GOVERNING THE UNGOVERNED: A COMPARATIVE ANALYSIS OF DATA PROTECTION REGIMES IN SOUTH ASIA THROUGH THE LENS OF DIGITAL SOVEREIGNTY, CONSENT ARCHITECTURE, AND CONSTITUTIONAL GUARANTEES

Akhil Sajeev & Anusree J, Assistant Professors, School of Law, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India

ABSTRACT

The rapid digitisation of South Asian economies has precipitated an urgent need for coherent, rights-respecting data governance frameworks. Despite sharing constitutional traditions rooted in the common law and constitutional democracy, the nations of South Asia — India, Bangladesh, Sri Lanka, Pakistan, Nepal, and Bhutan — have pursued divergent legislative and regulatory approaches to personal data protection. This paper undertakes a comparative doctrinal and policy analysis of existing and emerging data protection regimes across the sub-continent, with particular emphasis on India's Digital Personal Data Protection Act, 2023, Bangladesh's Personal Data Protection Bill, 2022, and Sri Lanka's Personal Data Protection Act, 2022. The analysis examines the structural architecture of consent, purpose limitation, and data fiduciary obligations; the constitutional underpinnings of informational self-determination; the regulatory treatment of sensitive personal data including biometrics and children's data; and the governance challenges posed by cross-border data flows and data localisation mandates. The paper contextualises these legislative developments within the broader framework of global data governance norms, including the General Data Protection Regulation (GDPR), United Nations resolutions on the right to privacy in the digital age, and the emerging convergence between data protection and trade law under the World Trade Organization's Joint Statement Initiative on E-Commerce. Drawing upon a sovereignty-based analytical framework, the paper argues that South Asian states are navigating a contested trilemma between individual privacy rights, state surveillance imperatives, and market integration pressures. It concludes with recommendations for regional regulatory convergence, informed by the Sustainable Development Goals, particularly SDG 16 and SDG 17, to build accountable, transparent, and interoperable data governance institutions across South Asia.

Keywords: Data Protection, Digital Sovereignty, South Asia, Consent Architecture, Data Fiduciary

I. INTRODUCTION

The governance of personal data has emerged as one of the defining legal and policy challenges of the twenty-first century. Across South Asia, the proliferation of digital infrastructure — from mobile payment systems and e-government platforms to social media ecosystems and biometric identity databases — has generated colossal volumes of personal data, the legal status and regulatory treatment of which remain deeply contested. Unlike the European Union, which has established a comprehensive and horizontally applicable data protection framework through the General Data Protection Regulation,[1] South Asian jurisdictions have adopted fragmented, sector-specific, or still-nascent approaches to data governance that reflect competing national priorities, institutional capacities, and constitutional traditions.

India, the region's largest democracy and digital economy, enacted the Digital Personal Data Protection Act, 2023[2] after more than six years of legislative deliberation triggered by the landmark Supreme Court judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India,*[3] which affirmed informational privacy as a fundamental constitutional right. Bangladesh has circulated a Personal Data Protection Bill, 2022,[4] and Sri Lanka enacted its Personal Data Protection Act, 2022,[5] making it among the first in the sub-region to establish a dedicated data protection authority. Pakistan and Nepal are at various stages of legislative deliberation, while Bhutan's digital regulatory environment remains in its formative stages.

This paper argues that while South Asian data protection regimes are converging towards certain structural similarities — consent-based processing, purpose limitation, and designated regulatory oversight — they remain divergent in their constitutional grounding, enforcement architecture, and treatment of state access to data. This divergence is not incidental but reflects deeper tensions between liberal rights discourse, developmental state governance, and the

[1]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, OJ L 119, 4.5.2016, pp. 1–88.
[2]Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[3]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India). The nine-judge bench of the Supreme Court of India unanimously held that the right to privacy is a fundamental right under Article 21 of the Constitution of India.
[4]Personal Data Protection Bill, 2022 (Bangladesh), published by the Ministry of Posts, Telecommunications and Information Technology, Government of the People's Republic of Bangladesh.
[5]Personal Data Protection Act, No. 9 of 2022 (Sri Lanka). See also: Information and Communication Technology Agency of Sri Lanka, *Data Protection Framework* (2022).

imperatives of national security. A comparative analysis of these regimes is therefore not merely of academic interest but of pressing policy relevance, particularly as South Asian states seek to negotiate digital trade agreements, manage cross-border data flows, and protect their citizens from the harms of data exploitation.

