accountabilitylab
PAKISTAN

POLICY BRIEF

The Digital Democracy Ecosystem In South Asia

Civic Ecosystems, Structural Constraints, Policy Regimes, and Regional Cooperation

/accountlabpk pakistan.accountabilitylab.org

Contents

Executive Summary

Digital democracy in South Asia is defined less by access to technology and more by the conditions under which that technology is used. Over the past decade, the region has witnessed rapid expansion in internet connectivity, mobile penetration and digital public infrastructure. However, these gains have not translated evenly into meaningful, safe and participatory civic engagement. Institutional arrangements, legal frameworks, platform dynamics and political context play a far more decisive role in shaping whether digital spaces function as arenas of participation or instruments of control.

Comparative evidence across regional and global indices underscores a fragmented landscape. Countries such as India and Bangladesh exhibit strong digital state capacity and growing connectivity but remain only "Partly Free" in terms of internet freedom. Pakistan combines moderate digital systems with a "Not Free" classification, reflecting legal and political constraints. Sri Lanka, Bhutan and Maldives show relatively high access with varying institutional safeguards, while Nepal remains transitional. Afghanistan stands apart with severe restrictions on both access and civic space. The key insight is consistent across contexts: digital capacity does not automatically translate into digital democracy.

A defining regional pattern is the emergence of managed civic closure. Rather than abrupt democratic breakdown, civic space is gradually narrowed through legal ambiguity, administrative control, surveillance, funding restrictions and informal coercion. Digital environments sit at the center of this process. While civil society uses digital tools for mobilization, communication and advocacy, states increasingly regulate, monitor and, at times, disrupt these activities. Evidence shows that this environment produces self-censorship, risk-averse behavior and reduced willingness to engage on politically sensitive issues. Civic closure is therefore as much about uncertainty and perceived risk as it is about formal restriction.

Digital governance has become the primary arena where these tensions are negotiated. Across South Asia, governments are deploying a wide range of regulatory tools, including cybercrime laws, online safety frameworks, intermediary rules, platform registration requirements, takedown powers, data governance regimes and, in some cases, internet shutdowns. While these measures often respond to legitimate concerns such as cybersecurity and online harm, their broad scope and uneven enforcement create a chilling effect on civic engagement. At the same time, compliance burdens fall disproportionately on civil society organizations, journalists and smaller actors, while large technology companies retain the capacity to absorb regulatory pressure and negotiate with states.

Platform dynamics further complicate the landscape. Social media platforms shape visibility and public discourse through algorithmic systems that reward speed, emotion and engagement. This creates a structural imbalance in which populist or polarizing content travels more easily than nuanced, evidence-based civic discourse. Civil society organizations face a strategic dilemma: to remain visible, they often adapt to platform logic, which can dilute policy depth and long-term advocacy goals. Monitoring evidence shows that while digital initiatives can generate strong engagement and participation, they often struggle to translate visibility into sustained civic learning or accountability outcomes.

At the same time, civil society capacity remains uneven. The region has a large and active ecosystem of organizations with strong interest in digital engagement, particularly around youth, inclusion, human rights and governance. However, institutional readiness is limited. Many organizations lack advanced systems for cybersecurity, legal compliance, data protection, analytics and long-term digital strategy. Digital tools are frequently treated as communication channels rather than as core infrastructure for advocacy, monitoring and accountability. These gaps are not merely technical; they reflect structural constraints, including funding limitations, regulatory pressure and evolving digital risks. Smaller, community-based organizations, often closest to marginalized populations, are particularly affected, contributing to an uneven civic ecosystem.

Regional dynamics further shape these outcomes. South Asia is experiencing increasing political and economic fragmentation, with strained bilateral relations, reduced cross-border cooperation and diverging development trajectories. This has weakened regional platforms and limited opportunities for shared learning and coordinated civic action. As a result, civic ecosystems are becoming more nationally bounded, even as digital platforms and the challenges they generate such as misinformation, surveillance and platform governance, remain inherently transnational.

Despite these constraints, important openings remain. Issue-based engagement around themes such as digital safety, misinformation, public-service accountability, climate and inclusion continues to provide viable entry points for civic action. Locally grounded interventions have demonstrated that meaningful participation can be sustained when programs are context-sensitive and inclusive. Regional learning persists through informal networks, while diaspora and exile-led initiatives offer alternative channels for engagement in high-risk contexts. Digital tools also enable forms of low-visibility, decentralized collaboration that can maintain civic connections across borders even in politically constrained environments.

The central challenge for digital democracy in South Asia is therefore structural rather than technological. The region possesses the connectivity, tools and civic intent necessary for participation. What remains uneven are the enabling conditions—legal clarity, institutional safeguards, trust, and space for engagement, that allow digital systems to function as platforms for meaningful democratic life. Strengthening these conditions, rather than expanding technology alone, will determine the future trajectory of digital democracy in the region.

1. Digital democracy ecosystem: Scope and framing

Digital democracy is not only about access to the internet. It is about whether people can use digital spaces to participate in public life safely, freely and meaningfully. A mobile phone or a social media account may allow someone to speak, but it does not guarantee that they will be heard, protected, or able to influence decisions. The concept of digital democracy denotes the relationship between collective self-government and mediating digital infrastructures[1] (Berg & Hofmann, 2021).

Like other regions, South Asia's digital democratic space is shaped by the interaction of several forces. Civil society organizations mobilize citizens, run campaigns, document rights issues and connect communities to the state. Digital platforms decide what content becomes visible, what spreads quickly and what is suppressed. Governments and regulators define or redefine the legal boundaries of online speech through cyber laws, platform rules, surveillance systems and shutdown powers. Donors and funding institutions influence what kinds of civic work receive support. Public institutions increasingly deliver services through digital systems such as identity databases, payment platforms and complaint portals. At the same time, regional political relations influence how information flows across borders and how civic actors collaborate with one another.

These forces do not operate equally. In South Asia, institutional, legal and political conditions play a much larger role in shaping digital democracy than access to technology alone. A country may have widespread internet coverage but still restrict online speech. It may offer digital public services but create fear around data use or surveillance. It may have active social media users but limited space for dissent, journalism or minority voices. In such contexts, technology expands possibility, but the system determines whether that possibility can be used.

This is why digital democracy is understood more as an ecosystem rather than a technology sector. What matters is not only who is online, but who feels safe to speak, who can afford to stay connected, whose content is visible, and whether digital engagement leads to real civic outcomes.

[1] https://policyreview.info/articles/analysis/digital-democracy

The Digital Democracy Initiative (DDI), managed by Accountability Lab, provides useful insight into one part of this ecosystem, particularly the role of civil society. DDI works across South Asia to strengthen civic space through grants, mentoring, capacity-building and regional learning. Its evidence base includes a mapping survey, a Digital Divide study and monitoring reports from supported initiatives.

The DDI mapping survey identified 407 organizations willing to work with DDI across eight South Asian countries, including NGOs, community-based organizations, social enterprises, networks, informal groups and hybrid entities. Many of these organizations are relatively young, having emerged alongside the growth of mobile internet and social media. This gives them energy and familiarity with digital tools, but it also means that many lack strong institutional systems for cybersecurity, data protection, monitoring and long-term advocacy. Many organizations are digitally visible, but fewer are digitally capable.

The DDI digital divide research adds an important dimension to this picture. It shows that the region has moved beyond a simple "access problem." While internet penetration is expanding, meaningful use remains uneven. On average, only about half of surveyed users report regular and reliable internet access, and affordability is a major barrier, with a majority describing data costs as high or prohibitive.

The divide is also social and not just technical. Women's participation in digital spaces remains significantly lower in several countries, and many users report concerns about online harassment, surveillance and misuse of personal data. These concerns directly affect whether people feel comfortable engaging in civic or political discussions online.

The research also highlights a gap between access and capability. Many users are able to connect to the internet, but lack the skills to verify information, protect their privacy, avoid scams, or use digital platforms for civic engagement. As a result, digital spaces are often used for consumption rather than participation, and for expression rather than accountability (Digital Divide in South Asia, Accountability Lab, 2025).

At the same time, civil society does not operate in isolation. Its effectiveness depends on the broader ecosystem. If laws are unclear or restrictive, organizations may avoid speaking. If platforms reward sensational content, serious civic messaging may struggle to reach audiences. If internet access is expensive or unreliable, participation becomes unequal. If regional tensions are high, cross-border learning and cooperation become difficult.

