohibited statements” with no legal precedent or context. Enforcement left to the regulator, composed solely of executive-appointed individuals. Enables takedown of online content critical of the government. Enacted without considering the Sri Lanka Code of Practice for Online Safety and Responsible Content developed by industry association.
The Computer Crimes Act No. 24 of 2007	forms the foundation of Sri Lanka's legal framework for addressing cybercrime. The law criminalizes activities such as unauthorized access to computer systems, data theft, denial-of-service attacks, and other forms of digital intrusion. provides investigative powers to law enforcement authorities, subject to judicial oversight, and enables cooperation with international partners to address cross-border cybercrime. Although the Act has played a crucial role in combating cyber offences, evolving technologies and increasingly sophisticated cyber threats continue to pose challenges for enforcement and legal interpretation.
Electronic Transactions Act No. 19 of 2006.	This act, introduced in 2006, establishes the legal framework for electronic communication, contracts, and digital signatures. It provides legal recognition and validity for electronic transactions and helps foster trust in online interactions. However, inadequate to address contemporary challenges in digital governance.
Intellectual Property Act No. 36 of 2003	This act safeguards intellectual property rights, including copyrights, trademarks, and patents. It addresses online copyright infringement and provides remedies for IP violations in cyberspace. However, the act is outdated and does not address AI-generated content, digital platforms, online infringement, and emerging forms of digital creativity.
Payment Devices Frauds Act No. 30 of 2006	This act criminalizes the use of payment devices, such as credit cards or debit cards, to commit fraud. It imposes strict penalties for those convicted of payment device fraud. This Act too must be updated to address contemporary challenges in the digital world.

Thematic Overlaps

The first edition identified five themes that cut across the region's digital rights challenges. This update keeps them, so that change can be tracked from one year to the next, and adds a sixth. The three shifts described in the introduction run through all of them: the narrowing of institutional checks is most visible under Vague and Oppressive Laws and Executive Overreach; the state's turn to building digital infrastructure under Techno-Nationalism, Identity-Based Disenfranchisement, and the new theme on Techno-Solutionism; and public pushback under Civil Society. Beneath all six lies a problem the first edition identified and that has not changed: governance models borrowed from the Global North continue to be adopted without the offline protections they assume, such as a well-established right to freedom of expression, and imposing them without first addressing these structural gaps risks deepening existing power imbalances.

Each theme below opens with a one-line assessment of how it has changed since the first edition, based on the developments documented in the country sections and input from contributing organizations, followed by the evidence.

Techno-Nationalism

Since 2025: intensified, and increasingly focused on AI.

Techno-nationalism, a political ideology that ties a country's technological advancement to its geopolitical standing (Capri, 2019), remains a defining feature of the region. Political elites equate national strength with technological capability, justify state control over digital ecosystems on grounds of national security and resistance to foreign influence, and pursue digital sovereignty in ways that extend state influence into traditionally protected offline spaces.

Over the past year, this ambition has turned decisively toward AI and the infrastructure behind it. India's AI governance guidelines, Pakistan's AI policy with its emphasis on AI sovereignty and domestic data-center capacity, Nepal's National Artificial Intelligence Policy, and Sri Lanka's sovereign, AI-ready GovCloud all frame computing capacity as a matter of national standing,

with little public debate about who will control these systems or the data they hold.

Vague and Oppressive Laws

Since 2025: intensified, with notable reversals.

The first edition described a wave of legislation marked by inconsistencies, abstract rhetoric, and remnants of colonial legal frameworks, in which key terms like "national security" and "public interest" are left undefined and interpreted at the discretion of government-appointed regulators. The past year showed how quickly such provisions are put to use. Pakistan's 2025 amendments to PECA, which criminalize "false and fake information" without clearly defining either, were used within a year to convict two human rights lawyers over social media posts (Front Line Defenders, 2026). In Bangladesh, the 2025 Cyber Protection Ordinance removed most of the speech offences inherited from the Digital Security Act era, but draft amendments published in September 2026 would reintroduce defamation and maligning offences, add new offences on rumours and misinformation, and increase executive representation on the National Cyber Protection Council (Mahmud, 2026).

