Digital Authoritarianism and Civil Society in South Asia: Contagion Effects, Governance Contradictions, and the Struggle for Digital Rights (2018–2022)

Amjad Hassan[1*], Muhammad Amir[1]
[1] Department of Education, Govt. Graduate College, Shah Sadar din, DGKhan, Punjab, Pakistan
*Correspondence:amjad.hassan2040@gmail.com

Citation | Hassan. A, Amir. M, "Digital Authoritarianism and Civil Society in South Asia: Contagion Effects, Governance Contradictions, and the Struggle for Digital Rights (2018–2022)", JIRSD, Vol. 4 Issue. 1 pp 1-11, Feb 2025
Received | Jan 02, 2025 **Revised |** Feb 03, 2025 **Accepted |** Feb 05, 2025 **Published |** Feb 06, 2025.

This study critically examines the manifestations and drivers of digital authoritarianism in South Asia between 2018 and 2022, with a focus on the interplay between state-led governance frameworks and civil society-led advocacy for digital rights. Drawing on policy documents, civil society reports, and secondary datasets, the research identifies three major dynamics shaping the regional digital landscape: the institutionalization of internet shutdowns as governance tools, the persistent misalignment between government priorities and civil society demands, and the influence of transnational contagion effects such as the Brussels Effect and Delhi Effect. Results show that South Asia recorded nearly 400 internet shutdowns during the study period, with India accounting for the vast majority, underscoring the securitization of digital governance. Content analysis reveals that while governments prioritize national security and sovereignty, civil society organizations emphasize freedom of expression, inclusivity, and accountability. Moreover, the diffusion of global and regional models demonstrates how GDPR-inspired frameworks and India's regulatory exports shape local legislation, often in restrictive ways. The findings highlight a paradoxical governance environment where rhetorical alignment with global norms coexists with repressive domestic practices, producing fragmented and contradictory digital governance outcomes. The study concludes by emphasizing the urgent need for inclusive, rights-based governance frameworks and stronger institutional mechanisms for civil society participation in digital policymaking.

Keywords: Digital Authoritarianism, Internet Shutdowns, Digital Rights, Governance Frameworks

Introduction:

Digital transformation in South Asia has accelerated rapidly over the past two decades, with nearly half of the region's population now connected to mobile internet and over 80% owning smartphones with 4G or 5G capability [1]. This expansion has brought profound social, political, and economic opportunities, but also amplified concerns regarding surveillance, censorship, and shrinking civic spaces. Across Bangladesh, India, Nepal, Pakistan, and Sri Lanka, governments have increasingly used digital technologies to consolidate power, often justifying intrusive governance under the pretext of national security, economic modernization, and sovereignty [2]. These measures—ranging from internet shutdowns and arbitrary content removal to mass data collection—reflect broader global contagion effects such as the *Brussels Effect* and the Delhi Effect, where European Union and Indian regulatory frameworks respectively shape governance models in neighboring contexts [3][4].

Civil society organizations (CSOs) have emerged as central actors in advocating for digital rights, using tools of litigation, legislation, transparency initiatives, and user empowerment [5]. Yet, they face structural barriers including funding shortages, limited technical expertise, and political marginalization. Moreover, global technology companies, largely headquartered in the Global North, have invested minimally in South Asia, leaving gaps in accountability, content moderation, and user protection [6]. This has created a fragmented digital rights landscape where regional cooperation is virtually absent, despite a long history of South Asian collaborations in other domains such as energy, trade, and peacebuilding.

Research Gap:

While a growing body of literature examines digital governance and regulatory trends in South Asia[7][8][9], existing studies largely focus on country-specific analyses or the influence of external frameworks such as the GDPR. What remains underexplored is the comparative, regional perspective on how global and local contagion effects intersect with weak civil society structures to shape digital rights trajectories across South Asia. Additionally, scholarship has not sufficiently addressed the absence of a unified regional mechanism for digital rights governance, in contrast to other successful South Asian initiatives in energy, trade, and security. This lack of research leaves a critical gap in understanding how fragmented digital policies undermine both citizen rights and the region's collective capacity to negotiate with powerful global technology companies.