This paper proceeds as follows. Part II examines the constitutional foundations of data protection in South Asia. Part III undertakes a comparative analysis of the legislative frameworks across key jurisdictions. Part IV analyses the regulatory treatment of sensitive data, including biometric and children's data. Part V addresses the intersection of data governance with digital sovereignty, cross-border flows, and trade law. Part VI situates the discussion within the Sustainable Development Goals framework. Part VII concludes with recommendations for regional regulatory convergence.

II. CONSTITUTIONAL FOUNDATIONS OF DATA PROTECTION IN SOUTH ASIA

The constitutional basis for data protection in South Asia derives primarily from the right to life and personal liberty, which has been interpreted broadly by apex courts across the region to encompass informational self-determination and dignitaries' privacy interests. In India, the constitutional moment arrived in 2017 when a nine-judge bench of the Supreme Court in Puttaswamy unanimously held that the right to privacy is a fundamental right protected under Article 21 of the Constitution of India, overruling earlier decisions that had denied this status.

The Puttaswamy judgment is transformative not merely because it recognises privacy as a fundamental right, but because it articulates a tripartite test for the proportionality of privacy limitations: legality, necessity, and proportionate aim. This constitutional standard has become the normative baseline against which subsequent data protection legislation in India must be measured, and it provides a rich doctrinal vocabulary for evaluating the adequacy of legislative choices. The Digital Personal Data Protection Act, 2023, however, has been criticised by constitutional scholars for failing to fully operationalise the Puttaswamy standard, particularly in its broad grants of exemptions to the state for purposes of national security and public order.

Bangladesh's Constitution, in Article 43, guarantees the right to privacy of correspondence and communication, though the courts have not yet had occasion to develop this provision into a comprehensive doctrine of informational privacy analogous to India's Post-Puttaswamy jurisprudence. Sri Lanka's constitutional framework, operating under the 1978 Constitution as

amended, recognises freedom from arbitrary arrest and the protection of private life under Article 14A, inserted by the Twenty-First Amendment of 2022. These constitutional provisions, while varying in their textual specificity and judicial interpretation, collectively signal a regional trend towards constitutional recognition of data privacy as an aspect of fundamental rights.

Critically, however, constitutional recognition alone does not translate into effective data protection unless it is buttressed by legislative precision, institutional independence of the regulatory authority, and accessible enforcement mechanisms. The gap between constitutional aspiration and legislative reality is a recurring theme in South Asian data governance, and it forms the central critical lens of this paper.

III. COMPARATIVE ANALYSIS OF LEGISLATIVE FRAMEWORKS

A. India: Digital Personal Data Protection Act, 2023

India's Digital Personal Data Protection Act, 2023 (DPDPA) represents the culmination of a legislative journey that began with the Justice Srikrishna Committee's report in 2018 and passed through multiple draft iterations. The DPDPA adopts a "Data Fiduciary" and "Data Principal" architecture, placing obligations on entities that process personal data and conferring rights upon individuals whose data is processed.[6] Consent is positioned as the primary ground for lawful processing, supplemented by "legitimate uses" which permit processing for state subsidies, employment purposes, and public interest functions without explicit consent.

Structurally, the DPDPA departs from the GDPR in several significant respects. First, it does not establish a statutory right to data portability. Second, it grants the Central Government broad powers to exempt agencies from the Act's provisions on grounds of national security, sovereignty, and public order, without requiring individualised justification. Third, it does not include provisions for algorithmic accountability or automated decision-making, which are increasingly recognised globally as essential safeguards in the age of artificial intelligence. Fourth, the Data Protection Board constituted under the Act is vested with adjudicatory powers but lacks the structural independence of a classical regulatory authority, raising concerns about

[6]Digital Personal Data Protection Act, 2023, s. 4 (India). The Act designates entities processing personal data as "Data Fiduciaries" and imposes obligations including notice, purpose limitation, data minimisation, and accuracy.

its effectiveness in checking state or corporate overreach.

The Act's provisions on children's data protection represent a notable advance, prohibiting the tracking, behavioural monitoring, or targeted advertising directed at children, and requiring verifiable parental consent for the processing of children's data.[7] However, the mechanism for age verification remains technically underspecified, and the delegation of implementation details to subordinate rules and regulations introduces uncertainty into the compliance framework.

B. Sri Lanka: Personal Data Protection Act, 2022

Sri Lanka's Personal Data Protection Act, No. 9 of 2022 (PDPA) is more structurally comprehensive than India's DPDPA in certain respects. It establishes an independent Data Protection Authority, defines sensitive personal data to include biometric data, genetic data, health data, racial and ethnic origin, political opinions, and religious beliefs, and requires data protection impact assessments for high-risk processing activities. The PDPA also includes provisions for data portability and the right to be forgotten, aligning it more closely with the GDPR's rights architecture.