Governments also continue to invoke legitimate concerns, such as protecting women and children online, combating hate speech, and addressing disinformation, to justify overbroad restrictions. The hate speech bills introduced in the Indian states of Karnataka and Telangana, which allow officials to take "preventive action" against anticipated speech, go further still, targeting speech before it occurs. The clearest reversal came from Nepal, where public pressure forced the withdrawal of the Social Network Bill, which would have criminalized anonymous accounts and online activity without clear intent standards.

Executive Overreach

Since 2025: intensified.

Executive overreach remains a common feature across the region. Regulatory bodies are placed under the direct influence of the executive, which controls their composition and agendas, allowing governments to

bypass judicial oversight and to implement measures such as mass surveillance and platform shutdowns with little transparency.

This pattern extended to every country in 2025 and 2026. In India, the IT Rules have become the main vehicle for regulating the digital space, with obligations on AI, content moderation, and user rights, added through executive amendment rather than legislation (SFLC.in, 2026). In Pakistan, the 27th amendment created a Federal Constitutional Court whose composition is initially determined by the executive (Chatham House, 2025), while surveillance systems such as the Lawful Intercept Management System operate without meaningful judicial authorization. In Nepal, a single ministerial directive was enough to block 26 platforms in September 2025 (Al Jazeera, 2025). Shutdowns, the bluntest executive tool, remain routine. India alone imposed 65 in 2025, the most of any democracy (Access Now, 2026).

Identity-Based Disenfranchisement

Since 2025: risks growing as digital identity systems expand.

Since 2025, exclusion has moved from particular systems to the gateways themselves: as digital ID becomes the default route to public services and the vote, anyone the system cannot recognize is shut out.

Nepal's integration of its biometric national ID with voter registration in 2025 left out citizenship-affected individuals (Nationality for All, 2025), and its Nagarik App now concentrates identity documents and access to public services in a single state platform. Sri Lanka is rolling out a biometric digital identity for citizens aged 15 and above as part of a drive to digitalize all government transactions, prompting calls to recognize a right to be offline so that citizens without digital access are not shut out of essential services (Herath, 2026). Digital access is no longer only a question of connectivity; it has become a condition of civic participation.

Civil Society Co-Option and Renewal

Since 2025: under greater financial and legal pressure,

but with new forms of mobilization.

The first edition found many CSOs constrained by restrictive funding environments, dependence on donors with conflicting interests, and political pressure, producing a compliance-driven landscape in which they struggle to act as a counterweight to the state.

Those pressures have grown. The 2025 donor funding cuts have left digital rights organizations reporting a loss of capacity to resist repressive legislation (ARTICLE 19, 2026). Legal avenues are narrowing too: in Pakistan, public interest litigation, long civil society's most effective tool against executive overreach, is no longer regarded as viable following the 26th and 27th amendments.

The past year also showed a different side of civil society. In Nepal, the Gen-Z movement delegitimized established civil society actors, whom many protesters saw as co-opted and as having failed to hold the government accountable, and gave rise to looser networks that move between online and offline organizing. These emerging networks have consolidated through repeated crises but remain under-resourced, and they now face direct pressure: journalists and activists have faced threats, arbitrary arrests ([Pokharel, 2026](#); [Portel, 2026](#)), and police violence for dissent under the new government ([Amnesty International Nepal, 2026](#)), and proposals to move oversight of NGOs and INGOs from the Social Welfare Council to a department within the Home Ministry would bring civil society further under state control ([EU SEE, 2025](#); [Sharma, 2026](#)). Nepal thus shows both sides of this theme: co-option can hollow out established organizations, yet new forms of mobilization can emerge quickly, and they need resources and protection if they are to last.