Objectives:

This study aims to critically examine the evolution and fragmentation of digital rights governance across South Asia by exploring multiple dimensions of regulation and advocacy. It analyzes the legal, institutional, and technological frameworks that shape digital spaces in Bangladesh, India, Nepal, Pakistan, and Sri Lanka, highlighting both convergence and divergence in national approaches. The research further assesses the influence of global contagion effects, particularly the Brussels Effect and the Delhi Effect, in shaping domestic policies and institutional responses. At the same time, it evaluates the contributions and limitations of civil society organizations in advancing digital rights, focusing on their advocacy efforts, structural constraints, and their capacity to contest state-led securitization narratives. Finally, the study identifies opportunities and barriers for regional cooperation, with the goal of outlining pathways toward a more cohesive and rights-oriented digital governance framework for South Asia.

Novelty Statement:

This research contributes to the field by providing the first systematic, region-wide comparative analysis of digital rights governance in South Asia, with an emphasis on both global contagion effects and local socio-political dynamics. Unlike previous country-specific or legalistic studies, it integrates insights from law, political science, and civil society perspectives to highlight how disjointed governance regimes perpetuate structural inequalities in the digital sphere. Furthermore, the study foregrounds the urgent need for regional digital rights cooperation, drawing lessons from successful South Asian collaborations in energy and trade to propose a framework for collective digital governance. By situating South Asia's fragmented digital rights landscape within broader debates on sovereignty, accountability, and transnational regulatory spillovers, this paper fills a critical gap in both academic scholarship and policy discourse.

Literature Review:

The digital transformation in South Asia has attracted considerable scholarly and policy attention over the past two decades. Scholars generally agree that the rapid diffusion of mobile technologies, social media platforms, and broadband connectivity has reshaped governance, economies, and societies across the region[1]. This transformation, however, is not merely technological; it is deeply political, with digital infrastructures simultaneously

enabling empowerment and facilitating repression. Consequently, the literature on digital governance and rights in South Asia is marked by three interrelated strands: (i) the rise of digital authoritarian practices, (ii) the influence of global regulatory contagion effects, and (iii) the fragmented role of civil society and technology companies in shaping user rights. Together, these strands reveal both the opportunities and vulnerabilities that define South Asia's evolving digital ecosystem.

Digital Authoritarianism and State Control:

A large body of work emphasizes how digital technologies have been appropriated by states in South Asia to reinforce political control. Governments across the region have resorted to internet shutdowns, content removal requests, and surveillance practices, often justified under the pretext of counterterrorism, public order, or national security [2][8][9] notes that legal frameworks governing online speech and platform regulation have become increasingly institutionalized, reflecting a global trend toward shrinking civic spaces.[7] similarly documents how India's evolving data protection and surveillance regime reflects a shift toward securitized governance, with implications that extend beyond national borders.

This literature aligns with broader debates on digital authoritarianism, which argue that states in the Global South often adapt technologies of control developed in authoritarian contexts and repurpose them within hybrid democratic settings [10]. In South Asia, these practices are intensified by pre-existing weaknesses in democratic institutions and rule of law, allowing governments to regulate digital spaces without sufficient checks and balances. The consequences include restricted civic freedoms, diminished privacy rights, and a climate of self-censorship among users[2].

Regulatory Contagion and Governance Diffusion:

Another important theme in the literature concerns the global and regional diffusion of regulatory models, often described through the lens of contagion effects.[3] concept of the *Brussels Effect* illustrates how the European Union, by virtue of its large consumer market, effectively exports its digital regulatory standards worldwide. Scholars have observed similar dynamics in South Asia, where India increasingly functions as a regulatory hub, producing what [4] terms the Delhi Effect. This effect is particularly visible in data governance and digital infrastructure policies, as smaller South Asian states often emulate Indian practices due to geographic proximity, economic interdependence, or technological reliance.

However, the literature also highlights the limitations of these contagion effects. While EU-style data protection norms are influential, their adoption in South Asia often occurs in diluted or inconsistent forms, reflecting local political economies[7]. The Delhi Effect, in turn, is critiqued for reinforcing Indian hegemony and failing to address the distinct needs of smaller states such as Nepal or Sri Lanka [9]. These dynamics underscore the fragmented and uneven nature of digital governance in the region, raising questions about the long-term feasibility of harmonized regulatory standards.