Sri Lanka's legislative choice reflects, in part, its aspirations for adequacy recognition from the European Union, which would facilitate data flows between Sri Lankan businesses and EU partners. This external normative pressure has served as a significant driver of legislative design, illustrating how the architecture of data protection laws in the Global South is often shaped as much by the demands of international trade and investment as by domestic rights considerations. The challenge for Sri Lanka lies in the effective operationalisation of these rights — the Data Protection Authority is newly established, resource-constrained, and yet to develop a robust body of regulatory practice and enforcement precedent.

C. Bangladesh: Personal Data Protection Bill, 2022

Bangladesh's draft Personal Data Protection Bill, 2022[8] adopts a consent-based framework but includes provisions that have attracted criticism from civil society and international observers

[7]Digital Personal Data Protection Act, 2023, s. 9 (India). Section 9 specifically addresses the processing of personal data of children and prohibits tracking, behavioural monitoring, and targeted advertising directed at children.

for tilting the balance towards state authority. The draft empowers government agencies to exempt themselves from the Bill's provisions broadly, and the oversight mechanism proposed — a regulatory body under ministerial superintendence — does not meet international standards of regulatory independence. The Bill also contains provisions that potentially criminalise the exercise of data subject rights in certain circumstances, which critics argue could chill legitimate advocacy and journalistic activities.

Despite these criticisms, the draft Bill marks an important legislative milestone for Bangladesh, signalling a recognition that the existing patchwork of sectoral regulations — applicable to telecommunications, banking, and e-commerce separately — is inadequate for the data-intensive economy that Bangladesh is rapidly becoming. The Bill draws partially from comparative models including the GDPR and India's earlier legislative drafts, though its contextualisation of these models to Bangladesh's constitutional and administrative traditions remains incomplete.

IV. BIOMETRIC DATABASES, CHILDREN'S DATA, AND SOCIAL PROTECTION SYSTEMS

The intersection of biometric data, social protection systems, and data governance represents perhaps the most practically consequential dimension of the South Asian data protection debate. India's Aadhaar system, established under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016,[9] has enrolled over 1.3 billion residents in a biometric database that serves as the foundational digital identity infrastructure for a vast array of welfare delivery, financial services, and government authentication purposes. The scale of this undertaking is unprecedented globally and has been the subject of sustained legal challenge and academic scrutiny.

In its 2018 constitutional bench judgment on Aadhaar,[10] the Supreme Court of India upheld the constitutional validity of the Aadhaar Act but struck down the provision permitting private entities to mandate Aadhaar authentication, thereby ring-fencing the system's use primarily to

[9]Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, No. 18, Acts of Parliament, 2016 (India). As of 2023, over 1.3 billion residents have been enrolled in the Aadhaar biometric database.

[10]Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar-5J), (2018) 1 SCC 809 (India). The five-judge constitutional bench upheld the Aadhaar Act with certain riders, striking down Section 57 which permitted private entities to use Aadhaar for authentication.

the delivery of state benefits. The judgment, however, did not definitively resolve questions about data security vulnerabilities, the proportionality of biometric collection at scale, and the exclusionary consequences for individuals who are unable to complete biometric authentication due to age, disability, or technical failure.

The use of biometric data in social protection systems — encompassing not only Aadhaar in India but analogous initiatives in Bangladesh's National Identity Registration Authority database and Pakistan's National Database and Registration Authority — raises profound questions about data minimisation and purpose limitation. Where biometric systems are deployed for welfare delivery, the concatenation of multiple databases — health, tax, social protection, migration — creates what scholars have termed a "surveillance infrastructure of welfare," which subjects the most economically vulnerable populations to the most intensive data collection regimes. This inversely proportional relationship between economic vulnerability and data exposure represents a structural failure in the design of consent-based data protection frameworks that assume a free and equal data subject capable of negotiating the terms of data sharing.

Children's data presents a related but distinct set of concerns. The digitisation of education in South Asia during and after the COVID-19 pandemic dramatically expanded the collection of children's personal and biometric data by edtech platforms, government learning management systems, and examination authorities. The absence of dedicated children's data protection provisions in most South Asian legislative frameworks — with the partial exception of India's DPDPA — leaves this population significantly exposed. The collection of children's biometric data for school attendance systems, examination fraud prevention, and nutrition programme monitoring raises particular concerns given the sensitivity of biometric data, the limited capacity of children to exercise meaningful consent, and the long-term consequences of data breaches involving minors.