Regional dynamics are particularly important in South Asia. Political tensions between countries, conflict in Afghanistan, democratic uncertainty in parts of the region, and polarized public discourse all influence how digital civic space evolves. These factors shape what organizations can do, whom they can work with, and how their work is perceived.

Digital democracy is not guaranteed by technology. It depends on whether the environment allows people to use technology to participate in public life. In South Asia, the technology has expanded quickly, but the conditions that make it democratic have not kept pace. That gap defines the region's digital democracy challenge.

1.1 Where do the South Asian countries stand

A comparative view of South Asia through global indices helps clarify the difference between four separate dimensions: internet freedom, digital state capacity, mobile connectivity, and information and communication technology (ICT) development. Freedom House's Freedom on the Net measures online freedoms[2] (Freedom House, 2025). The World Bank's GovTech Maturity Index[3] (World Bank, 2022) measures digital government

[2] https://freedomhouse.org/sites/default/files/2025-11/Freedom_on_the_Net_2025_Digital.pdf
[3] https://www.worldbank.org/en/data/interactive/2022/10/21/govtech-maturity-index-gtmi-data-dashboard

capacity. Global System for Mobile Communications Association's (GSMA) Mobile Connectivity Index[4] (GSMA, 2024) measures conditions for mobile internet adoption, including infrastructure, affordability, consumer readiness, and content and services. International Telecommunication Union's (ITU) ICT Development Index[5] (ITU, 2025) measures progress toward universal and meaningful connectivity.

Country	Freedom on the Net 2025	Freedom on Net Status	World Bank GovTech Maturity Index (GTMI)	GSMA Mobile Connectivity Index	ICT Development Index	DDI Digital-Readiness Index (DRI) Median
Afghanistan	Not covered	—	0.121	26.8	36.5	1.4/5
Bangladesh	45	Partly Free	0.882	56.7	64.9	2.9/5
Bhutan	Not covered	—	0.814	64.4	85.7	2.4/5
India	51	Partly Free	0.969	69.2	Not assessed	3.1/5
Maldives	Not covered	—	0.359	64.2	81.7	3/5
Nepal	Not covered	—	0.517	53.1	Not assessed	2.6/5
Pakistan	27	Not Free	0.679	49.1	56.4	2.3/5
Sri Lanka	53	Partly Free	0.657	64.0	71.4	2.7/5

A comparative view across South Asia shows that countries in the region are moving at very different speeds across digital systems, connectivity and civic space and, importantly, progress in one area does not necessarily translate into progress in another.

At one end of the spectrum, India and Bangladesh show relatively strong performance in building digital systems and connectivity. India records the highest GovTech maturity score at 0.969 and a strong mobile connectivity score of 69.2, alongside a relatively higher digital-readiness level of 3.1 out of 5. Bangladesh also shows high GovTech maturity at 0.882 and a solid connectivity score of 56.7, with a digital-readiness level of 2.9. Yet both countries are classified only as "Partly Free" in terms of internet freedom, indicating that strong digital infrastructure does not automatically create open civic space.

Sri Lanka presents a similar pattern. It has a relatively high Freedom on the Net score of 53 and is categorized as "Partly Free," with moderate digital-readiness (2.7) and connectivity (64.0). However, its GovTech score of 0.657 suggests that while services and access exist, institutional capacity and governance systems are still evolving. Bhutan, although not covered in Freedom on the Net, performs strongly on connectivity (64.4) and particularly on ICT development (85.7), but its digital-readiness remains moderate at 2.4, reflecting gaps in civic use and institutional capacity.

Maldives also shows relatively high connectivity (64.2) and ICT development (81.7), but its lower GovTech score (0.359) indicates weaker institutional systems. Its digital-readiness score of 3 suggests that users are active online, but the enabling environment for governance and structured civic engagement remains limited.

Pakistan reflects a different kind of imbalance. With a Freedom on the Net score of 27, it falls in the "Not Free" category despite having a mid-level GovTech score of 0.679 and a connectivity score of 49.1. Its digital-readiness

[4] https://www.mobileconnectivityindex.com/index.html#year=2024&zoneIsocode=BGD,BTN,IND,NPL,PAK,LKA
[5] https://datahub.itu.int/data/?y=2025

score of 2.3 further indicates that while systems and access exist, civic use remains constrained by affordability, gender gaps, and a restrictive environment.

Nepal occupies a middle position across most indicators. Its GovTech score of 0.517 and connectivity score of 53.1 suggest moderate development, while its digital-readiness score of 2.6 reflects growing but uneven civic engagement. However, the absence of Freedom on the Net data makes it harder to fully assess the openness of its digital space, although emerging regulatory trends suggest increasing control.

Afghanistan stands apart from the rest of the region. With extremely low GovTech maturity (0.121), very weak connectivity (26.8), and the lowest digital-readiness score (1.4), it reflects a context where both access and civic space are severely constrained. Even basic digital participation is limited, and the broader political environment further restricts the use of digital tools for civic engagement.

1.2 Comparative perspective: Digital capacity, connectivity and civic space in South Asia

A comparative reading of South Asia across digital government capacity, connectivity, and civic space reveals a consistent but uneven pattern. Countries in the region are advancing in digital infrastructure and state-led digital systems, yet these gains are not translating uniformly into open, participatory or secure digital civic environments.

At the upper end of digital capacity, India and Bangladesh demonstrate strong performance in building digital systems and expanding connectivity. India stands out with the highest level of digital government maturity and one of the strongest connectivity environments in the region, alongside relatively higher digital readiness among users. Bangladesh also shows substantial progress, combining rapid digital adoption with an active civil society ecosystem. However, both countries remain categorized as only “Partly Free” in terms of internet freedom. This indicates that improvements in infrastructure and service delivery do not necessarily expand civic space. Instead, legal frameworks, platform regulation, and political dynamics continue to shape how digital spaces are used.

A second group of countries, including Sri Lanka, Bhutan and Maldives, illustrates a different configuration. These countries perform relatively well on connectivity and, in some cases, on broader ICT development indicators. Sri Lanka, for example, combines moderate digital government capacity with relatively strong connectivity and a “Partly Free” classification. Bhutan shows high levels of ICT development and stable digital policy direction, while Maldives reflects high user access. Yet across this group, digital readiness remains moderate, and institutional systems for civic engagement, data protection and accountability are still evolving. The result is an environment where access exists, but meaningful and protected participation remains limited or uneven.

Pakistan and Nepal occupy a middle position across most indicators, but for different reasons. Pakistan’s profile is defined by a moderate level of digital government capacity and expanding connectivity coexisting with a “Not Free” classification and relatively low digital readiness. This reflects the combined effect of legal restrictions, affordability challenges, gender gaps and constrained civic space. Nepal, by contrast, shows moderate performance across indicators without extreme constraints in any single dimension, but remains in a transitional phase. Its expanding connectivity and usage are not yet matched by stable regulatory frameworks or strong institutional capacity, creating uncertainty about the future direction of its digital civic space.

Afghanistan stands apart as an outlier across all dimensions. With extremely low digital government capacity, very weak connectivity and the lowest level of digital readiness in the region, it reflects a context where both access and civic space are severely restricted. Digital participation is limited not only by infrastructure deficits but also by broader political and security conditions that constrain even basic forms of communication and expression.

This comparison highlights three structural features of South Asia’s digital ecosystem. First, there is no direct relationship between digital capacity and digital democracy. Countries with stronger digital government systems or higher connectivity do not necessarily provide more open or participatory digital spaces. Second, the region is

moving from a "coverage gap" to a "usage and capability gap," where access exists but meaningful engagement is constrained by affordability, skills, safety and trust. Third, institutional and legal conditions remain the decisive factor. Across countries, it is these conditions, rather than technology itself, that determine whether digital spaces function as tools of participation or as managed and constrained environments.

This pattern points to a widening gap between digital expansion and democratic deepening. South Asia is becoming more digitally connected and more digitally governed, but not uniformly more digitally democratic.

2. Civic closure as the regional phenomenon

Civic closure in South Asia is increasingly managed rather than openly declared. Most countries retain formal democratic institutions, elections, courts, legislatures, and constitutional language. However, civic space is gradually narrowed through legal regulation, administrative control, funding restrictions, surveillance, online harassment, and informal coercion.

Civic closure in South Asia often occurs through incremental institutional and regulatory change rather than abrupt democratic breakdown. What emerges is not the disappearance of civic space, but its continuous reshaping into a more controlled and risk-sensitive environment.