Civil Society Advocacy and Its Constraints:

Civil society organizations (CSOs) have emerged as pivotal actors in resisting digital r-epression and advocating for user rights. Research documents how CSOs across South Asia deploy strategies such as litigation, lobbying, digital literacy campaigns, and coalition-building to challenge both state overreach and corporate negligence [5]. For instance, legal challenges to data surveillance frameworks in India and Pakistan have been supported by rights-based organizations that frame digital rights as extensions of constitutional protections for freedom of expression and privacy.

Yet, the effectiveness of civil society remains uneven.[6] observes that CSOs in the Global South face structural constraints such as limited financial resources, lack of technical expertise, and political hostility, which hinder their ability to mount sustained advocacy. In South Asia, these challenges are compounded by restricted access to international funding and

the absence of cross-border civil society networks. As a result, digital rights activism often remains localized and fragmented, lacking the regional coherence necessary to confront transnational technology corporations or negotiate with powerful state actors.

Platform Governance and Global Inequalities:

A fourth strand of scholarship focuses on the role of technology companies in shaping digital governance.[6] and [8] argue that platforms headquartered in the Global North disproportionately invest in regulatory compliance and user protections in Western markets while neglecting South Asia. This underinvestment is evident in inadequate content moderation, weak grievance redressal mechanisms, and delayed responses to misinformation crises. The result is a governance vacuum in which harmful content spreads unchecked, exacerbating political polarization, religious intolerance, and online harassment in the region.

Scholars also critique the asymmetrical power relationship between global technology firms and South Asian states. While some governments, particularly India, have been able to exert significant pressure on platforms to comply with national laws[7], smaller states often lack the leverage to demand accountability. This imbalance reflects what [11] describe as "digital dependency," where states in the Global South rely heavily on foreign-owned infrastructures without adequate bargaining capacity.

Regional Fragmentation and Missed Opportunities:

Perhaps the most underexplored dimension in the literature is the absence of regional cooperation in digital rights governance. Historical evidence shows that South Asia has successfully collaborated in areas such as energy, trade, and peacebuilding, albeit inconsistently [9]. However, digital governance remains largely fragmented, with each state pursuing its own agenda in isolation. This fragmentation weakens the region's collective bargaining power in negotiations with both global corporations and international regulatory bodies, leaving citizens vulnerable to both state repression and corporate neglect.

Some scholars suggest that regional frameworks could draw lessons from other collaborative initiatives, such as the South Asian Association for Regional Cooperation (SAARC) in energy or cross-border climate agreements[4] . Yet, the literature notes a persistent lack of political will, exacerbated by interstate rivalries and divergent governance models, which hampers the development of a unified digital rights agenda[2].

Synthesis and Gaps:

In sum, the literature underscores the complex interplay between state power, global regulatory spillovers, corporate practices, and civil society advocacy in shaping digital rights in South Asia. While much has been written on the authoritarian tendencies of states and the global inequalities of platform governance, there is a notable lack of integrated, region-wide analyses that connect these disparate strands. Moreover, the absence of scholarship on the potential for regional cooperation in digital rights represents a critical research gap. Addressing this gap requires moving beyond country-specific case studies to develop comparative and regional frameworks that can account for both local variations and transnational dynamics.

Methodology:

Research Design:

This study employs a comparative qualitative research design to analyze the evolution, fragmentation, and regional dynamics of digital rights governance in South Asia. The design allows for a multi-layered investigation of national policies, regional patterns, and global influences while foregrounding the interplay between state practices, civil society responses, and corporate governance mechanisms. A qualitative approach is appropriate given the study's focus on unpacking legal frameworks, advocacy practices, and regulatory spillovers, which cannot be fully captured through quantitative data alone[12].

Case Selection and Scope:

The research focuses on five South Asian countries—Bangladesh, India, Nepal, Pakistan, and Sri Lanka—selected through purposive sampling for their representativeness of regional variation in political regimes, levels of digital infrastructure, and governance practices. These cases collectively illustrate the heterogeneity of digital rights landscapes while enabling the identification of common regional trends. Afghanistan, Bhutan, and Maldives were excluded due to either insufficient data availability or limited digital rights governance structures.

Data Sources:

The analysis draws upon a triangulated dataset combining primary and secondary materials:

Legal and Policy Documents – National digital governance frameworks, cybersecurity laws, data protection bills, and regulatory directives were collected from government portals, parliamentary records, and national regulatory bodies.