Techno-Solutionism and State Digital Infrastructure

A theme that has sharpened since the 2025 edition is the growing reliance on state-built digital infrastructure and AI as fixes for structural problems. The platforms described in the introduction share a design pattern: they centralize identity, payments, and access to services in a single state system, and they make participation conditional on being digitally legible to the state. Nepal's Nagarik App requires registration through a phone number held in the user's

legal name and stores critical identity documents, without accounting for the digital divide; Pakistan's Digital Nation Act gives a new central authority broad coordination powers that are not yet matched by privacy, oversight, or redress safeguards; and Sri Lanka's digitalization agenda has been largely top-down, with few materials available in Sinhala or Tamil. The result is a concentration of sensitive data in state hands, justified as modernization. Nepal's March 2026 elections, in which AI-generated content circulated largely unchecked, showed how poorly existing laws are equipped for the harms these technologies bring.

Taken together, the six themes point in one direction: control over the digital sphere is concentrating in the executive, through rules that bypass legislatures, courts brought under political influence, and infrastructure the state alone designs and runs. Resistance depends on public pressure and coordination that can be sustained beyond a single crisis.

Policy Considerations

This edition builds on the principles set out in the first, with specific recommendations, each of which applies those principles to a problem that the past year brought into sharper focus. The recommendations are organized around the three shifts identified in the introduction and directed at those who can act on them: governments, technology companies, and those who fund and support civil society. The section closes by assessing which routes to accountability held up over the past year.

Restore Institutional Checks on State Power

The narrowing of institutional checks was the clearest trend of the past year. Governments should:

Legislate through parliament, not executive rules. Major obligations on platforms and users, such as those introduced through successive amendments to India's IT Rules, should be set out in primary legislation that is debated in parliament and open to public consultation, rather than imposed through delegated rules or ministerial directives.

Repeal vague speech offences and narrowly define the restrictions permitted under the International Covenant on Civil and Political Rights. Offences built on undefined terms such as "false and fake information," "rumours and misinformation," or "maligning," or similar, should be repealed. Any restriction on freedom of expression should fall within the legitimate grounds for restriction recognised under Article 19(3) of the ICCPR, which all five countries have ratified, and must also satisfy the requirements of legality, legitimate aim, necessity and proportionality. Criminal defamation should be abolished.

Require independent authorization for surveillance, blocking, and shutdowns. Interception, content blocking, and network shutdowns should require prior authorization from an independent judicial body, be time-bound, and meet the standards of legality, necessity, and proportionality set out in *Anuradha Bhasin v. Union of India*. Orders should be published, and surveillance systems such as Pakistan's Lawful Intercept Management System should be placed on a clear legal footing with independent oversight.

Protect judicial independence. Reforms to judicial appointments and constitutional review, such as Pakistan's 26th and 27th amendments, should not bring the courts under executive or military control. Courts remain the last formal check on digital restrictions, and their independence is a precondition for every other recommendation in this section.

Safeguards Before Scale for Digital Infrastructure and AI

The platforms and AI systems described above are outpacing the rules meant to govern them. Governments, and the development partners that finance these systems, should:

Put data protection in force first. No digital identity or service platform should become mandatory until a data protection law is in force and an independent data protection authority is operational, with powers that extend to state agencies as well as private companies.

Guarantee offline alternatives. Access to essential services should never depend on a digital ID or a smartphone. The right to be offline should be recognized in law, and no one should be excluded from services or from voting for lack of documents.

Consult before rollout. Digital public infrastructure and public-sector AI should be subject to public consultation, including in local languages, and to published human rights impact assessments before deployment.

Match AI ambition with AI safeguards. National AI policies should come with enforceable rules on transparency, accountability, and redress, particularly for AI used in public services, policing, and elections.

Platform Accountability in South Asia

Platforms face pressure from two directions: governments demand faster removals, while the companies' own investment in the region is shrinking. Companies should:

Invest in local-language capacity. Resource human moderation and fact-checking in South Asian languages in proportion to their user base in the region, rather than cutting integrity teams and relying on automated systems.

Publish what governments ask for. Report government takedown and user data requests by country, including requests made through informal or portal-based channels, and disclose when and why they comply.