Digital space is central to this process. Civil society organizations use social media, messaging applications, online campaigns, digital storytelling, data visualization, and virtual meetings to bypass traditional gatekeepers. At the same time, governments monitor, regulate, throttle, block, or criminalize aspects of online activity. Monitoring evidence suggests that this tension plays out in practice as a constant negotiation rather than a clear boundary. In several DDI-supported initiatives, organizations were able to operate and engage communities, but often within carefully managed thematic and operational limits, avoiding overtly political framing while still pursuing civic outcomes.

The DDI Digital Divide study shows how this environment affects civic behavior. Respondents across countries reported self-censorship, surveillance fears, legal uncertainty, and hesitation in online engagement. This is important because civic closure is not measured only by arrests or bans. It is also measured by what citizens and organizations stop saying, stop sharing, or stop organizing because the risks are unclear. Monitoring reports reinforce this pattern. Participants in digital engagement activities often showed strong interest in skills such as content creation, fact-checking, and digital communication, but were more cautious or less expressive when discussions moved toward governance, rights or accountability themes.

Civic openings linked to elections also remain temporary and reversible. Monitoring reports from Bangladesh show that election environments affected mobilization and participation in several DDI-supported activities. Subarna-Bhumi Foundation reported difficulty mobilizing target groups in an election environment, while CPD Narayanganj noted that election conditions affected participation of some government officials in consultation. At the same time, projects that depended on institutional collaboration, such as civic complaint platforms, faced delays or reduced responsiveness during politically sensitive periods.

This illustrates a broader regional pattern i.e. elections may temporarily increase civic interest, but they also increase political sensitivity, administrative caution, misinformation risk, and state monitoring. Even where formal space exists, the operating environment becomes more restrictive in practice.

Monitoring evidence also shows how digital engagement itself is shaped by platform and contextual pressures. In some initiatives, youth participants were highly successful in generating digital content and engagement, including videos and social media posts with significant reach. However, retention of governance-related learning and sustained civic action was more limited, suggesting that while participation is encouraged at the level of

expression, it is less supported at the level of accountability. This reflects a wider ecosystem where visibility is easier than influence.

Managed civic closure also changes civil society behavior. Organizations may shift toward less confrontational themes, focus on service delivery, avoid rights language, reduce online criticism, or frame civic work as digital literacy, youth empowerment, or public-service improvement. Monitoring reports suggest that this is not only a strategic choice but often a practical necessity. Projects framed around neutral or developmental themes such as digital skills, misinformation awareness, or service delivery were more likely to secure participation and institutional engagement than those framed explicitly around rights or political accountability. These adaptations may help organizations survive, but they can also dilute democratic advocacy if not balanced with long-term rights strategies.

In Afghanistan, civic closure has become extreme. DDI could not materialize a single project in the country due to non-availability of banking channels to remit funds to selected organizations. In Pakistan, it is legal-regulatory and political. In Bangladesh, it is linked to cyber law, shutdowns, and political volatility. In Sri Lanka, it is associated with online-safety regulation and post-crisis governance. In Nepal, the risk is emerging through platform regulation. In India, civic closure is uneven, operating through platform pressure, shutdowns, legal requirements, and political polarization. Maldives and Bhutan have different risk profiles but still require stronger institutional safeguards.

The regional character of civic closure means that digital democracy support cannot be designed only at national level. It must include comparative learning, regional early warning, shared legal analysis, and protective networks. Monitoring evidence shows that while local initiatives can succeed, they operate within shared regional constraints. Addressing these constraints therefore requires approaches that go beyond individual countries and engage with the broader ecosystem shaping digital civic space across South Asia.

3. Digital governance and civic space restrictions

Digital governance has become one of the most important arenas in which civic space is being defined in South Asia. Governments across the region are adopting cybercrime laws, online safety laws, social media rules, data protection frameworks, cybersecurity strategies, platform registration requirements, AI rules, and public-sector digital transformation policies. Some of these reforms respond to real governance needs. States do need cybersecurity systems, data protection, safeguards against online fraud, rules against technology-facilitated violence, and mechanisms to address harmful digital conduct.

The problem arises when these frameworks are defined in broad language, enforced selectively, or placed under executive-controlled bodies without adequate judicial oversight. In such cases, laws that are presented as tools for safety, security or misinformation control can very well become instruments for shrinking civic space. The civic-space concern is therefore not only the existence of digital regulation. It is the design, scope, enforcement and institutional control of that regulation.

The DDI Digital Divide research describes this effect as a chilling environment. Awareness of restrictive laws and surveillance possibilities reduces citizens' willingness to engage online. This is the core governance problem as when digital laws create uncertainty, citizens and organizations begin regulating themselves before the state even acts.

Across South Asia, at least seven regulatory tools are now shaping civic space: cybercrime laws, online safety laws, social media registration regimes, platform takedown powers, internet shutdowns and throttling, data and surveillance frameworks, and NGO/funding compliance controls. These tools vary by country, but they create a

common regional pattern: civic actors operate in a digital environment where legal boundaries are unclear, state discretion is wide, and the cost of speaking can be unpredictable.

3.1 Cybercrime laws and the criminalization of expression

Cybercrime laws are the most common digital regulatory tools used in the region. They are usually justified as necessary for preventing fraud, hacking, cyber harassment, identity theft, misinformation and threats to national security. These are legitimate concerns. However, the same laws often include vague offences related to "false information," "public order," "national security," "religious sentiment," "defamation," "anti-state activity," or "offensive" content. Such wording allows authorities to treat ordinary civic speech, journalism, satire, criticism, rights advocacy or political commentary as a criminal matter.

Pakistan's Prevention of Electronic Crimes Act, 2016 (PECA) illustrates this pattern. The 2025 amendments created a stronger social media regulatory framework and introduced offences relating to "false and fake information" (National Assembly of Pakistan, 2025).[6] The amendment provides for removal or blocking of such information within a short time frame, while rights groups have warned that the vague wording can chill online expression. Journalism bodies and digital rights activists criticized the amendments as a threat to press freedom because they created a social media regulatory authority, investigation agency and tribunals, with penalties including imprisonment and fines for spreading "false or fake" information.

Bangladesh has followed a similar trajectory, although through successive replacement of laws rather than a single regulatory framework. The Digital Security Act 2018 was widely criticized as repressive, particularly for its impact on online expression and journalism. It was subsequently replaced by the Cyber Security Act 2023, which retained much of the earlier framework while aiming to regulate digital security and online activity. The International Centre for Not-for-Profit Law (ICNL) Cyber Security Act Handbook[7] (ICNL, 2024) notes that the law was introduced to repeal the Digital Security Act and regulate digital activity, but raised concerns due to its similarity to the earlier legislation and its potential impact on freedom of expression.

The regulatory framework continued to evolve with the introduction of the Cyber Security Ordinance 2025. A description of the ordinance highlights that it establishes a comprehensive cybersecurity framework, including provisions on critical infrastructure protection, enforcement mechanisms, and penalties for cyber-related offences. At the same time, rights organizations have argued that newer digital governance frameworks do not adequately address underlying structural concerns. A joint statement by Human Rights Watch[8] (HRW, 2025) on emerging digital laws in Bangladesh notes that draft cyber protection and data protection frameworks fail to address broader systemic challenges in line with constitutional and international human rights standards.

3.2 Online safety laws and the regulation of "harmful" content

A second major tool is the online safety framework. These laws are often presented as necessary to address cyberbullying, child protection, online abuse, misinformation and harmful digital conduct. Again, the policy rationale is not inherently illegitimate. The problem is that "online safety" can become a broad umbrella for state intervention in public debate.

Sri Lanka's Online Safety Act 2024 is the clearest example. The law established an Online Safety Commission and created mechanisms to act against prohibited or false online statements. INCL notes that the Act prohibits communication of "false statements" deemed threats to national security, public health, public order or inter-

[6] https://www.na.gov.pk/uploads/documents/679255ee36f45_595.pdf
[7] https://www.icnl.org/wp-content/uploads/Bangladesh-CSA-Handbook-Nov-2024.pdf
[8] https://www.hrw.org/news/2025/02/25/joint-statement-emerging-digital-laws-bangladesh

group harmony, and grants the Commission powers to remove content, restrict access and initiate proceedings against individuals and organizations, with penalties including fines and imprisonment (ICNL, 2026)[9].