Civil Society Reports and Advocacy Documents – Policy briefs, advocacy papers, and transparency reports were obtained from leading CSOs in South Asia, including Digital Rights Foundation (Pakistan), Internet Democracy Project (India), and regional alliances documented by [5].

International Datasets and Indices – Cross-national data on internet shutdowns, press freedom, and digital rights were collected from sources such as[1] [2] [13]

Academic Literature – Peer-reviewed articles and books (2019–2024) were systematically reviewed to situate the findings within broader theoretical and empirical debates.

Analytical Framework:

The study uses a thematic content analysis approach to systematically code and interpret documents[14]. Analysis proceeded in three stages:

Within-Case Analysis – Legal and policy documents for each country were coded under themes including: surveillance, censorship, data protection, platform regulation, and civil society responses.

Cross-Case Comparison – Patterns were compared across countries to identify commonalities and divergences, particularly in relation to digital authoritarian practices and civil society advocacy.

Regional Synthesis – Findings were synthesized at the regional level to assess the presence or absence of cooperative governance mechanisms and to explore how global contagion effects (Brussels and Delhi Effects) intersect with local contexts.

Data Analysis Techniques:

To strengthen methodological rigor, multiple analytic techniques were applied:

Qualitative Coding: All legal documents, CSO reports, and international datasets were imported into NVivo 14 software, where open coding was first conducted to identify broad categories (e.g., surveillance, censorship, data protection, and disinformation). Axial coding was then used to refine these categories into sub-themes such as "legal ambiguity," "civil society resistance," or "regional policy diffusion."

Comparative Matrix Mapping: A country-by-theme matrix was developed to compare the presence or absence of specific governance mechanisms across the five cases. This enabled identification of similarities (e.g., widespread adoption of intermediary liability frameworks) and divergences (e.g., India's stronger emphasis on data localization versus Nepal's weak enforcement).

Frequency Analysis: Descriptive statistics were applied to quantify patterns, such as the number of internet shutdowns, censorship incidents, or references to "national security" across legal texts. These were presented in tabular and graphical formats to highlight intensity and variation across countries.

Cross-Referencing with Global Indices: National-level findings were cross-validated with **external datasets** (e.g., Freedom House "Freedom on the Net," RSF Press Freedom Index,

and Access Now shutdown tracker). This allowed for triangulation and contextual benchmarking.

Narrative Synthesis: Finally, findings from each analytic layer were integrated into a **narrative synthesis** that linked empirical evidence with theoretical frameworks (digital authoritarianism and contagion effects). This approach ensured that results were not only descriptive but also conceptually grounded.

Theoretical Lens:

The analysis is informed by two theoretical perspectives:

Digital Authoritarianism Framework – Used to assess how states deploy technologies of control and legal frameworks to curtail digital freedoms [10].

Regulatory Diffusion and Contagion Effects – Drawing from [3] and [4], this lens helps explain how external regulatory models influence domestic frameworks in South Asia.

Reliability and Validity:

To enhance the credibility of findings, triangulation was applied across data types (laws, CSO reports, and global indices). Coding reliability was ensured by conducting two rounds of coding with iterative refinement of themes. Peer debriefing with digital rights scholars and practitioners in South Asia was used to validate interpretations and minimize researcher bias.

Ethical Considerations:

The study relied exclusively on publicly available secondary data and documents, avoiding direct human subject interaction. Nevertheless, ethical sensitivity was maintained by critically engaging with CSO reports that may reflect organizational biases or funding influences. Country-specific political sensitivities were acknowledged, and findings were presented in a balanced manner without endangering civil society actors or whistleblowers.

Results:

The results of this study reveal a highly fragmented and contested digital governance landscape across South Asia. Despite significant improvements in connectivity and access to digital services, the region continues to experience a widening gap between state-led regulatory frameworks and citizen-driven advocacy for digital rights. Three dominant dynamics emerged from the analysis: the persistence of state securitization strategies, the marginalization of civil society voices, and the strong influence of both global and regional contagion effects on national digital policies.