Prepare for crises and elections. Maintain crisis protocols, developed with regional civil society, for protests, platform bans, and elections, where the past year showed that restrictions and AI-generated disinformation escalate fastest.

Engage regional civil society before crises, not after. Create standing channels of engagement with South Asian civil society rather than reaching out only once a ban or shutdown is under way.

Resource and Protect Civil Society

Civil society organizations are carrying more of the burden of accountability with less money and less protection. Funders and governments should:

Fund core work, not only projects. Donors should provide flexible, multi-year core funding to South Asian digital rights organizations and regional networks, so

that capacity lost after the 2025 U.S. funding cuts can be rebuilt on terms set by the region.

Reach new forms of organizing. Funding and protection mechanisms should extend to the looser, youth-led networks, similar to the ones that emerged in Nepal.

Protect civic space. Governments should stop using digital laws against journalists, lawyers, and activists, and should refrain from moving the oversight of NGOs under security ministries.

What Held Up: Routes to Accountability

The first edition highlighted judicial activism and civil society networks as proven local routes to accountability. The past year tested both, and added a third

Courts

Courts remain an important but increasingly unreliable check. In India, the Supreme Court's ruling in *Anuradha Bhasin v. Union of India* set standards for internet shutdowns, and in 2024 the Bombay High Court struck down the Fact-Check Unit provision of the IT Rules (*Kunal Kamra v. Union of India*, 2024). But courts have also upheld executive power, including the Karnataka High Court's 2025 dismissal of X Corp's challenge to the government's Sahyog takedown portal and the judiciary's validation of emergency action against Telegram, while WhatsApp's 2021 challenge to the traceability requirement remains undecided. In Pakistan, constitutional amendments have closed off public interest litigation almost entirely (International Commission of Jurists, 2024).

Public Mobilization

As Nepal's experience shows, public pressure proved the most decisive route of the past year. But it is also the costliest, and its gains are the least secure, as

they depend on the governments it brings to power. Nepal's new government has itself faced criticism for its treatment of journalists and activists.

Civil Society Networks

Coordinated action, such as the community of practice among Sri Lankan organizations that aligns messaging across conferences, panels, and public forums, remains valuable, although mobilization in Sri Lanka still tends to respond to immediate threats rather than sustain long-term advocacy. Each route is fragile on its own and largely confined within national borders. That is the case for regional coordination the first edition made, and it is stronger now.

Conclusion

The urgency the first edition described has not eased. Emerging technologies are still being used to suppress dissent, target marginalized communities, and consolidate power, and efforts to hold public and private actors to account are still constrained by limited resources and shrinking civic space.

Three developments defined the year. Public pressure in Nepal showed that repressive measures can still be reversed, but at a heavy cost. Constitutional amendments in Pakistan, executive rule-making in India, and attempts to revive speech offences in Bangladesh narrowed the institutional checks on state power. And across the region, governments began building AI and digital identity systems ahead of the rules needed to govern them. The recommendations in this paper are aimed at closing those gaps before they harden.

References

Abbas, Z. (2024). The surveillance system keeping tabs on millions. Dawn. <https://www.dawn.com/news/1843299>

Access Now. (2026). #KeepItOn: Internet shutdowns in 2025 annual report. <https://www.accessnow.org/>

<wp-content/uploads/2026/03/KeepItOn-Internet-Shutdowns-2025-Annual-Report.pdf>

Afrin, S. (2025). Personal data protection ordinance: Risk of misuse due to unchecked executive powers Prothom Alo. <https://en.prothomalo.com/bangladesh/ikh9acxpg5>

Ahmed S. Z., Yilmaz, I, Akbarzadeh, S., & Bashirov, G. (2023). Digital Authoritarianism and Activism for Digital Rights in Pakistan - ECPS. ECPS. <https://www.populismstudies.org/digital-authoritarianism-and-activism-for-digital-rights-in-pakistan/>

Al Jazeera. (2025). Nepal lifts social media ban after 19 killed in protests against corruption. <https://www.aljazeera.com/news/2025/9/9/nepal-lifts-social-media-ban-after-19-killed-in-protests-report>