V. DIGITAL SOVEREIGNTY, CROSS-BORDER DATA FLOWS, AND TRADE LAW

The concept of digital sovereignty — understood as the aspiration of states to exercise meaningful regulatory control over data generated within their territorial jurisdictions — has become an organising principle of data governance policy across South Asia. Data localisation requirements, which mandate the storage of certain categories of personal data within national borders, are the most visible legislative expression of this aspiration. India's DPDPA grants the

Central Government broad powers to restrict the transfer of personal data to specified foreign jurisdictions, effectively enabling selective data localisation without prescribing it universally. Sri Lanka's PDPA similarly restricts transfers to jurisdictions without adequate data protection laws, subject to regulatory exceptions. Bangladesh's draft Bill proposes localisation requirements for sensitive data.

These localisation mandates sit in tension with the liberalisation commitments that South Asian states have undertaken or are negotiating in the context of digital trade. The WTO's Joint Statement Initiative on E-Commerce, which is working towards binding disciplines on cross-border data flows and data localisation prohibitions,[11] has not attracted support from India, which has consistently argued that the JSI's proposed data flow disciplines would unduly constrain regulatory sovereignty and constitute a new form of digital colonialism. This position reflects a broader Global South critique of the global data governance architecture, which South Asian states argue was designed primarily to serve the interests of large technology platforms domiciled in the United States and the European Union.

The intersection of data governance with national security is equally fraught. The 2021 Reserve Bank of India guidelines on digital lending[12] illustrate how sectoral regulators in the financial domain are asserting data governance authority independently of the broader legislative framework, creating regulatory fragmentation. Simultaneously, intelligence and law enforcement agencies across South Asia exercise extensive data access powers under national security laws that are effectively immune from the oversight mechanisms established in data protection legislation, a lacuna that directly implicates the constitutional proportionality standards articulated in Puttaswamy and its equivalents in other jurisdictions.

The emerging architecture of data governance in South Asia thus reflects a contested sovereignty claim, in which states seek to retain control over data as a strategic national resource while simultaneously participating in international digital economic integration. This trilemma — between individual rights, state authority, and market integration — is the defining structural tension of South Asian data governance and one that legislative frameworks,

[11]World Trade Organization, *Joint Statement Initiative on E-Commerce: Consolidated Negotiating Text* (WTO, 2024), INF/ECOM/87, 26 July 2024. India and most South Asian nations are not signatories to this JSI.
[12]Reserve Bank of India, *Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps* (RBI, 2021); see also RBI Master Direction on Digital Lending, 2022, Circular No. RBI/2022-23/111 DoR.CRE.REC.66/21.07.001/2022-23.

however sophisticated, cannot resolve without accompanying institutional investment, judicial oversight, and international regulatory cooperation.

VI. DATA GOVERNANCE AND THE SUSTAINABLE DEVELOPMENT GOALS

The relationship between data governance and the United Nations Sustainable Development Goals (SDGs) is mutually constitutive and deserving of explicit recognition in South Asian policy discourse.[13] SDG 16, which commits to building "peaceful, just and strong institutions," directly implicates the design of data protection regimes: the independence, accountability, and effectiveness of Data Protection Authorities are institutional indicators of the quality of governance. SDG 17, which mandates global partnerships for sustainable development, is relevant to the question of regulatory convergence across South Asian jurisdictions and the harmonisation of data governance norms with international frameworks.

Beyond SDG 16 and SDG 17, the data governance choices made by South Asian states have profound consequences for the achievement of the full spectrum of SDGs. Effective data protection frameworks, by building public trust in digital systems, facilitate the adoption of e-government services that underpin SDG 1 (No Poverty), SDG 2 (Zero Hunger), SDG 3 (Good Health and Well-Being), and SDG 4 (Quality Education). The safe and rights-respecting management of social protection data — including Aadhaar-linked welfare transfers in India and analogous systems elsewhere in South Asia — directly affects whether the most vulnerable populations receive the entitlements to which they are legally entitled without discriminatory exclusion or data-driven profiling.

Conversely, data protection failures impose disproportionate SDG costs on already marginalised communities. Data breaches involving biometric databases, the discriminatory use of algorithmic systems in credit scoring, and the surveillance of civil society through digital means all undermine the social contract that underpins sustainable development. The SDG framework thus provides both a normative mandate and an analytical toolkit for evaluating the adequacy of data governance regimes in South Asia — not as ends in themselves, but as institutional prerequisites for the realisation of human development.

[13]United Nations, *Transforming our World: the 2030 Agenda for Sustainable Development*, UN Doc A/RES/70/1 (25 September 2015). SDG 16 (Peace, Justice and Strong Institutions) and SDG 17 (Partnerships for the Goals) are directly relevant to data governance.