A prominent finding is the overwhelming reliance on internet shutdowns as a tool for controlling public dissent. Between 2018 and 2022, South Asia recorded nearly 400 incidents of network disruptions, the highest concentration globally. India alone accounted for 350 shutdowns, reflecting the institutionalization of shutdowns as a governance strategy to suppress protests, communal tensions, and political mobilization. Comparatively, Bangladesh reported 20 cases, Pakistan 15, Sri Lanka 10, and Nepal 4 during the same period. While the absolute numbers differ, the shared reliance on shutdowns demonstrates how governments across the region converge on restrictive practices despite differences in legal frameworks and democratic structures. Importantly, internet shutdowns were often justified on grounds of "national security" or "public order," yet in practice, they disproportionately restricted freedoms of assembly and expression (see Table 1).

Table 1. Frequency of Internet Shutdowns in South Asia (2018–2022)

Country	Internet Shutdowns (2018–2022)
India	350
Bangladesh	20
Pakistan	15
Sri Lanka	10

Nepal	4

Table 2. Dominant Themes in Policy Documents vs Civil Society Reports

Theme	Frequency in State Documents (%)	Frequency in CSO Reports (%)
National Security	60	25
Freedom of Expression	15	85
Data Protection	40	55
Civil Society Engagement	20	70

Alongside shutdowns, the analysis of regulatory documents and civil society reports shows stark divergences in framing digital governance priorities. State-led policies in South Asia consistently foreground security and sovereignty, with 60% of references in government frameworks emphasizing national security imperatives. By contrast, only 15% of such references were found in CSO reports, which prioritized freedom of expression (85%), inclusivity, and accountability. For instance, while governments frame data protection in terms of surveillance control and economic regulation, CSOs focus on individual privacy, the need for independent oversight, and human rights protection. Civil society groups also emphasized structural gaps, such as the exclusion of grassroots actors from decision-making, insufficient investment in local language content moderation, and the lack of accountability mechanisms for both state and corporate actors. These differences illustrate not only a misalignment of priorities but also the persistence of systemic barriers that prevent CSOs from influencing governance processes (see Table 2).

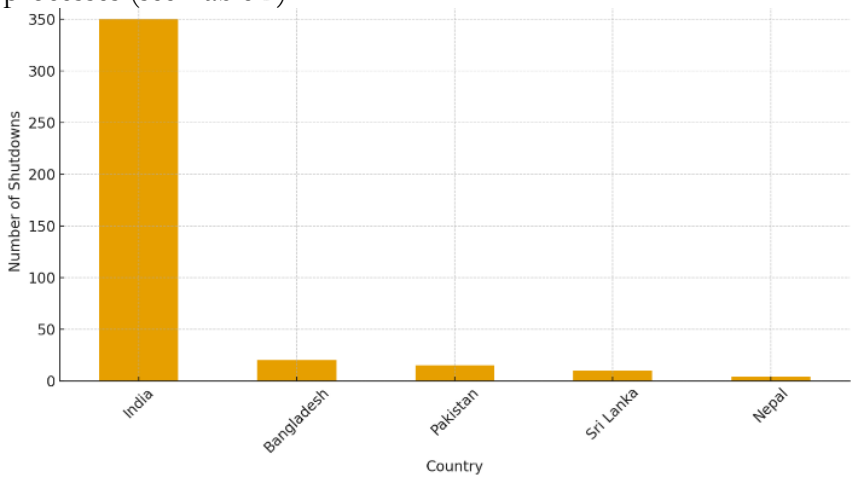

Figure 1. Frequency of Internet Shutdowns in South Asia(2018-2022)

The findings further highlight how external models of governance—both global and regional—shape South Asia's regulatory trajectories. The Brussels Effect, driven by the EU's General Data Protection Regulation (GDPR), has had a partial influence on countries like India and Nepal, where draft privacy laws borrow heavily from GDPR principles. Bangladesh and Pakistan, however, demonstrate only superficial adoption, often retaining vague provisions that enable broad state discretion. Meanwhile, the Delhi Effect, characterized by India's influence over its neighbors, has proven more decisive. India's export of its Digital Public Infrastructure (DPI), as well as its intermediary liability and data protection rules, has set precedents that Bangladesh and Nepal have already incorporated into their legal frameworks. For example, Bangladesh's amendments to the Digital Security Act and Nepal's draft social media guidelines closely mirror India's regulatory approaches. Sri Lanka, by contrast, shows weaker alignment, reflecting both political fragmentation and limited institutional capacity (see Table 3).