Ali, K. (2024). PTA speaks on 'technical glitch', insists on VPN registration. Dawn. <https://www.dawn.com/news/1871781/pta-speaks-on-technical-glitch-insists-on-vpn-registration>

Ali, K. (2024). Unregistered VPNs won't work after Nov 30, says PTA chief. Dawn. <https://www.dawn.com/news/1873356>

Ali, K., & Ali, U. (2024). Interior Ministry demands VPNs blockage, claims it is used by 'terrorists to facilitate violent activities.' Dawn. <https://www.dawn.com/news/1872561>

Amnesty International Nepal. (2026). Nepal: Immediately release detained activist Ansari and ensure right to protest. https://amnestynepal.org/press_release/nepal-immediately-release-detained-activist-ansari-and-ensure-right-to-protest

Amnesty International. (2025). Pakistan: Authorities pass bill with sweeping controls on social media. <https://www.amnesty.org/en/latest/news/2025/01/pakistan-authorities-pass-bill-with-sweeping-controls-on-social-media/>

Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).

ARTICLE 19. (2026). Targeted: How cuts to US foreign aid threaten freedom of expression and its defenders. https://www.article19.org/wp-content/uploads/2026/04/ARTICLE-19_Targeted_FINAL_April-2026.pdf

Aruppala, D., Gunawardana, K., & Razi, M. J. M. (2025, February 19). Challenges and barriers to digital transformation in Sri Lankan government organizations: Managers' perceptions. <https://www.researchgate>

[net/publication/389696414_Challenges_and_Barriers_to_Digital_Transformation_in_Sri_Lanka_Government_Organizations_Managers'_Perceptions](https://www.techglobalinstitute.com/publication/389696414_Challenges_and_Barriers_to_Digital_Transformation_in_Sri_Lanka_Government_Organizations_Managers'_Perceptions)

Asad, M. (2024). Senior lawyers challenge ISI's surveillance powers in IHC. <https://www.dawn.com/news/1845339>

Asian Development Bank. (2025). Digital public infrastructure landscape and opportunities in South Asia. <https://www.adb.org/sites/default/files/publication/1114321/digital-public-infrastructure-south-asia.pdf>

Aziz, F. (2022). Project Peca I: How to silence a nation. <https://www.dawn.com/news/1725805>

Aziz, F. (2024). Project PECA I: How to silence a nation. Prism. <https://www.dawn.com/news/1725805>

Aziz, F. (2024). Surveillance central. Dawn. <https://www.dawn.com/news/1845889/surveillance-central>

Aziz, F. (2024). The ministry of (dis)information and the ban on X. Dawn. <https://www.dawn.com/news/1828972/the-ministry-of-disinformation-and-the-ban-on-x>

Aziz, F. (2024). The privacy myth. Dawn. <https://www.dawn.com/news/1844158>

Bangladesh Legal Aid and Services Trust (BLAST). (2026). Submission to Information and Communication Technology Division on Draft Cyber Protection (Amendment) Act 2026. https://blast.org.bd/content/Recommendation/Final_English_BLAST_CPA_recommendations_24_Sep_2026.pdf

Bhalla, V. (2026). India recorded 65 internet shutdowns in 2025, highest among democracies: Access Now report. The Indian Express. <https://indianexpress.com/article/india/india-recorded-65-internet-shutdowns-in-2025-highest-among-democracies-access-now-report-10613113/>

Bradford, A. (2020) The European Union in a globalised world: the "Brussels effect" - Groupe d'études géopolitiques. Groupe D'études Géopolitiques. <https://geopolitique.eu/en/articles/the-european-union-in-a-globalised-world-the-brussels-effect/>

Business Standard. (2025). Govt approves Cyber Security Ordinance 2025, repeals 9 sections of previous law. <https://www.tbsnews.net/bangladesh/govt-approves-cyber-security-ordinance-2025-repeals-9-sections-previous-law-1135181>