VII. TOWARDS REGIONAL CONVERGENCE: RECOMMENDATIONS

This comparative analysis surfaces five priority areas for legislative, institutional, and regional reform in South Asian data governance.

A. Strengthening Regulatory Independence

Data protection authorities across South Asia must be structurally insulated from executive direction. This requires statutory guarantees of security of tenure for authority members, financial independence from annual appropriations, and transparent appointment processes involving parliamentary or independent judicial oversight. The Sri Lankan model of a dedicated Data Protection Authority, despite its early-stage limitations, provides a more structurally independent design than India's Data Protection Board, which adjudicates complaints but lacks proactive regulatory and standard-setting powers.

B. Harmonising Consent Architectures

The divergent approaches to consent across South Asian data protection regimes — ranging from India's layered consent-and-legitimate-use model to Bangladesh's proposed consent-centric framework — create compliance fragmentation for regional digital businesses and reduce the portability of data subject rights across borders. South Asian states should work through SAARC and BIMSTEC frameworks to develop a regional minimum standard for consent architecture, including uniform requirements for freely given, specific, informed, and unambiguous consent, and harmonised rules for the withdrawal of consent.

C. Codifying Children's Data Protections

Every South Asian jurisdiction should legislate dedicated provisions for children's data protection, extending beyond parental consent requirements to address the systemic collection of children's biometric data in education and social protection programmes, the prohibition of profiling and targeted advertising directed at minors, and the mandatory conduct of data protection impact assessments before deploying digital systems in educational settings. The DPDPA's provisions on children's data offer a starting point, but implementation through subordinate legislation must be expedited.

D. Designing Proportionate State Access Regimes

The constitutionally mandated proportionality standard in Puttaswamy, and its equivalents in other South Asian constitutional traditions, requires that state access to personal data be authorised by law, necessary for a specified legitimate aim, and proportionate in scope and duration. South Asian legislatures should introduce dedicated statutory frameworks governing intelligence and law enforcement access to data, incorporating judicial authorisation requirements, data retention limits, and meaningful oversight mechanisms, rather than relying on broad national security exemptions in data protection legislation.

E. Engaging the SDG Architecture for Normative Legitimacy

Regional data governance reform in South Asia should explicitly align with and draw normative legitimacy from the SDG framework, particularly SDG 16's commitment to accountable and transparent institutions. SAARC and BIMSTEC should adopt a regional declaration on data governance principles, referencing the SDG 2030 Agenda, the UN resolutions on the right to privacy in the digital age,[14] and the emerging body of international soft law on artificial intelligence and digital governance, to build a coherent normative architecture that reflects both universal human rights standards and Global South developmental priorities.

VIII. CONCLUSION

South Asian data governance stands at a pivotal juncture. The legislative initiatives undertaken by India, Sri Lanka, and Bangladesh — however imperfect in their current form — represent meaningful steps towards the recognition of personal data protection as a fundamental legal entitlement rather than a discretionary regulatory choice. Yet the analysis presented in this paper demonstrates that the gap between legislative text and lived regulatory reality remains wide, shaped by institutional deficits, contested sovereignty claims, and the structural power asymmetries of the global digital economy.

The global normative architecture — anchored by the GDPR, UN resolutions, and the SDG framework — provides South Asian states with a rich repository of principles and best

[14]United Nations General Assembly Resolution 68/167, "The Right to Privacy in the Digital Age," UN Doc A/RES/68/167 (18 December 2013); see also UN Human Rights Council Resolution 28/16, UN Doc A/HRC/RES/28/16 (1 April 2015).

practices, but contextualisation to the sub-region's developmental realities, constitutional traditions, and governance capacities is non-negotiable. The challenge is not simply to transplant Northern regulatory models but to build data governance institutions that are capable of simultaneously protecting individual rights, enabling digital development, managing legitimate security concerns, and contributing to the equitable governance of the global data economy.

Regional convergence, pursued through the existing mechanisms of SAARC and BIMSTEC[15] and informed by the SDG architecture, offers the most promising pathway towards a South Asian data governance ecosystem that is interoperable, rights-respecting, and institutionally resilient. The legal academy, civil society, and the emerging community of data protection practitioners across the sub-continent have an indispensable role to play in building the intellectual foundations and advocacy capacity that this governance transformation demands. The South Asian Law and Policy Conclave 2026 provide precisely the kind of interdisciplinary, Global South-centred forum that this conversation requires.

[15]South Asian Association for Regional Cooperation (SAARC), *SAARC Convention on Mutual Assistance in Criminal Matters* (2008); see also BIMSTEC Framework Agreement on Trade in Services (2018) which includes emerging provisions on digital trade but lacks a binding data protection protocol.