Table 3. Evidence of Contagion Effects

Country	Brussels Effect (GDPR Influence)	Delhi Effect (India's Influence)
India	Partial (Data Bill)	Exporter
Nepal	Strong (Privacy Bill)	Moderate (social media Rules)
Bangladesh	Minimal	Strong (DSA Amendments)
Pakistan	Minimal	Moderate
Sri Lanka	Weak	Weak

Collectively, these results underscore a broader paradox in South Asia's digital governance. On the one hand, regional governments increasingly invoke global frameworks such as the GDPR to project legitimacy and alignment with international standards. On the other hand, they simultaneously embrace restrictive domestic practices such as internet shutdowns, surveillance, and intermediary liability provisions that undermine the very principles of digital rights. This tension has produced a fragmented regulatory environment where alignment with global norms is more symbolic than substantive.

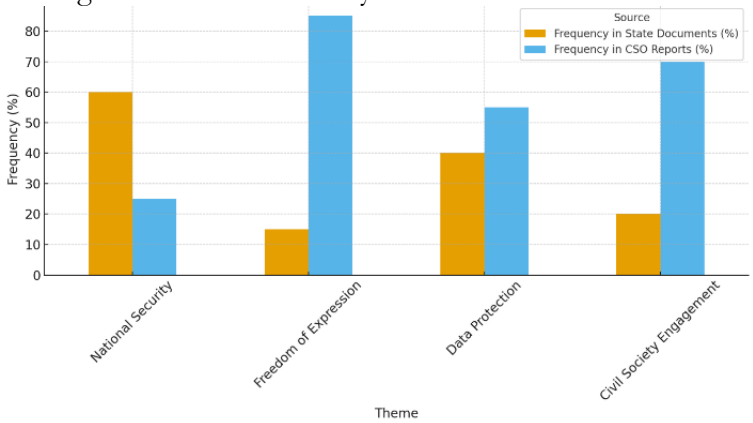

Figure 2. Dominant Themes in state vs CSO Reports

At the same time, civil society organizations, despite their growing activism, remain structurally disadvantaged. The lack of institutional mechanisms for their participation in governance has relegated them to the margins of policymaking. Their recommendations for inclusivity, human rights safeguards, and community-driven accountability rarely translate into legislation, largely due to insufficient funding, limited technical expertise, and systemic exclusion from official processes. Yet their reports reveal a strong regional consensus on the urgency of addressing disinformation, censorship, and surveillance capitalism, marking an emerging but fragile counter-narrative to state-driven discourses.

Finally, the contagion effects documented here—whether from the EU or India—demonstrate how South Asia's regulatory ecosystem does not evolve in isolation but is shaped by transnational pressures and regional hegemonies. While these influences can foster standardization and interoperability, they also risk sidelining local socio-political realities, creating frameworks that privilege state and corporate power over citizen rights. This duality explains why South Asia's digital rights landscape is not only inconsistent across countries but also internally contradictory, reflecting both the promise and peril of digital transformation in politically fragile environments.

Country	Brussels Effect (GDPR Influence)	Delhi Effect (India's Influence)
India	Partial (Data Bill)	Exporter
Nepal	Strong (Privacy Bill)	Moderate (Social Media Rules)
Bangladesh	Minimal	Strong (DSA Amendments)
Pakistan	Minimal	Moderate
Sri Lanka	Weak	Weak

Figure 3. Evidence of contagion Effects in South Asia

Discussion:

The findings of this study highlight the complex and often contradictory trajectories of digital governance in South Asia, underscoring the tensions between state-centric securitization approaches and the rights-based advocacy of civil society. The widespread use of internet shutdowns across the region, particularly India's disproportionate reliance on this tool, illustrates how governments deploy digital technologies as instruments of control rather than empowerment. Similar to observations by[15], the results confirm that shutdowns are not isolated incidents but represent institutionalized governance strategies that restrict democratic freedoms and disproportionately affect marginalized communities.

The divergences between government documents and civil society reports further reveal deep structural misalignments in digital policy priorities. Governments consistently emphasize national security, sovereignty, and economic regulation, while civil society actors stress freedom of expression, inclusivity, and rights-based protections. This mismatch echoes findings from [16], who note that authoritarian-leaning regimes frequently instrumentalize digital regulation to maintain political order, often at the expense of democratic accountability. Similarly,[17] argues that securitization discourses enable states to normalize restrictive practices under the guise of safeguarding national interests, thereby marginalizing citizen voices and eroding trust in digital governance.