Business Standard. (2025). Nepal GenZ protests: PM Oli resigns, Parliament set afire amid clashes. [https://](https://www.techglobalinstitute.com)

www.business-standard.com/world-news/nepal-genz-protests-social-media-oli-125090900716_1.html

Capri, A. (2019). Techno-Nationalism: what is it and how will it change global commerce? Forbes. <https://www.forbes.com/sites/alexcapri/2019/12/20/techno-nationalism-what-is-it-and-how-will-it-change-global-commerce/?sh=6765528c710f>

Center for the Study of Organized Hate. (2025, June 30). X's Community Notes and the South Asian misinformation crisis. <https://www.csohate.org/2025/06/30/x-community-notes-south-asia/>

Chakraborty, D. (2026). Nepal gets a new govt: Balen Shah now world's youngest PM, leading world's youngest cabinet. ThePrint. <https://theprint.in/world/nepal-gets-a-new-govt-balen-shah-now-worlds-youngest-pm-leading-worlds-youngest-cabinet/2890500/>

Chatham House. (2025). Pakistan's 27th constitutional amendment moves it one step closer to authoritarian rule. <https://www.chathamhouse.org/2025/12/pakistans-27th-constitutional-amendment-moves-it-one-step-closer-authoritarian-rule>

CNN. (2023, November 14). Nepal bans TikTok because of 'disruption' to social harmony. <https://www.cnn.com/2023/11/14/tech/nepal-tiktok-ban-hnk-intl/index.html>

Cyber Protection Act, Section 26 (2026) (Bangladesh). Daily Star. (2025). Govt repeals Cyber Security Act; new Cyber Security Ordinance issued. <https://online.thedailystar.net/tech-startup/news/govt-repeals-cyber-security-act-new-cyber-security-ordinance-issued-3900681>

Daily Star. (2026). Civil society organisations voices concern over proposed Cyber Protection Act amendments. <https://www.thedailystar.net/news/bangladesh/rights/news/civil-society-organisations-voices-concern-over-proposed-cyber-protection-act-amendments-4275486>

EU SEE. (2025). Draft NGO Registration, Regulation and Management Bill raises concerns of shrinking civic space in Nepal. <https://eusee.hivos.org/alert/draft-ngo-registration-regulation-and-management-bill-raises-concerns-of-shrinking-civic-space-in-nepal/>
European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial

intelligence (Artificial Intelligence Act). Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

Fernando, H., & Keppitipola, I. (2024). Barriers to digital transformation in a public organization in Sri Lanka [master's thesis]. <https://www.diva-portal.org/smash/get/diva2:1955548/FULLTEXT01.pdf>

Financial Express. (2026). Mobile subscriptions go up by 0.65m in Aug, The Financial Express. <https://today.thefinancialexpress.com.bd/trade-market/mobile-subscriptions-go-up-by-065m-in-aug-1790181763>

Front Line Defenders. (2026). Pakistan: Imaan Zainab Mazari and Hadi Ali Chattha sentenced to 17 years imprisonment. <https://www.frontlinedefenders.org/en/case/pakistan-imaan-zainab-mazari-and-hadi-ali-chattha-sentenced-17-years-imprisonment-1>

GSMA. (2026). The state of mobile internet connectivity report 2026. <https://www.gsma.com/somic/wp-content/uploads/2026/09/The-State-of-Mobile-Internet-Connectivity-2026.pdf>

Herath, V. (2026, July 18). No smartphone, no service? The right to be offline. Daily Mirror. [No smartphone, no service? The Right to be Offline - News Features | Daily Mirror](https://www.dailymirror.lk/news/features/no-smartphone-no-service-the-right-to-be-offline-news-features)

Human Rights Treaty Monitoring Coordination Centre. (2020). Shadow report on the implementation of the International Covenant on Civil and Political Rights (ICCPR) in Nepal. https://cdn.ccprcentre.org/files/documents/INT_CCPR_ICS_NPL_43954_E.pdf