Reporting by Associated Press confirms that the law enables government authorities to remove online content and pursue legal action against internet users, while critics have described it as a threat to freedom of expression, particularly in a politically sensitive and post-crisis context[10] (AP, 2024). The concern is not that online harms should be ignored. The concern is that broad terms such as false statement, public order, hostility, national security or harmful content can be stretched to include criticism of public officials, reporting on corruption, minority-rights advocacy, satire, or mobilization around protests.

Online safety laws therefore create a particular kind of civic risk. They do not necessarily ban organizations or media houses. Instead, they create uncertainty about whether a post, video, cartoon, campaign, public-interest investigation or civic appeal may later be categorized as false, harmful or destabilizing. That uncertainty is sufficient to produce self-censorship, even in the absence of direct enforcement.

3.3 Social media registration, local presence and platform licensing

A third regulatory tool is the requirement that social media platforms register with the state, appoint local representatives, establish local offices or comply with national content-removal instructions. On paper, these measures are defended as ways to make platforms accountable. In practice, they can also create leverage over platforms and increase state influence over online speech.

Nepal's Social Media Bill 2081, tabled in 2025, reflects this emerging trend. Analyses of the bill note that it would require social media platforms to register in Nepal, appoint legal representatives and remove content deemed harmful or illegal. A legal review highlights that the bill proposes penalties for non-compliance and establishes obligations for platforms to operate under national jurisdiction (LawGandhi,2025)[11].

A legal analysis prepared under the auspices of UNESCO notes that the bill would empower authorities to issue directives to platforms for the removal of content considered illegal and to refer such content to other competent authorities for action (UNESCO, 2025)[12].

The risks became visible when Nepal moved to block major platforms that had not complied with registration requirements. In September 2025 Nepal blocked several major platforms, including Facebook, X and YouTube, after they failed to register and appoint a liaison office, prompting warnings that such measures could be used for censorship and suppression of dissent.

The social and political consequences were severe. Mass "Gen Z" protests following the ban resulted into deaths and injuries during the crackdown, after which the restrictions were eventually lifted. The Gen Z 'revolution' caused a major political change by overthrowing the government and the country ultimately elected a new government in March 2026. This episode shows how platform registration rules can move quickly from administrative regulation to civic crisis. If citizens rely on global platforms for communication, protest organization, journalism, emergency information and public debate, blocking those platforms is not a technical compliance action, it is taken as a restriction on civic life.

In India, the regulatory challenge is shaped by a combination of strong intermediary rules, expansive takedown powers, platform pressure and periodic internet shutdowns, alongside the rapid expansion of digital public infrastructure. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

[9] https://www.icnl.org/resources/civic-freedom-monitor/sri-lanka
[10] https://apnews.com/article/sri-lanka-internet-bill-freedom-of-expression-wickremesinghe-527e0195a8f8f76573aa8d7185562b12
[11] https://www.lawgandhi.com/social-media-bill-2081-2025/
[12] https://articles.unesco.org/sites/default/files/medias/fichiers/2025/03/SM%20bill%20legal%20Analysis%20%282%29.pdf

require platforms to exercise due diligence, remove content upon government or court orders, and appoint local compliance officers, with potential liability for non-compliance. Civil society organizations have argued that these provisions, particularly those enabling expedited content takedowns and traceability requirements, risk undermining freedom of expression and user privacy. A joint submission by Access Now and partner organizations has called for review of the IT Rules, warning that amendments must ensure safeguards for freedom of expression, association and privacy, and must include judicial oversight and transparency mechanisms (Access Now, 2022)[13].

This creates a structural tension in India's digital ecosystem. On the one hand, the country has developed one of the most extensive digital public infrastructures in the region, enabling large-scale access to services and digital transactions. On the other, regulatory pressures on platforms, combined with shutdown practices and broad content-control provisions, shape the conditions under which citizens can engage online. As a result, high levels of digital access coexist with contested civic space, reinforcing the broader regional pattern where digital capacity expands faster than protections for digital freedom.

3.4 Takedown powers, blocking orders and executive-controlled regulators

A fourth tool is the creation of regulatory authorities with powers to order content removal, block access, impose penalties, suspend services, or direct platforms. These bodies are often placed under executive influence, raising concerns about independence and due process.

Pakistan's 2025 PECA amendments created the Social Media Protection and Regulatory Authority, with powers to regulate and remove online content. Commentary from legal and policy sources has described the authority as having wide powers over content deemed unlawful or offensive, including the ability to block or suspend platforms. Commentary from legal and policy sources notes that the authority has broad powers over content deemed unlawful or offensive, including the ability to block or suspend platforms, raising concerns about overreach and lack of independent oversight (SAHSOL, 2025)[14].

Sri Lanka's Online Safety Commission raised a similar concern. A joint civil society letter highlighted that the proposed commission lacks independence because its members are appointed by the executive, and warned that vague offences could lead to over-censorship and self-censorship (Committee to Protect Journalists, 2024)[15].

Maldives has also moved toward a more centralized media regulatory structure. The Maldives Media and Broadcasting Regulation Act, ratified in September 2025, replaced two previous regulatory bodies with a new commission. International Institute for Democracy and Electoral Assistance (IDEA) notes that the law is intended to address disinformation and defamation concerns, but has raised questions about its impact on media independence (International IDEA, 2025)[16].

Regulatory bodies in the region ordinarily lack independence, content regulation becomes vulnerable to political use. Even when the stated goals are combating fake news, defamation, hate speech or public disorder, the absence of safeguards can turn regulation into intimidation.

3.5 Internet shutdowns, throttling and access disruption

A fifth regulatory tool is the direct disruption of access. Shutdowns, throttling, platform blocks and service suspensions are among the most severe restrictions because they do not target specific unlawful content; they disable communication infrastructure itself.

[13] https://www.accessnow.org/press-release/india-it-rules-amendments-joint-submission/
[14] https://sahsol.lums.edu.pk/node/25604
[15] https://cpj.org/wp-content/uploads/2024/01/Sri-Lanka-Joint-Letter.pdf
[16] https://www.idea.int/democracytracker/report/maldives/september-2025

Afghanistan is the extreme case. In 2025, Taliban authorities restricted fiber-optic internet in several provinces and later imposed wider disruptions, citing moral and social concerns. Reporting by Al Jazeera notes that telecommunications were cut after authorities restricted fiber-optic connections in multiple provinces to prevent what they described as "vice" (Aljazeera, 2025)[17]. After people took to the streets in rare protests against regime, the administration restored the internet communications (BBC, 2025)[18].

Bangladesh's digital divide evidence and monitoring environment also point to shutdown risk around civic mobilization. The DDI digital divide study records exposure to internet disruptions in Bangladesh, particularly around moments of protest and political tension. While these conditions do not always amount to formal shutdowns, they demonstrate how political sensitivity can constrain civic activity even where digital access remains technically available.

Nepal's 2025 platform-blocking episode also falls into this category. Although framed as enforcement of registration rules, blocking major platforms had the practical effect of restricting citizens' access to communication channels used for public debate and mobilization.

Access disruption is especially damaging for civil society because it interrupts campaigns, trainings, virtual meetings, documentation, emergency response, evidence-sharing and media outreach. It also affects education, livelihoods and public services. For marginalized groups, women, rural communities and activists, the shutdown or restriction of digital channels can mean sudden isolation from both civic networks and essential services.

3.6 Data protection, surveillance and the paradox of privacy laws

Data protection laws are often seen as protective, and in principle they are essential for digital democracy. Citizens need safeguards over how their personal information is collected, stored, shared and used. However, in South Asia, data protection frameworks often develop alongside expanding surveillance capacity, digital identity systems and weak oversight. This creates a paradox as privacy laws may exist on paper, while citizens still fear state or platform misuse of data.

Bangladesh's 2025 Personal Data Protection Ordinance is part of a wider digital-governance package, alongside the Cyber Security Ordinance. Policy material from the UNESCO notes that Bangladesh adopted both instruments in 2025 as part of its expanding digital governance framework, covering data protection, cybersecurity and digital regulation (UNESCO, 2025)[19].

Sri Lanka has established a personal data protection framework and a Data Protection Authority under its Personal Data Protection Act, while simultaneously adopting the Online Safety Act[20]. Pakistan's digital policy language refers to privacy and data governance, but a comprehensive rights-based data protection regime remains incomplete. The Digital Pakistan Policy outlines commitments to data protection and privacy, yet a fully operational and rights-enforcing legal framework has not been implemented.

Data governance cannot be separated from political trust. If citizens believe that their online activity, identity data, location information or communications can be monitored or misused, they may avoid civic engagement even when platforms remain technically accessible. The DDI Digital Divide research captures this through reported surveillance fears and self-censorship.