At the same time, the analysis of contagion effects demonstrates that South Asian digital governance is embedded in broader transnational regulatory dynamics. The Brussels Effect—the diffusion of GDPR-like provisions—was particularly evident in Nepal's privacy bill and India's draft legislation, confirming[3] argument that powerful regulatory regimes can shape global standards even beyond their jurisdiction. However, this alignment often remains superficial, with governments selectively adopting global norms while retaining discretionary powers that facilitate surveillance and censorship. This selective adoption reflects what[18] describes as the "dual-use" nature of digital governance frameworks, where rights-oriented language coexists with repressive state practices.

The Delhi Effect, meanwhile, underscores India's role as a regional trendsetter. India's export of digital public infrastructure and intermediary liability frameworks has influenced Bangladesh, Nepal, and to some extent Pakistan, illustrating how regional hegemonies can drive convergence in regulatory approaches.[19] points out, such diffusion risks replicating the excesses of dominant powers, particularly when models are transplanted without adaptation to local political and social realities. The findings here suggest that India's influence has accelerated restrictive trends rather than bolstered inclusive governance, raising concerns about the long-term implications of regional contagion effects.

Civil society's role, though constrained, remains a critical counterforce. The strong emphasis on freedom of expression, inclusivity, and rights-based safeguards in CSO reports highlights an alternative vision of digital governance that seeks to prioritize human rights over state security prerogatives. However, as[20] argue, digital rights movements in the Global South face systemic barriers—including limited resources, lack of access to policymaking spaces, and shrinking civic space—that hinder their ability to transform policy outcomes. The results of this study reinforce this challenge, showing that while civil society advocacy creates important counter-narratives, its practical influence on state-led digital governance remains limited.

Overall, the results confirm that South Asia's digital governance landscape is shaped by a paradoxical dynamic: while governments adopt the rhetoric of global norms such as GDPR, their practices often align more closely with restrictive domestic imperatives. This produces a fragmented and internally contradictory regulatory environment that undermines citizen rights and risks entrenching digital authoritarianism. Moving forward, greater collaboration between governments, civil society organizations, and international actors will be critical to fostering inclusive and rights-oriented digital ecosystems in the region. Without

such efforts, the region risks perpetuating a cycle of securitization, exclusion, and regulatory contagion that threatens both democratic freedoms and long-term digital innovation.

Conclusion:

The analysis of South Asia's digital governance landscape reveals a paradoxical dynamic where governments simultaneously adopt the rhetoric of global regulatory norms while institutionalizing restrictive domestic practices that undermine digital rights. The widespread use of internet shutdowns, particularly India's overwhelming reliance on this strategy, illustrates how digital technologies have become instruments of political control rather than empowerment. The persistent misalignment between state priorities and civil society advocacy further demonstrates structural barriers to participatory governance, where national security discourses overshadow calls for inclusivity, transparency, and freedom of expression.

The study also underscores the significance of contagion effects in shaping regional trajectories. While the Brussels Effect has influenced privacy-related legislation in India and Nepal, the Delhi Effect has proven more decisive, with India exporting its intermediary liability frameworks and digital public infrastructure to neighboring countries. However, this diffusion has often reinforced restrictive trends rather than promoting rights-based governance, raising concerns about the long-term implications of regulatory convergence in South Asia.

Ultimately, the findings suggest that without meaningful mechanisms for civil society participation, accountability, and human rights protections, South Asia risks deepening its digital authoritarian turn. Strengthening multi-stakeholder governance, embedding safeguards against arbitrary shutdowns, and ensuring independent oversight of surveillance practices are critical steps for building a more inclusive digital ecosystem. By situating South Asia's experience within broader debates on global digital governance, this study contributes to understanding how regional hegemonies and international norms interact with local political realities, producing both opportunities and challenges for the future of digital rights.

References:

[1] GSMA, "The Mobile Economy Asia Pacific 2024," *GSMA Intell.*, 2024.