Human Rights Watch. (2018). No Place for Criticism: Bangladesh Crackdown on Social Media Commentary
Hussain, A. (2024). Pakistan tests secret China-like 'firewall' to tighten online surveillance. <https://www.aljazeera.com/news/2024/11/26/pakistan-tests-china-like-digital-firewall-to-tighten-online-surveillance>

ICJ. (2024). Pakistan: 26th Constitutional amendment is a blow to the independence of the judiciary. <https://www.icj.org/pakistan-26th-constitutional-amendment-is-a-blow-to-the-independence-of-the-judiciary/>
Information and Communication Technology Agency of Sri Lanka. (2025). Sri Lanka's digital economy blueprint. https://www.icta.lk/icta-assets/uploads/2025/10/digital-economy-blueprint-2026-01-21_1768987510_69709b768efd5.pdf

Internet Freedom Foundation. (2026). Analysis of the 2026-2027 Budget. <https://internetfreedom.in/analysis-of-the-2025-2026-budget/>

Jacob, H. (2024). The end of South Asia. Foreign Affairs. <https://www.foreignaffairs.com/south-asia/end-south-asia>

Jahangir, R. (2024). Pakistan on verge of Techno-Authoritarian turn. Tech Policy Press. <https://www.techpolicy.press/pakistan-on-verge-of-techno-authoritarian-turn/>

Kathmandu Post. (2025, August 18). IT and Cybersecurity bill raises free speech concerns. <https://kathmandupost.com/national/2025/08/18/it-and-cybersecurity-bill-raises-free-speech-concerns>

Kathmandu Post. (2026). Government moves to withdraw Social Media Bill. <https://kathmandupost.com/national/2026/02/07/government-moves-to-withdraw-social-media-bill>

Khan, I. (2021). Disinformation and freedom of opinion and expression (A/HRC/47/25). UN Human Rights Council. <https://docs.un.org/en/A/HRC/47/25>

Khan, I. (2023). Communication to the Government of Bangladesh concerning the draft Cyber Security Act (OL BGD 7/2023). UN Human Rights Council. <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gld=28358>

Khan, I. (2025). Communication to the Government of Bangladesh concerning the draft Cyber Protection Ordinance (OL BGD 2/2025). UN Human Rights Council. <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gld=29800>

Kunal Kamra v. Union of India, Writ Petition 9792 of 2023 (Bombay High Court, India, Sept. 26, 2024).

Lalani, F. M. (2024) Predicting the direction of digital sovereignty in Post-Election India. New America. <https://www.newamerica.org/planetary-politics/blog/predicting-the-direction-of-digital-sovereignty-in-post-election-india/>

Lalani, F. M., & Irugalbandara, S. (2024). The Sri Lanka Model: The impact of civil advocacy on tech Policy. Tech Policy Press. <https://www.techpolicy.press/the-sri-lanka-model-the-impact-of-civil-advocacy-on-tech-policy/>

Lamichhane, R. (2022). Digital inclusion and digital equity. The Kathmandu Post. <https://kathmandupost.com/columns/2022/08/28/digital-inclusion-and-digital-equity>

Mahmud, F. (2026). Bangladesh's new cyberlaw rebrands the same old censorship. Asia Times. <https://asiatimes.com/2026/09/bangladeshs-new-cyberlaw-rebrands-the-same-old-censorship/>

Mahmood, S. (2022). Bangladesh: New online content regulation, localisation rules threaten privacy. <https://www.context.news/digital-rights/opinion/how-bangladeshs-new-online-content-regulation-threatens-privacy>

Migliano, S. (2025). Government Internet Shutdowns Cost \$7.69 Billion in 2024. Top10VPN. <https://www.top10vpn.com/research/cost-of-internet-shutdowns/>

News Laundry. (2025). DIGIPUB, Editors Guild warn India's new data rules will cripple journalism. <https://www.newslaundry.com/2025/11/19/cripple-rti-endanger-journalism-digipub-slams-data-rules-urges-reform>

OECD. (2026). International aid fell sharply in 2025, says OECD. <https://www.oecd.org/en/about/news/press-releases/2026/04/international-aid-fell-sharply-in-2025-says-oecd.html>