For civil society organizations, the risk is even higher. They collect participant data, beneficiary lists, training records, digital campaign analytics, complaint information and sometimes sensitive testimonies. Weak data

[17] https://www.aljazeera.com/news/2025/9/30/afghanistan-imposes-internet-blackout-what-has-the-effect-been-so-far
[18] https://www.bbc.com/news/articles/c0jq2q5jnw3o
[19] https://www.undp.org/sites/g/files/zskgke326/files/2025-11/final_digital_bangladesh_ai_ram.pdf
[20] https://www.dlapiperdataprotection.com/index.html?t=law&c=LK

protection can endanger activists, minorities, women, journalists and local communities. This is why digital democracy programming must include secure data practices, not only public communication.

3.7 Cybersecurity strategies and critical infrastructure controls

Cybersecurity strategies can strengthen digital resilience, but they can also broaden state authority over networks, systems, platforms and information flows. The difference lies in safeguards, transparency and the separation between technical security and political control.

Bhutan provides a more developmental example. Its National Cybersecurity Strategy 2024–2029 lays out a plan to secure cyberspace in alignment with digital transformation goals, including cybersecurity governance, legislation, critical infrastructure protection and incident response. The strategy emphasizes resilience, institutional coordination and protection of digital infrastructure (Govt Tech, 2025)[21]. In Bhutan's case, the risk is not the same as in Pakistan or Sri Lanka as the issue is ensuring that cybersecurity modernization remains rights-sensitive and does not become a future pathway for overbroad control.

Bangladesh's Cyber Security Ordinance also includes institutional and critical infrastructure measures. Such frameworks are necessary for protecting public systems, but they must clearly distinguish cyberattacks and infrastructure threats from civic speech, journalism and public debate.

The broader regional issue is that "cybersecurity" can become an elastic term. If cybersecurity is interpreted to include national reputation, public order, political stability or control of misinformation, it can easily become a justification for restricting civic activity.

3.8 NGO regulation, funding compliance and administrative pressure

Digital civic space is also shaped by non-digital laws. NGO registration regimes, foreign funding restrictions, audit requirements, tax scrutiny, banking compliance and administrative permissions all affect whether civil society organizations can function effectively. These tools are often treated as routine governance measures, but in practice they shape the boundaries of civic action, including digital engagement. When access to funding is restricted, approvals are delayed, or compliance burdens are intensified, organizations may limit their activities, avoid sensitive issues, or reduce their public visibility.

India provides a clear example of how non-digital regulation affects digital civic space. Amendments to the Foreign Contribution (Regulation) Act (FCRA) have tightened rules on foreign funding, restricted sub-granting, and increased compliance requirements for civil society organizations. These changes have led to the suspension or cancellation of licenses for thousands of organizations, constraining their ability to operate and engage in advocacy. Authorities use (FCRA) to harass outspoken rights groups and restrict their ability to obtain foreign funding (HRW, 2020)[22]. Similarly, financial and regulatory restrictions have forced some organizations to scale down or cease operations altogether, including in areas related to human rights and civic engagement. While these measures are not framed as digital regulation, they directly affect the ability of organizations to sustain online campaigns, digital advocacy and civic engagement.

In practice, digital democracy organizations across South Asia (Pakistan, Nepal, Bangladesh, Sri Lanka) face overlapping compliance burdens. They may need to satisfy NGO regulators, donor requirements, cybercrime laws, platform policies, data protection obligations, tax authorities and local administrative expectations simultaneously. This creates a dense and often opaque regulatory environment in which compliance becomes

[21] https://tech.gov.bt/national-cybersecurity-strategy/
[22] https://www.hrw.org/world-report/2020/country-chapters/india

resource-intensive. For many organizations, particularly smaller ones, the risk of inadvertent non-compliance or selective enforcement becomes a deterrent in itself.

The DDI mapping survey shows that many organizations are formally registered and willing to participate in digital democracy programming, but institutional capacity remains uneven. The DDI Digital Divide and monitoring evidence further indicate that smaller civil society organizations often lack cybersecurity protocols, data protection systems, analytics capacity and legal-risk preparedness. This means that regulatory pressure does not affect all actors equally. Larger organizations with legal teams and compliance systems may be able to absorb these burdens. Smaller, community-based groups, however, are more likely to respond by self-censoring, narrowing their thematic focus, or avoiding politically sensitive work altogether.

This creates an uneven civic ecosystem. Digital participation may appear vibrant at the surface, but the underlying field is shaped by differential capacity to manage risk. Over time, this can lead to a concentration of voice among better-resourced actors, while grassroots organizations, often closest to marginalized communities, withdraw from more contentious forms of civic engagement.

3.9 Regulatory ambiguity and compliance burden on civic actors

Across South Asia, one of the most consequential features of the digital environment is not only restriction, but uncertainty. Laws governing online speech, platform use, data, cybersecurity and public order are often drafted in broad or overlapping terms, leaving significant room for interpretation. For civil society organizations, journalists and digital activists, this creates a “scary” form of regulatory ambiguity. It is not always clear what constitutes unlawful speech, what triggers enforcement, or how rules will be applied in practice. This uncertainty is reinforced by selective or inconsistent enforcement, where similar forms of expression may be tolerated in some cases and penalized in others. As a result, the boundary of permissible speech is not defined by law alone, but by perceived risk.

Monitoring evidence and Digital Divide research consistently show that this leads to self-censorship, cautious messaging and avoidance of politically sensitive issues. The effect is cumulative: over time, civic actors internalize the limits of the system and adjust their behavior even in the absence of direct sanctions.

At the same time, compliance burdens are distributed unevenly across the digital ecosystem. Civil society organizations are required to navigate complex layers of regulation, NGO registration, funding restrictions, tax compliance, cybercrime laws, platform policies and data protection requirements, often with limited institutional capacity. Journalists and independent media face similar pressures, including legal exposure, licensing requirements and editorial constraints.

By contrast, large technology companies, despite being central to the digital public sphere, are often better equipped to absorb regulatory demands, negotiate with governments, or adapt compliance systems at scale. In some cases, regulatory frameworks formally target platforms, but in practice shift the burden onto users through content removal, account restrictions or liability risks. This creates an asymmetry where smaller civic actors bear higher operational and legal risk relative to their resources, while larger platforms retain structural advantages.

3.10 Comparative country pattern

In Pakistan, digital governance has shifted toward stronger content regulation through PECA, new authority structures, false-information offences and platform-control powers. The result is a high-risk environment for journalists, rights defenders, political actors and civil society.

In Bangladesh, the replacement of the Digital Security Act with newer cyber frameworks has not removed civic-space concerns because broad cyber regulation, shutdown exposure and political volatility continue to affect trust.

In Sri Lanka, the Online Safety Act illustrates how online harm regulation can create a chilling effect when broad offences and executive-linked regulatory institutions are used to control digital speech.

In Nepal, platform registration and content-control proposals show how a state can move from under-regulation to overbroad control. The 2025 platform-blocking episode shows how quickly administrative rules can become a civic crisis.

In India, the regulatory challenge lies in strong intermediary rules, takedown powers, platform pressure, shutdowns and the tension between digital public infrastructure and civic freedoms. Civil society groups have called for review of the IT Rules, 2021 and warned that amendments must protect freedom of expression, association and privacy.

In Maldives, the concern is growing media regulation and institutional control. The 2025 media law created a new commission with sanctioning powers, raising press freedom concerns.

In Bhutan, the legal environment is less confrontational, but cybersecurity modernization, funding requirements, defamation laws and limited institutional safeguards still require attention. CIVICUS has flagged restrictive funding requirements, defamation laws and constraints on civil society and journalists.

In Afghanistan, the problem is no longer regulatory ambiguity alone but direct coercive control over connectivity, platforms, women's access and information flows.

4. Platform power and civic participation

Digital platforms now shape civic participation across South Asia. Facebook, YouTube, TikTok, X, WhatsApp, Instagram, and messaging platforms are not merely tools of communication. They determine visibility, speed, reach, amplification, moderation, and monetization.

Civil society organizations depend on platforms, but they do not control their rules. Algorithms reward content that generates attention, reaction, emotion, outrage, humor, spectacle, or identity-based mobilization. As a result, populist and polarizing narratives often travel faster than careful policy content.

For civil society, this creates a strategic dilemma. To remain visible, organizations often feel pressure to simplify, dramatize, personalize, or emotionalize complex governance issues. This may help reach audiences, but it can also weaken policy depth. The risk is that civic actors begin to adopt the communication logic of platforms rather than shaping platforms for civic purposes.