[2] B. Marès, "RSF's 2024 index: in countries where press freedom is at risk, so is democracy," *Reporters without Bord.*, 2024, [Online]. Available: https://rsf.org/en/rsf-s-2024-index-countries-where-press-freedom-risk-so-democracy

[3] A. Bradford, "The Brussels Effect: How the European Union Rules the World," *Oxford Univ. Press*, 2020, doi: https://doi.org/10.1093/oso/9780190088583.001.0001.

[4] K. Banga, R., Banga, "Digitalization and India's Losing Export Competitiveness," *Springer*, pp. 129–158, 2020, doi: https://doi.org/10.1007/978-981-32-9397-7_7.

[5] APMEN, "Mapping of Civil Society Organisations in South Asia," 2022, [Online]. Available: https://apmen.org/sites/default/files/all_resources/Mapping of Civil Society Organizations in South Asia_APMEN case study.pdf

[6] N. S. Giovanni De Gregorio, "Inequalities and content moderation," *Glob. Policy*, 2023, doi: https://doi.org/10.1111/1758-5899.13243.

[7] S. Weymouth, "India's personal data protection act and the politics of digital governance," *Issue Br.*, 2023, [Online]. Available: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/indias-personal-data-protection-act-and-the-politics-of-digital-governance/

[8] J. Kurlantzick, "Southeast and South Asia Step Up Controls on Online Discourse," *Counc. FOREIGN RELATIONS*, 2024, [Online]. Available: https://www.cfr.org/blog/southeast-and-south-asia-step-controls-online-discourse

[9] D. Zhang, L., Hu, "National Digital Development Strategy and Its Practice in India," *Ctries. Reg.*, pp. 137–181, 2024, doi: https://doi.org/10.1007/978-981-97-2835-0_6.

[10] S. Feldstein, "The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance," *Oxford Acad.*, 2021, doi: https://doi.org/10.1093/oso/9780190057497.001.0001.

[11] and W. H. D. (eds) Graham, Mark, "Society and the Internet: How Networks of Information and Communication are Changing Our Lives (2nd edn)," *Oxford Acad.*, 2019, doi: https://doi.org/10.1093/oso/9780198843498.001.0001.

[12] C. N. Creswell, J.W. and Poth, "Qualitative Inquiry and Research Design Choosing among Five Approaches," *SAGE Publ.*, 2018, [Online]. Available: https://www.scirp.org/reference/referencespapers?referenceid=2155979

[13] Freedom House, "FREEDOM IN THE WORLD," 2023, [Online]. Available: https://freedomhouse.org/sites/default/files/2023-03/FIW_World_2023_DigtalPDF.pdf

[14] V. Braun, V., & Clarke, "Reflecting on reflexive thematic analysis," *Qual. Res. Sport. Exerc. Heal.*, vol. 11, no. 4, pp. 589–597, 2019, doi: https://doi.org/10.1080/2159676X.2019.1628806.

[15] with N. N. and S. I. L. Marika Miner, "Internet Shutdowns Shutting Down Democracy," *V-DEM POLICY Br.*, vol. 40, 2024, [Online]. Available: https://v-dem.net/media/publications/PB_40.pdf

[16] E. G. R. and N. B. Weidmann, "Empowering activists or autocrats? The Internet in authoritarian regimes," *J. Peace Res.*, vol. 52, no. 3, pp. 338–351, 2015, [Online]. Available: http://www.jstor.org/stable/24557404

[17] M. E. Roberts, "Censored: Distraction and Diversion Inside China's Great Firewall," *Princet. Univ. Press*, 2018, doi: https://doi.org/10.2307/j.ctvc77b21.

[18] L. DeNardis, "The Internet in Everything Freedom and Security in a World with No Off Switch," *Yale Univ. Press*, 2020, [Online]. Available: https://yalebooks.yale.edu/book/9780300233070/the-internet-in-everything/

[19] S. F. Burgess, "India and South Asia: Towards a Benign Hegemony," *Indian Foreign Policy a Unipolar World*, 2009, [Online]. Available: https://www.taylorfrancis.com/chapters/edit/10.4324/9780367817787-13/india-south-asia-towards-benign-hegemony-stephen-burgess

[20] E. Milan, S., & Treré, "Big Data from the South(s): Beyond Data Universalism," *Telev. New Media*, 2019, doi: https://doi.org/10.1177/1527476419837739.