OHCHR. (2025). Fact-Finding Report: Human Rights Violations and Abuses related to the Protests of July and August 2024 in Bangladesh. <https://www.ohchr.org/sites/default/files/documents/countries/bangladesh/ohchr-fftb-hr-violations-bd.pdf>

Opiah, A. (2024). Nepal reverses mandatory national ID requirement for social security benefits. Biometric Update | Biometrics News, Companies and Explainers. <https://www.biometricupdate.com/202407/nepal-reverses-mandatory-national-id-requirement-for-social-security-benefits>

Pokharel, G. (2026). Vehicle linked to RSP leader among those blocking three media houses. The Kathmandu Post. <https://kathmandupost.com/national/2026/07/13/vehicle-linked-to-rsp-leader-among-those-blocking-three-media-houses>

Portel, P. (2026). Police detain political analyst Bharat Dahal in Morang. The Kathmandu Post. <https://kathmandupost.com/national/2026/09/20/political-analyst-bharat-dahal-detained-in-morang>

Qazi, F. (2025). The Politics of Exposure: Audio Leaks and the Erosion of Privacy and Democracy in Pakistan. GW Law. <https://www.law.gwu.edu/sites/g/files/zaxdzs5421/files/2025-10/FQ-audio-leaks-case-study.pdf>

SFLC.in. (2026). SFLC.in's concerns with the IT Rules (Second Draft Amendments), 2026. <https://sflc.in/it-rules-second-draft-amendments-2026-submit-your-comments-now/>

Shahid, U. (2026). Meta's AI ambitions and platform integrity in South Asia. Association for Progressive Communications. <https://www.apc.org/en/blog/metasis-ai-ambitions-and-platform-integrity-south-asia>

Sharma, B. (2026). Social Welfare Council under review amid calls for reform. Nepal News. <https://english.nepalnews.com/s/society/social-welfare-council-under-review-amid-calls-for-reform>

Sinha, A. (2026). India's Telegram Ban Risks Normalizing Platform-Wide Blocking. Tech Policy Press. <https://www.techpolicy.press/indias-telegram-ban-risks-normalizing-platform-wide-blocking/>

Tech Global Institute. (2024). A New Digital Frontier: A Blueprint for Reforms towards Rights-Respecting Information and Technology Laws in Bangladesh. <https://techglobalinstitute.com/wp-content/uploads/2024/12/Whitepaper-A-New-Digital-Frontier-Bangladesh.pdf>

Tech Global Institute. (2024). Reimagining 'Tech accountability' in the global majority. <https://techglobalinstitute.com/research/reimagining-tech-accountability-in-the-global-majority/>

Tech Global Institute. (2025). Launch of the South Asians for Digital Rights Coalition. <https://techglobalinstitute.com/announcements/launch-of-the-south-asians-for-digital-rights-coalition/>

Tech Global Institute. (2025). The Impact of Funding Cuts on Internet Freedom in the Global Majority. <https://techglobalinstitute.com/announcements/blog/the-impact-of-funding-freezes-on-internet-freedom-in-the-global-majority/>

Transparency International Bangladesh. (2026). The Interim Government's Reluctance to Pursue Reforms in Ordinance Formulation: Position Paper. <https://ti-bangladesh.org/upload/files/position-paper/2026/Position-Paper-on-Reluctance-to-Pursue-Reforms-TIB-En.pdf>

Tworek, H. (2021). Facebook's America-centrism is now plain for all to see. Centre for International Governance Innovation. <https://www.cigionline.org/articles/facebooks-america-centrism-is-now-plain-for-all-to-see>

Nationality for All. (2025). Nepal. Statelessness

Encyclopedia Asia Pacific. <https://seap.nationalityforall.org/digital-id/regional-overview/south-asia/nepal/>

UN High Commissioner for Human Rights. (2022). Civil society space: COVID-19: The road to recovery and the essential role of civil society (A/HRC/51/13). United Nations. <https://docs.un.org/en/A/HRC/51/13>