Monitoring evidence across DDI-supported initiatives reflects this tension. Youth-focused digital programs have been particularly successful in generating content and engagement, including dozens of outputs and, in some cases, high viewership. However, learning retention has often been uneven. Participants tend to engage more strongly with content creation, storytelling and digital visibility than with deeper themes such as governance, rights or accountability. This suggests that while platforms are effective for entry-level engagement, they are less reliable for sustained civic learning unless deliberately structured.

Lal Sabuj Society in Bangladesh trained 21 young people and generated more than 60 content pieces. Some videos crossed 10,000 views. However, monitoring also found that participants remembered ethical journalism and content creation more vividly than the human rights governance component.

More layered interventions show what works better. Creative approaches such as art-based civic messaging, interactive tools, and simulated democratic processes, have demonstrated stronger links between participation and understanding. These models use platform-friendly formats but anchor them in civic learning, helping bridge the gap between expression and comprehension. Similarly, community-based training on misinformation and digital safety has shown strong uptake, particularly among youth and marginalized groups, but requires follow-up structures to translate skills into civic action.

At the same time, monitoring evidence highlights structural constraints. Connectivity limitations, device access, and resource gaps continue to affect participation, especially in remote or marginalized communities. Even where engagement is high, sustainability remains a challenge: content production may continue beyond project targets, but without institutional support, moderation systems, or strategic direction, its long-term civic impact remains uncertain.

The platform lesson is clear. South Asian civil society cannot avoid platforms, but it must avoid becoming dependent on their logic. Digital visibility is not the same as civic influence. Organizations need strategies that combine reach with credibility, safety, evidence and long-term engagement.

Platform power should therefore be treated as a structural democratic issue.

5. Civil society capacity and institutional gaps

Evidence across South Asia shows a large, diverse and motivated civil society ecosystem with strong interest in digital engagement. The DDI Mapping Survey, covering 407 organizations across eight countries, reflects a broad base of actors working across youth empowerment, human rights, gender inclusion, civic participation, peacebuilding and accountability. Organizations are already engaging with digital tools for communication, mobilization and outreach, and most report willingness to expand their digital work. This indicates that the constraint is not lack of interest or relevance, but the conditions under which this interest can be translated into sustained digital civic practice.

At the same time, this interest is not matched by institutional readiness. While most organizations are formally registered and operational, digital capacity remains uneven. Many organizations are able to use social media and basic communication tools, but fewer possess advanced systems such as cybersecurity protocols, digital risk management frameworks, data protection practices, analytics capacity or structured digital advocacy strategies. The DDI digital divide research reinforces this finding, showing that organizational readiness tends to cluster at basic or intermediate levels rather than at institutional maturity.

A key gap lies in the way digital tools are conceptualized. Across the region, digital engagement is often treated as an auxiliary function, primarily for visibility, communication or campaign amplification, rather than as core institutional infrastructure. This limits the ability of organizations to use digital tools for evidence generation, accountability, monitoring, coalition-building and sustained civic engagement. The result is a pattern where digital outputs increase, but their connection to governance outcomes remains weak.

Monitoring evidence illustrates this distinction. Across multiple initiatives, organizations have been able to generate strong participation, content output and community engagement using digital tools. Youth-led programs, digital literacy interventions and creative civic approaches have demonstrated clear demand and responsiveness. However, these efforts also reveal recurring gaps: limited retention of governance-related learning, weak linkages between digital engagement and institutional accountability, and insufficient follow-through mechanisms to sustain civic action. This suggests that while digital tools are effective entry points, they require deliberate structuring to translate engagement into impact.

Capacity constraints are therefore not simply technical. They reflect broader structural pressures. Civil society organizations operate within constrained funding environments, complex regulatory regimes and evolving digital risks. Compliance requirements, legal uncertainty and resource limitations shape how organizations prioritize their work. Smaller and community-based organizations, in particular, often lack the financial and institutional capacity to invest in cybersecurity, legal preparedness, data systems or long-term digital strategies. As a result, they may focus on short-term, low-risk activities rather than sustained or rights-based engagement.

This creates an uneven civic landscape. Larger organizations with access to resources, expertise and institutional support are better positioned to absorb compliance burdens and experiment with digital tools. Smaller actors, often closest to marginalized communities, face higher relative risk and are more likely to limit their engagement or avoid sensitive issues. Over time, this can narrow the diversity of voices in digital civic space, even as overall participation appears to expand.

The overall picture is therefore one of high intent but constrained capacity. The region has strong civic energy, creativity and demand for digital engagement. However, this must be matched by investment in institutional systems. Digital democracy programming should move beyond one-off trainings and content generation toward building durable organizational capacity—covering digital security, legal literacy, data systems, monitoring and learning, and strategic integration of digital tools into core civic functions.

5.1 Capacity needs emerging from evidence

The evidence points to several capacity needs. Civil society organizations need digital security capacity. This includes secure communications, password practices, device safety, phishing awareness, protection from online harassment, and protocols for staff and beneficiaries.

Legal literacy: Cybercrime laws, platform rules, data protection obligations, and online safety provisions are increasingly complex. Organizations need to understand what they can safely do, how to reduce risk, and how to respond to legal threats.

Data and monitoring systems: Many digital projects produce content, but fewer track meaningful engagement, behavioral change, civic action, institutional response, or policy uptake.

Platform strategy: Organizations must understand algorithms, moderation rules, analytics, audience segmentation, and risks of platform dependency.

Sustainability planning: Digital pages, tools, apps, and networks require ownership, moderation, hosting, maintenance, safety protocols, and ongoing resources after project completion.

Inclusion systems: Participation of women, minorities, indigenous communities, persons with disabilities, refugees, IDPs, and gender minorities cannot be assumed. It must be designed, budgeted, monitored, and protected.

6. Regional political fractures and spillover effects

Regional politics strongly shape digital democracy in South Asia. Civic actors do not operate only within national digital environments. They also operate within a region marked by interstate mistrust, conflict narratives, border tensions, refugee flows, exile politics, securitized nationalism, and polarized media ecosystems.

Afghanistan has no foreseeable democratic restoration pathway under current conditions, leaving civil society without meaningful domestic protection. Bangladesh and Nepal faced growing democratic uncertainty unless the elections in February and March brought back some sense of stability. Sri Lanka's post-bankruptcy environment has narrowed civic mobilization despite relatively greater openness. India and Pakistan's adversarial relationship

restricts cross-border civic exchange. These dynamics weaken regional solidarity and reduce trust needed for cooperation.

Digital platforms partly overcome these barriers, but they also reproduce nationalist narratives, misinformation, and surveillance risks. Cross-border digital cooperation can be branded as foreign interference, especially in politically sensitive contexts. Civil society organizations may avoid regional collaboration because of reputational, legal, or security concerns.

Another structural factor shaping digital democracy in South Asia is the weakening of regional economic and political interconnectedness. Traditionally, geographic proximity and shared histories created the basis for regional exchange, cooperation and learning. However, in recent years, economic trajectories and policy directions across key countries, particularly India, Pakistan and Afghanistan, have become increasingly disconnected from one another.

This shift is reinforced by strained bilateral relations and limited cross-border engagement. Trade, mobility, institutional collaboration and information flows across borders have all narrowed, reducing opportunities for shared problem-solving and regional civic cooperation. In practical terms, proximity is no longer translating into connectivity. Instead, it often introduces additional political sensitivity, regulatory barriers and risk for civil society actors attempting cross-border engagement.

These trends are also reflected in evolving international classifications and development frameworks. From September 2025, the World Bank regrouped Pakistan and Afghanistan within broader Middle East and Africa analytical clusters, rather than South Asia, for certain operational and analytical purposes[23] (The Diplomatic Insight, 2026). While largely administrative, this shift reflects a growing recognition that economic pathways, governance challenges and development trajectories in parts of the region are diverging rather than converging.

For digital democracy, this fragmentation has important implications. It limits the scope for regional learning, weakens cross-border solidarity among civil society actors, and reduces the potential for coordinated responses to shared challenges such as misinformation, platform governance, digital rights and civic space restrictions. As a result, digital civic ecosystems are becoming more nationally bounded, even as digital platforms themselves remain transnational.

This is why digital democracy cooperation in South Asia must be carefully designed. It should not begin with highly visible political declarations. It should begin with issue-based, protective, technical, and learning-oriented cooperation.

Afghanistan requires special treatment. Domestic civil society is severely constrained, so diaspora and exile-led networks become essential. Pakistan and India require low-visibility issue-based engagement because bilateral hostility affects civic exchange. Bangladesh, Nepal, Sri Lanka, Maldives, and Bhutan offer more space for thematic cooperation, but each has its own regulatory and political sensitivities.

Regional spillovers are also visible in misinformation and online harm. Political narratives, religious tensions, ethnic conflicts, and migration anxieties travel across borders. Digital repression models also travel. Laws framed around fake news, online safety, cybercrime, or national security increasingly resemble one another across the region.

[23] https://thediplomaticinsight.com/what-pak-reclassification-to-mena-means/

7. Strategic openings and the case for regional cooperation

Entry points: Despite tightening restrictions, meaningful openings for digital democracy persist across South Asia. These openings are not uniform, but they provide workable entry points where civic engagement can continue with reduced political friction. Issue-based engagement remains particularly viable. Themes such as climate resilience, labour rights, migration, youth participation, women's empowerment, digital safety, misinformation, public-service accountability and local governance allow civil society to operate within acceptable boundaries while still strengthening democratic practice. These areas may not always be framed as political, but they build the foundations of participation, awareness and accountability.

Local interventions: Evidence from ongoing initiatives shows that small, locally grounded interventions can generate meaningful outcomes when they are context-sensitive and practically designed. Community-based programs, youth engagement models and accessible digital tools have demonstrated the ability to build participation and awareness even in constrained environments. The lesson is not about scale but effectiveness: interventions that are embedded in local realities, inclusive in design and linked to everyday civic concerns are more likely to sustain engagement and produce tangible results.

Regional learning: Even as formal interstate cooperation weakens, regional learning continues through civil society networks. Organizations are sharing tools, methods and experiences across borders, including digital safety practices, legal updates, advocacy approaches, monitoring frameworks and civic-tech innovations. These exchanges provide an important layer of resilience, allowing actors to adapt to restrictive environments by learning from comparable contexts. In a fragmented region, such informal knowledge flows are increasingly critical.

Diaspora networks: Diaspora and exile-led networks are becoming central to sustaining civic engagement in high-risk environments. This is particularly relevant for Afghanistan and for activists facing pressure within their own countries. These networks contribute to documenting violations, preserving institutional memory, enabling secure communication and maintaining continuity of civic work beyond national constraints. They also serve as bridges between local realities and international advocacy spaces.

Confidence building: Digital democracy initiatives can also function as confidence-building mechanisms in a politically fragmented region. While they cannot resolve broader geopolitical tensions, they help sustain civic relationships across borders. Low-visibility cooperation on digital safety, misinformation response, women's online participation and public-service accountability enable continued engagement even where formal political channels are limited. In this sense, digital civic work becomes a means of preserving regional connection in the absence of political alignment.

Digital bridging: In a region marked by growing political and economic divergence, digital tools offer practical pathways to sustain limited but meaningful cross-border civic connection. Rather than relying on formal interstate cooperation, civil society can engage through low-visibility, decentralized mechanisms such as shared knowledge platforms, multilingual content exchanges, and issue-based collaboration on themes like climate resilience, digital safety, misinformation and public-service accountability. These approaches reduce political sensitivity while enabling continued learning and coordination. Diaspora networks and remote collaboration models further extend this space, providing neutral channels for dialogue, documentation and exchange where domestic conditions are restrictive.

At the same time, digital engagement must be anchored in resilience and trust. Shared digital safety protocols, secure communication systems, and adaptable civic-tech tools can allow organizations to collaborate without exposing themselves to undue risk. Subnational partnerships, remote fellowships and cross-border misinformation monitoring can sustain cooperation at a functional level even in fragmented political contexts. The

objective is not to recreate regional integration, but to maintain connective tissue, ensuring that civic knowledge, practices and solidarity continue to circulate across borders despite broader geopolitical constraints.

7.1 Strategic openings by country

In Afghanistan, civic space within the country remains severely constrained, shifting the locus of engagement outward. Strategic openings lie in supporting secure access to information, women's learning and digital inclusion, diaspora-led initiatives, documentation of rights conditions and protective mechanisms for at-risk actors. The focus is less on expansion and more on preservation and protection of civic capacity.

In Bangladesh, opportunities are strongest in youth-centered engagement, digital literacy, misinformation response and locally grounded civic tools. Work with marginalized and indigenous communities also remains important. However, initiatives must be designed with awareness of political sensitivity, including potential shutdowns and regulatory risks, requiring built-in flexibility and resilience.

Bhutan presents a relatively open environment for developmental approaches. Opportunities lie in civic-tech innovation, youth engagement in environmental and local governance issues, digital literacy and community-level monitoring of public services. The priority is to translate access into meaningful participation before restrictive dynamics emerge.

In India, scale and diversity make subnational engagement the most effective entry point. State-level initiatives, language-specific interventions, misinformation literacy, privacy awareness and digital fraud prevention offer practical pathways. Expanding civic space and access to digital public systems for marginalized communities also remains a key area of engagement.

In Maldives, the focus is on strengthening trust in digital systems. Priorities include affordability, privacy protections, youth participation, digital livelihoods and public confidence in emerging regulatory frameworks. Ensuring that governance keeps pace with digital expansion is central to sustaining civic engagement.

Nepal's openings lie in strengthening local governance, improving legal literacy and addressing geographic barriers to connectivity. Balanced approaches to platform regulation, combined with youth engagement and community-level participation, can help shape a more inclusive digital ecosystem.

In Pakistan, the most viable entry points center on digital safety, legal awareness and secure civic engagement. Expanding women's digital access, strengthening misinformation resilience, supporting public-service accountability and enabling safer communication channels are critical to sustaining participation in a constrained environment.

In Sri Lanka, openings exist in monitoring the implementation of digital laws, improving usability of e-governance systems and strengthening digital literacy. Youth-led civic-tech initiatives and post-crisis accountability processes provide additional pathways for engagement, particularly where regulatory frameworks remain contested.

8. Recommendations for ecosystem actors

8.1 For donors

Donors should treat digital democracy in South Asia as an ecosystem challenge rather than a set of isolated communication or innovation projects. The brief shows that the region is becoming more digitally connected and more digitally governed, but not necessarily more digitally democratic. This means funding should prioritize the conditions that make digital participation safe and meaningful: digital security, legal literacy, data protection, monitoring systems, platform strategy, and regional learning. Short-term outputs such as trainings, videos, social

media posts or digital campaigns can be useful, but they should not become the main measure of success. The priority should be durable civic capacity.

Donors should support regional and cross-border initiatives that focus on digital safety, learning and coordination, but these initiatives must be politically sensitive and low-visibility where necessary. In a fragmented region, especially with strained India-Pakistan, Pakistan-Afghanistan and India-Afghanistan relations, regional cooperation cannot depend on formal state channels. Donors can instead support quiet practitioner exchanges, shared digital safety protocols, legal update mechanisms, regional helpdesks, remote fellowships, and multilingual knowledge repositories. These tools can preserve regional civic connection without exposing organizations to unnecessary political risk.

Funding should also move from project outputs to shared infrastructure. Civil society organizations across the region need pooled access to cybersecurity expertise, legal advice, secure hosting, data-protection templates, monitoring tools, fact-checking resources, and platform analytics support. Smaller and community-based organizations are often closest to marginalized groups but least able to absorb compliance and digital-risk burdens. Donor support should therefore create common systems that smaller organizations can use without having to build everything independently.

Flexible funding is essential. Digital civic space in South Asia can change suddenly because of elections, shutdowns, platform bans, cyber-law amendments, political unrest or regulatory pressure. Rigid workplans are poorly suited to this environment. Donors should allow adaptive programming, contingency budgets, emergency legal and digital security support, and adjustments to implementation timelines when civic conditions deteriorate. This is especially important in contexts such as Afghanistan, Pakistan, Bangladesh, Nepal and Sri Lanka, where political or regulatory shifts can quickly affect civic activity.

Finally, donors should invest in evidence and learning. The DDI experience shows the value of mapping, digital divide research and monitoring evidence in understanding where capacity exists and where systems remain weak. Future support should include stronger monitoring of whether digital activities actually lead to civic outcomes: safer participation, institutional response, improved accountability, sustained networks, and inclusion of women, minorities, rural communities and other marginalized groups.

8.2 For civil society organizations

Civil society organizations should treat digital engagement as an institutional strategy rather than a communications function. Being visible online is not the same as being digitally capable. Digital capability requires secure communications, data protection, legal awareness, platform strategy, analytics, response plans for online harassment, and clear links between online engagement and offline civic action. Organizations should therefore move beyond ad hoc social media activity and integrate digital tools into advocacy, evidence generation, coalition-building, accountability and monitoring.

CSOs should also balance digital visibility with mission integrity. Platform algorithms reward speed, emotion and engagement, but democratic advocacy requires credibility, evidence and sustained public trust. Organizations should avoid allowing platform logic to shape their civic purpose. Content should be designed for reach, but also for accuracy, inclusion, safety and long-term advocacy goals. Campaigns should ideally connect digital engagement to concrete civic pathways such as public complaints, RTI requests, community meetings, policy submissions, legal support, public hearings or institutional dialogue.

Collective approaches are essential. Many organizations cannot individually afford cybersecurity support, legal advice, content moderation systems, secure data infrastructure or analytics tools. CSOs should therefore invest in pooled expertise, shared platforms, peer-learning networks and joint resource hubs. Stronger organizations can

mentor smaller organizations, while grassroots groups can help larger organizations remain connected to local realities. Such collaboration can reduce duplication and improve resilience across the ecosystem.

Civil society organizations also need stronger internal safeguards. They collect sensitive information, including participant data, beneficiary lists, testimonies, campaign analytics and community complaints. Weak data practices can expose activists, women, minorities, journalists and marginalized communities to harm. Every digital democracy initiative should therefore include minimum standards for consent, data minimization, secure storage, access control, retention periods and incident response.

CSOs should also build legal literacy into their work. Cybercrime laws, online safety laws, platform regulations, data protection rules and NGO compliance requirements are becoming more complex across South Asia. Organizations should know the legal risks associated with online speech, digital campaigns, participant data, cross-border collaboration and donor-funded activities. This does not mean avoiding difficult issues, but it does mean working with clearer risk assessment and preparedness.

8.3 For regulators and governments

Governments and regulators should ensure that digital governance frameworks are clear, proportionate and rights-respecting. South Asian states have legitimate reasons to address cybercrime, fraud, online abuse, child protection, misinformation and data misuse. However, laws framed around "false information," "public order," "national security," "harmful content" or "online safety" must not be so broad that they capture journalism, civic advocacy, satire, minority-rights work or criticism of public officials. Vague laws create fear even before enforcement begins.

Digital regulation should include strong safeguards: judicial oversight, transparency, independent appeals mechanisms, clear definitions, time-bound restrictions, public reporting, and protection for lawful expression. Regulatory bodies that can remove content, block platforms or impose penalties should be independent and accountable. Executive-controlled regulators risk turning content moderation into political control.

Governments should avoid internet shutdowns, throttling and platform blocking except under the strictest standards of legality, necessity and proportionality. Access disruption harms not only political communication but also education, livelihoods, emergency response, public services and community safety. For civil society, shutdowns interrupt campaigns, trainings, documentation, evidence-sharing and media outreach. They are blunt instruments with wide social costs.

Civil society consultation should be built into digital policymaking. Governments should engage journalists, digital rights groups, women's organizations, youth networks, minority groups, disability advocates, technologists, academia and community-based organizations before adopting cyber laws, AI rules, online safety laws, platform regulations or data protection frameworks. Consultation should be meaningful, documented and accessible, not symbolic.

Governments should also recognize that digital public infrastructure requires trust. Digital identity systems, payment platforms, grievance portals and service-delivery applications can improve governance, but only when citizens trust that their data will not be misused. Privacy, accountability and redress must therefore be treated as core elements of digital transformation, not secondary concerns.

8.4 For intermediaries and interlocutors

Intermediaries and interlocutors should act as connectors across a fragmented region. Their role is especially important because formal regional cooperation is weak and bilateral relations are strained. Intermediaries can support regional learning ecosystems without requiring high-profile political alignment. They can convene quiet

exchanges, produce comparative legal updates, host digital safety clinics, maintain resource libraries, and connect organizations facing similar risks.

They should also support documentation of digital repression and digital innovation. South Asia needs better comparative evidence on shutdowns, takedown orders, platform restrictions, cyber-law enforcement, online harassment, surveillance fears and civic-tech successes. Documentation should not only record violations; it should also capture what works, including safe engagement models, inclusive digital literacy methods, public-service accountability tools and youth-led civic approaches.

Protective networks should be a priority. Intermediaries can help establish rapid-response rosters for legal advice, cybersecurity incidents, account takedowns, online harassment, data breaches and emergency relocation or protection needs. These networks are particularly important for journalists, women activists, minority rights defenders, Afghan civic actors, and smaller organizations without institutional protection.

Intermediaries should also support digital bridging in a region where proximity has become politically sensitive. Low-visibility cooperation around digital safety, misinformation, women's online participation, privacy, civic-tech and public-service accountability can keep regional civic relationships alive even when formal diplomacy is limited. The goal is not to recreate regional integration from above, but to maintain civic connective tissue from below.

Finally, intermediaries should help translate between different parts of the ecosystem. Donors, grassroots groups, technologists, lawyers, digital rights advocates, public institutions and platforms often speak different languages. Intermediaries can turn legal risks into practical guidance, technical tools into usable templates, monitoring data into policy arguments, and local experiences into regional learning. In South Asia's digital democracy ecosystem, this convening and translation role is not auxiliary; it is central.

References

- Access Now. (2023). Joint submission on India IT rules amendments.
- Accountability Lab Pakistan. (2025a). Digital divide research report.
- Accountability Lab Pakistan. (2025b). Grantee mapping survey.
- Accountability Lab Pakistan. (2025c). Monitoring reports for DDI projects in Pakistan, India, Bangladesh, Nepal, Sri Lanka and Maldives.
- Al Jazeera. (2025, September 30). Afghanistan imposes internet blackout: What has the effect been so far.
- Associated Press. (2024). Sri Lanka internet bill raises freedom of expression concerns.
- BBC News. (2025). [Article on Afghanistan or regional digital restrictions].
- Centre for Law and Democracy. (2025). Maldives media regulation developments.
- Committee to Protect Journalists. (2024). Sri Lanka joint civil society letter on online safety law.
- DLA Piper. (2025). Data protection laws of the world: Sri Lanka.
- Freedom House. (2025). Freedom on the Net 2025: The fight for trust online.
- Government of Bhutan. (2024). National cybersecurity strategy 2024–2029.
- Human Rights Watch. (2020). World report 2020: India.
- Human Rights Watch. (2025). Joint statement on emerging digital laws in Bangladesh.
- International Center for Not-for-Profit Law. (2024). Bangladesh Cyber Security Act handbook.
- International Center for Not-for-Profit Law. (2025). Civic freedom monitor: Sri Lanka.
- International Telecommunication Union. (2025). ICT development index datahub.
- LawGandhi. (2025). Nepal Social Media Bill 2081 analysis.
- LUMS SAHSOL. (2025). Analysis of Pakistan's PECA amendments.
- Ministry of Information Technology and Telecommunication, Pakistan. (2025). Prevention of Electronic Crimes Act (amendments).
- Policy Review. (2021). Digital democracy.
- The Diplomatic Insight. (2025). What Pakistan's reclassification to MENA means.
- UNDP. (2025). Digital Bangladesh AI readiness assessment report.
- UNESCO. (2025). Legal analysis of Nepal Social Media Bill 2081.
- World Bank. (2022). GovTech maturity index data dashboard.
- GSMA. (2024). Mobile connectivity index.

About Accountability Lab Pakistan

Accountability Lab Pakistan (ALP) is a think-and-do tank focused on making governance work for people by supporting active citizens, responsible leaders, and accountable institutions. Our approach reimagines how accountability can be built and sustained, envisioning a governance ecosystem where resources are used effectively, decision-making is inclusive and evidence-based, and public institutions respond to citizen needs. Distinct from traditional approaches, ALP positions accountability as a cross-cutting value embedded across governance systems. This includes work spanning public sector reform, civic engagement, human rights, service delivery, and institutional strengthening. Through knowledge production, leadership development, innovation and institutional reforms, ALP contributes to shaping more transparent, responsive, and resilient governance structures. ALP's work is anchored in strengthening the relationship between citizens and the state by advancing institutional effectiveness, public trust, and inclusive governance. By integrating research, practice, and coalition-building, the ALP supports reform processes and contributes to a more accountable and responsive governance ecosystem in Pakistan.